UNIVERSITY OF PÉCS

FACULTY OF LAW

DOCTORAL DISSERTATION

Big Data and Artificial Intelligence
An examination of the existing legal framework from a data protection perspective

AUTHOR: Branka MANIA
SUPERVISOR: Dr. Gergely SZŐKE

PÉCS 2023

Abstract

This dissertation examines the legal framework for Big Data and Artificial Intelligence from a data protection perspective. This research aims to contribute to the body of knowledge with regards to present and future legal conditions applicable to the processing of personal data in the context of automated and algorithmic data processing systems. The approach taken was to explain characteristics and identify various potential risks of Big Data and AI, and to provide a comprehensive overview of the existing and proposed legal regime that applies to the processing of personal data when novel technologies are used with a focus on but not limited to the General Data Protection Regulation. The investigation of legal resources showed that the regulation of automated or algorithm-based data processing is not in its infancy, and that existing data protection laws address issues that arise out of the use of Big Data and AI. It also demonstrated challenges and limitations of traditional concepts such as transparency and privacy self-management, and discussed whether and how they could be further developed, including new control mechanisms which may be based on numerous international initiatives that have provided expert guidance and recommendations for the use and regulation of AI.

Ez a disszertáció a Big Data és a mesterséges intelligencia jogi kereteit vizsgálja adatvédelmi szempontból. A kutatás célja, hogy hozzájáruljon a személyes adatok automatizált és algoritmus alapú kezelésére vonatkozó, jelenlegi és jövőbeli jogi szabályozással kapcsolatos ismeretanyaghoz. A dolgozat célja a Big Data és a mesterséges intelligencia jellemzőinek ismertetése és a különböző potenciális kockázatok azonosítása, valamint átfogó áttekintés nyújtása a személyes adatoknak az új technológiák keretében történő feldolgozására vonatkozó jelenlegi és javasolt jogi szabályozásáról, különös tekintettel, de nem kizárólag az általános adatvédelmi rendeletre. A felhasznált források vizsgálata kimutatta, hogy az automatizált vagy algoritmusalapú adatfeldolgozás szabályozása részben kidolgozott, a meglévő adatvédelmi jogszabályok is foglalkoznak a Big Data és a mesterséges intelligencia alkalmazásából eredő kérdésekkel. Bemutatta továbbá az olyan hagyományos fogalmakkal kapcsolatos kihívásokat és korlátokat, mint az átláthatóság és az adatvédelmi önszabályozás, és javaslatott tett arra, hogy ezeket hogyan lehetne továbbfejleszteni, beleértve az új ellenőrzési mechanizmusokat is. Ezek számos olyan nemzetközi kezdeményezésen alapulhatnak, amelyek iránymutatást és ajánlásokat adtak a mesterséges intelligencia felhasználására és szabályozására vonatkozóan.

Table of contents

Abbreviations / Glossary

ACM	Association for Computing Machinery
ADPPA	American Data Privacy and Protection Act
AHEG	UNESCO’s Ad Hoc Expert Group
AI	Artificial Intelligence
AIDA	Artificial Intelligence and Data Act
AIGO	OECD’s Working Party on Artificial Intelligence Governance
AILD	AI Liability Directive
ALKS	Automated Lane Keeping Systems
ANN	Artificial Neural Network
APEC	Asia-Pacific Economic Cooperation
APPI	Act on the Protection of Personal Information
A/IS	Artificial Intelligence and Autonomous Systems
Art29WP	Article 29 Working Party
AVMSD	Audiovisual Media Services Directive
B2B	Business-to-Business
B2C	Business-to-Consumer
B2G	Business-to-Government
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BIPA	Illinois Biometric Information Privacy Act
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BREXIT	British Exit from the European Union
CAHAI	Ad Hoc Committee on Artificial Intelligence
CAI	Committee on Artificial Intelligence
CCTV	Closed Circuit Television
CalOPPA	California Online Privacy Protection Act
CCPA	California Consumer Privacy Act

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPEJ	European Ethical Charter on the Use of AI in Judicial Systems
CETA	Comprehensive Economic and Trade Agreement
Charter	Charter of Fundamental Rights of the European Union
CDEI	Centre for Data Ethics and Innovation
CIPA	California Invasion of Privacy Act
CIPL	Centre for Information Policy Leadership
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
COE	Council of Europe
CPA	Colorado Privacy Act
CPRA	California Privacy Rights Act
Commission	European Commission
Convention	European Convention on Human Rights
COPPA	Children's Online Privacy Protection Act
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CRA	Cyber Resilience Act
CRM	Customer Relations Management
CSA	Cyber Solidarity Act
CTA	Consumer Technology Association
CTR	Clinical Trials Regulation
DORA	Digital Operational Resilience Act
DGA	Data Governance Act
Directive	Data Protection Directive
DMA	Digital Markets Act
DPA	Data Protection Agreement
DPIA	Data Protection Impact Assessment

DPO	Data Protection Officer
DSA	Digital Services Act
DSK	Datenschutzkonferenz
DSAR	Data Subject Access Request
DSRI	Deutsche Stiftung für Recht und Informatik
EAD	Ethically Aligned Design
EEA	European Economic Area
ECHR	European Convention on Human Rights
ECNL	European Center for Non-For-Profit-Law
ECPAIS	IEEE’s Ethics Certification Program for Autonomous and Intelligent Systems
ECtHR	European Court of Human Rights
EDRi	European Digital Rights Association
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EFF	Electronic Frontier Foundation
EFTA	European Free Trade Association
EHDS	European Health Data Space
ENISA	European Union Agency for Network and Information Security
EP	European Parliament
EU	European Union
ETSI	European Telecommunications Standards Institute
DETOUR Act	Deceptive Experiences to Online Users Reduction Act
FAT/ML	Fairness, Accountability, and Transparency in Machine Learning
FCRA	Fair Credit Reporting Act
FFHA	Fair Housing Act
FIPP	Fair Information Practice Principles
FLIA	Foundation for Law and Internal Affairs
FLoC	Federated Learning of Cohorts

FOIA	Freedom of Information Act
FRA	European Union Agency for Fundamental Rights
FTC	Federal Trade Commission
GAN	Generative Adversarial Networks
GAPPs	Generally Accepted Privacy Principles
GATS	World Trade Organization’s General Agreement on Trade and Services
GDD	Gesellschaft für Datenschutz und Datensicherheit
GINA	Genetic Information Nondiscrimination Act
GLBA	Gramm-Leach-Bliley Act
GPAI	Global Partnership on AI
GDPR	General Data Protection Regulation
GPEN	Global Privacy Enforcement Network
HIPAA	Health Insurance Portability and Accountability Act
HLEG	High-Level Expert Group on Artificial Intelligence
HRIA	Human Rights and Algorithmic Impact Assessments
HRAIS	High-risk Artificial Intelligence Systems
HUDERAC	Human Rights, Democracy, and the Rule of Law Assurance Case
HUDERAF	Human Rights, Democracy, and the Rule of Law Assurance Framework
HUDERIA	Human Rights, Democracy, and the Rule of Law Impact Assessment
IAF	Information Accountability Foundation
IAPP	International Association of Privacy Professionals
ICCPR	International Covenant on Civil and Political Rights
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICO	Information Commissioner’s Office
ICT	Information and Communications Technology
IDFA	ID for advertisers
ICESCR	International Covenant on Economic, Social and Cultural Rights
IEC	International Electro-technical Commission

IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IRCAI	International Research Center on Artificial Intelligence
ISMS	Information Security Management Systems
ISO	International Standards Organization
ISP	Internet Service Provider
ITPDCA	Transparency and Personal Data Control Act
ITU	International Telecommunication Union
IWGDPT	International Working Group on Data Protection in Telecommunications
LAWS	Regulations with regards to the use of lethal autonomous weapons systems
LIBE	EP's Committee on Civil Liberties, Justice and Home Affairs
MDPPA	Massachusetts Data Privacy Protection Act
MEP	Member of European Parliament
MiFiD	Markets in Financial Instruments Directive
MILA	Quebec Artificial Intelligence Institute
MIPSA	Massachusetts Information Privacy and Security Act
MIT	Massachusetts Institute of Technology
ML	Machine Learning
NDAA	National Defense Authorization Act
NGO	Non-governmental Organization
NISD	Network and Information Security Directive
NIST	National Institute of Standards and Commerce
NITI	National Institution for Transforming India
NLP	Natural Language Processing
NYOB	None of Your Business (NGO)
OECD	Organization for Economic Development
OI	Organoid Intelligence
ONE AI	OECD's Network of Experts on AI

OSTP	White House Office of Science and Technology Policy
OWASP	Open Web Application Security Project
PAI	Partnership on AI
PDPC	Personal Data Protection Commission
PECD	Privacy and E-Communications Directive
PET	Privacy Enhancing Technologies
PHI	Protected Health Information
PII	Personally Identifiable Information
PIMS	Privacy Information Management System
PIN	Personal Identification Number
PIU	Pathological Internet Use
PLD	Product Liability Directive
PSD2	Payment Services Directive
PSI	Public Sector Information
R&D	Research and Development
SA	Supervisory Authority
SCAI	Partnership on AI’s Safety-Critical AI Working Group
SCC	Standard Contractual Clauses
SDAA	Stop Discrimination by Algorithms Act
SDG	Sustainable Development Goals
SOC	Security Operations Center
TCC	Trade and Technology Council
TCPA	Telephone Consumer Protection Act
TFEU	Treaty on the Functioning of the European Union
TKG	German Telecommunications Act
TMG	German Telemedia Act
TPP	Trans-Pacific-Partnership
TTC	U.S.-EU Trade and Technology Council

TTDSG	German Telecommunications Telemedia Data Protection Act
UCPA	Utah Consumer Privacy Act
UCTD	Unfair Contract Terms Directive
UDHR	Universal Declaration of Human Rights
UGAI	Universal Guidelines for Artificial Intelligence
UK	United Kingdom
UN	United Nations
UNECE	United Nations Economic Commission for Europe
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGP	United Nations Guiding Principles on Business and Human Rights
UNHROHC	UN Human Rights Office of the High Commissioner
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNI	UNI Global Union
UNODA	United Nations Office for Disarmament Affairs
U.S.	United States
U.S.A.	United States of America
VCDPA	Virginia Consumer Data Protection Act
WTO	World Trade Organization

1. Introduction, hypotheses, and methodology

1.2. Introduction

From a business perspective, the use of algorithmic data processing systems is very attractive as it allows for time and cost efficiency as well as real-time insights, detailed analytics, and forecasting. From an individual`s perspective, the use of Big Data, automated decision-making, and Artificial Intelligence (AI) may lead to a variety of consequences: complex data processing operations which are performed by self-learning machines that are solely based on data-driven predictive models may not be transparent anymore. Any such processing is thus potentially opaque and may lack human oversight and could lead to secondary and unpredictable use of personal information, (secret) scoring and profiling, or may even have the potential for discrimination or surveillance. These effects can pose serious threats to individuals' chances in life as nowadays, housing, loan or job decisions are often taken with the help of AI systems. Privacy self-management seems hard to achieve given the lack of choices, market dominance, imbalance of powers or information mismatch between data subjects and controllers. From a data protection perspective, these circumstances together with effects like data aggregation and maximization or derivative use of personal information may contradict with common principles of data protection laws such as lawfulness, fairness, transparency, or purpose limitation and accountability. This in turn leads to the question what the current legal framework looks like given the various implications that go with the use of algorithmic technology. To answer this question, the characteristics, benefits, use cases and especially risks of Big Data and Artificial Intelligence must be assessed, as well as the existing legal framework that applies to the algorithmic, autonomous, probabilistic, data processing and decision-making that is based on personal, user, behavior, sensor, etc. data. The evaluation included further relevant sources of law such as product, trade, security, liability, or data and processing specific rules at international, European, national, or sectoral level to complete the picture about existing regulatory conditions in this context and to provide a global overview because data processing does not stop at borders. The research focused on the General Data Protection Regulation since it is a role model law for many other jurisdictions and elaborated on the legal situation in the U.S. because the U.S.A. are home to all relevant Big Tech players, meaning that any applicable local privacy or consumer protection laws de facto have global impact. As regards the viability of traditional concepts in data protection laws and whether these approaches capture novel risks of AI, the Thesis elaborates on challenges of transparency and privacy self-management and phenomena like fragmentation and the shifting of the protection of fundamental rights. It concludes with a comprehensive outlook on legislative, regulatory, or non-governmental proposals and expert guidelines that have been suggested for the regulation of Artificial Intelligence to identify recurring motifs and statements that may serve as a basis for a future-proof regulation of AI. Artificial Intelligence has the potential to shape our lives in good and bad ways like the case of Clearview AI[1] or the role of AI in medicine[2] demonstrate. At the same time, the use of Big Data, ADM, and AI pose various data protection risks, and that is why this research topic is valuable from a scientific point of view.

1.2. Hypotheses

Within the framework of this Thesis, the following three main hypotheses are formulated: first, privacy self-management failed for a variety of reasons. In many instances, it deteriorated into a mere click-mechanism, a take-it-or-leave-it-approach, a repetitive element in data-for data-services-business-models. Privacy self-management requires valid consent, but that is difficult to imagine given the information asymmetries and imbalances between parties. Current data subject rights such as the right to right to information, the right to withdraw consent, the right to object, or the right to restrict data processing do not result in explainability of processing operations or reproducibility of decisions, which may perhaps be needed to take informed decisions and properly exercise individual rights. Depending on the circumstances, secondary use of personal information may be admissible, or processing may be privileged for various reasons, leaving little space for the exercise of such rights. In consequence, privacy self-management does not lead to the desired protections, especially not in an era in which is characterized by the inconsistency between peoples' opinions on the relevance of privacy and their actual behavior, for example, by accepting so-called ambient intelligence[3] and luxury surveillance[4] which enable constant monitoring and analysis of activities and behavior. Second, the transparency principle needs to be further developed, moving away from lengthy one-time notices that address individuals that are written by lawyers for lawyers in the direction of comprehensive, meaningful, and appropriate[5] information, towards publicity obligations that address a wider audience. Even if information is provided in a compliant manner, individuals are often overwhelmed with privacy notices,

[1] What used to be the preserve of law enforcement identification services and subject to judicial review, became a flourishing private sector service, see Samuel Stolton: After Clearview AI scandal, Commission 'in close contact' with EU data authorities. Article published February 12 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/. Retrieved September 26, 2021.

[2] What used to be the preserve of physicians and surgeons who have studied and trained for many years, became a use case for diagnostics or robot surgery and promises to revolutionize patient care, see MedTech Europe, the European trade association for the medical technology industry including diagnostics, medical devices and digital health provides background information on AI in the health sector on their website, available at https://www.medtecheurope.org/resource-library/ai-in-medical-technologies/. Retrieved July 22, 2022.

[3] Ambient intelligence is a term that describes a technology where devices are not perceived as they slip into the background, but they are "always on", meaning that they constantly collect (sensitive) information, see Diane Cook, Juan Augusto, Vikramaditya Jakkula: Ambient intelligence: Technologies, applications, and opportunities. Article published in Pervasive and Mobile Computing 2009, vol. 5, issue 4, pp. 277-298, available at https://www.sciencedirect.com/science/article/abs/pii/S157411920900025X#:~:text=Ambient%20intelligence%20is%20an%20emerging%20discipline%20that%20brings,and%20sensor%20networks%2C%20pervasive%20computing%2C%20and%20artificial%20intelligence. Retrieved October 18, 2021.

[4] Chris Gilliard: The rise of luxury surveillance. Article published October 18 2022, available at https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/. Retrieved October 18, 2022.

[5] That means ad hoc and repetitive, see GDPR Art. 13 III.

and transparency obligations are limited, not only because of trade secrets.[6] Information on the underlying logic of an algorithm is not the same as explainability of the processing or replicability of the decision in question, and information addressed to concerned data subjects is not the same as, for example, general labeling obligations when humans interact with AI irrespective of legal or other significant effects, or public AI registries that allow for better access to relevant information such as details on risk evaluations, or information on sub-processors: making true operators known could truly help with clarity on controllers and their accountability share. Such duties could increase the chances for the needed awareness and social debate, which is an important instrument as it allows for better insight into how algorithmic apps can be used like the case on leaks on Meta's practices has proven,[7] and it could furthermore foster individual engagement, which is a factor that should not be underestimated as a single person's commitment has brought down an entire mechanism for international data transfers. Third, new controls are needed on top of existing standard documentation, self-evaluation, and vendor management requirements. In the context of new controls, ideas range from mandatory external assessments and auditing requirements, monitoring of AI systems, and the formation of specialist independent oversight bodies with simplified coherence mechanisms, including the right to issue orders against any processor and manufacturers to capture all players. Further suitable concepts could be the introduction of specific technical standards, the use of synthetic data, the use of sandboxes, or a standardization of testing procedures because poor data quality and errors in the design of AI apps may lead to bias and discrimination. New data subject rights such as having personal information replaced rather than having the processing restricted could be a more effective way to avoid re-identification. There are also debates about data ownership to fight data monetization, but it is questionable how that may work in practice, however, contractual limitations of the use of personal data are not unimaginable given that service-for-data is a well-established business model, but at present, it is strictly unilateral. From an individual's perspective, the right to participation and the right to human intervention as well as enhanced redress mechanisms and a broader right of action for consumer protection and competition authorities could be useful to successfully enforce individual's rights. AI's capability for surveillance[8] and its potential impact on human rights[9] makes it worthwhile to think about mandatory human rights impact assessments and the introduction of further principles such as non-

[6] Sandra Wachter, Brent Mittelstadt, Luciano Floridi: Why a right to explanation of automated decision-making does not exist in the GDPR. International Data Privacy Law 2017, vol. 7, issue 2, pp. 76-99. Retrieved September 26, 2021.

[7] Ryan Browne: Facebook whistleblower behind major leak is going to testify in Europe. Article published October 12 2021, available at https://www.cnbc.com/2021/10/12/facebook-whistleblower-behind-major-leak-is-going-to-testify-in-europe.html. Retrieved January 22 2022.

[8] Melissa Heikkilä: The rise of AI surveillance. Article published May 26 2021, available at https://www.politico.eu/article/the-rise-of-ai-surveillance-coronavirus-data-collection-tracking-facial-recognition-monitoring/. Retrieved February 21, 2022.

[9] Amnesty International, Privacy International, and the Centre for Research on Multinational Corporations published a report "Operating from the shadows" in which they want to draw attention to the human rights risks of the global surveillance industry. Report published 2021, available at https://www.privacyinternational.org/sites/default/files/2021-06/DOC1041822021EN.pdf. Retrieved February 28, 2023.

discrimination and inclusion, equality and diversity that should be applied whenever algorithmic processing is in question. The mass application of Big Data, AI and automated decision-making not only affects individuals but society, and digital workforce aspects show that there is an important intersection between individual rights and societal values. Consequently, new values shall not only be judged at data subject level but consider the societal perspective and therefore include public safety and termination obligations in the event AI gets out of control. A repetitive request in the context of taking a human-centric approach that serves society is the demand to embed ethics into Big Data, ADM, and AI. But ethics are an ambivalent requirement because the interpretation of ethically acceptable standards may vary, and ethics may moreover serve as an escape from regulation.[10] While it is comprehensible that industry may prefer a deregulated landscape for novel technology claiming that regulation stifles innovation, self-regulation has not proven to work: "legislative history in the course of industrial revolutions and across various sectors, be it transportation, chemical engineering, communications, aviation or biotechnology and digitization has shown that voluntary codes or self-regulation may simply not work, and that regulatory discussions should not primarily focus on specific harms or individual risks but also take the systemic and structural risk of AI into consideration."[11] The dominating perception of AI is its huge positive impact in operations, analytics, or medicine, but what is often overlooked is that Artificial Intelligence also has a remarkable potential for malicious use. Risks are growing[12] as fast as processing capabilities: with today's technology, a single photo is enough to create a Deep Fake to embarrass or blackmail somebody;[13] biometric data taken from public events can be used to fool security systems to gain illegitimate access to systems and data,[14] or to exploit human vulnerabilities by using speech synthesis for impersonation.[15] Already today, AI is incorporated in slaughter-bots,[16] and it is therefore incomprehensible why this technology should be treated in a different manner than any other technology for which imminent high risks have been identified such as autonomous vehicles, weapons,

[10] Ben Wagner: Ethics as an escape from regulation. From ethics-washing to ethics-shopping? In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds.): Being profiled – cogitas ergo sum. 10 years of profiling the European citizen. Amsterdam University Press 2018, pp. 84-88.

[11] Julia Black, Andrew Murray: Regulating AI and Machine Learning: setting the regulatory agenda, European Journal of Law and Technology 2019, vol. 10, issue 3, available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 22, 2021.

[12] Zoe Kleinman, Chris Vallance: AI 'godfather' Geoffrey Hinton warns of dangers as he quits Google. Article published May 3 2023, available at https://www.bbc.com/news/world-us-canada-65452940. Retrieved May 5, 2023.

[13] Karen Hao: A horrifying new AI app swaps women into porn videos with a click. Article published September 13 2021, available at https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/. Retrieved October 22, 2021.

[14] An election poster of former German chancellor Dr. Angela Merkel was enough to present how easily an iris scan can be manipulated, see Stefan Krempl: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck. Article published December 28 2014, available at https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html. Retrieved October 23, 2021.

[15] Dominic David: Analyzing the rise of deepfake voice technology. Article published May 10 2021, available at https://www.forbes.com/sites/forbestechcouncil/2021/05/10/analyzing-the-rise-of-deepfake-voice-technology/. Retrieved October 22, 2021.

[16] Sam Shead: UN talks to ban 'slaughter-bots' collapsed – here's why that matters. Article published December 22 2021, available at https://www.cnbc.com/2021/12/22/un-talks-to-ban-slaughterbots-collapsed-heres-why-that-matters.html. Retrieved January 22, 2022.

or nuclear power.[17] Consequently, many recognize the necessity to draw red lines[18] and therefore insist on prohibitions of certain AI, for example, Artificial Intelligence that is used for secret profiling, social scoring, or facial recognition. An important conclusion therefore is that algorithmic accountability is needed, ideally, with a specific liability regime in the style of product liability and consumer protection regulations.

1.3. Methodology

To examine whether the legal and regulatory framework captures and matches possible risks involved in the use of novel technology such as Big Data and AI applications, the Thesis first takes a descriptive approach by explaining the history of data privacy and emergence of data protection laws and what they aim to protect. The Thesis then explains the main unique properties of Artificial Intelligence and explores on various potential risks that come with the use of this novel technology. In the context of the examination of existing laws, the Thesis starts with legal definitions which are relevant for the scope and applicability of laws and elaborates on numerous laws and regulations that include data protection provisions, be it on international, EU, sectoral or national level. The Thesis takes a systematic, analytical, and critical approach by identifying relevant legal and regulatory sources globally, including a variety of legislative as well as civil society and private sector proposals for the future regulation of AI. The Thesis provides introductory notes as well as brief summaries for each chapter and concludes with a comprehensive summary of findings with are relevant for the hypotheses.

2. History of privacy, development of data protection laws and the emergence of Big Data, Automated Decision Making, and AI

As an introduction to the Thesis topic, this chapter provides a brief history of the right to privacy and explains the development of data protection laws by illustrating the foundations of the right to privacy, and relevant legislative developments in recent decades. This chapter furthermore deals with the emergence of Big Data, automated decision-making, and Artificial Intelligence owing to technological progress to demonstrate the relevance of AI in today's world.

[17] Microsoft founder Bill Gates is quoted to have said that "A.I. is like nuclear energy – both promising and dangerous" during the 2019 2019 Human-Centered Artificial Intelligence Symposium at Stanford University. Source: https://www.cnbc.com/2019/03/26/bill-gates-artificial-intelligence-both-promising-and-dangerous.html. Retrieved October 22, 2021.

[18] MILA's chief executive Valérie Pisano believes the slapdash approach to safety in AI systems would not be tolerated in any other field, see Josh Taylor, Alex Hern: 'Godfather of AI' Geoffrey Hinton quits Google and warns over dangers of misinformation. Article published May 2 2023, available at https://www.theguardian.com/technology/2023/may/02/geoffrey-hinton-godfather-of-ai-quits-google-warns-dangers-of-machine-learning. Retrieved May 5, 2023.

2.1. Brief history of the right to privacy

It is difficult to say when exactly the first ideas on the right to privacy came up. Some years ago, the Bavarian State Commissioner for Data Protection[19] organized an exhibition called "From the oath of Hippocrates to Edward Snowden: a short journey through 2500 years of data protection".[20] This title shows that the origins of data protection – or at least some aspects like patient confidentiality – are much older than one would suggest, and this does not only apply to the medical field: first basic ideas about privacy came up in the late Middle Ages and the early Renaissance: the confessional secret dates back to the fourteenth century and the banking secrecy dates back to the sixteenth century.[21] However, there were times in which, apart from any legal protection, even walls and single beds were regarded as a means of privacy.[22] Already in 1890, two lawyers from the United States, wrote an Article called "The Right to Privacy",[23] in which they argued that laws must be adapted to reflect technological change due to the increasing capacity of certain institutions to invade previously inaccessible aspects of personal activity. They defined the protection of the private as the foundation of individual freedom in the modern age and concluded that legal remedies had to be developed to enforce definite boundaries between public and private life.[24] Later on in his career as a judge, one of the authors explained[25] that the right to be let alone as the most comprehensive of rights. Basic concepts of respecting the right to privacy were set out around 1950, decades before computer usage grew exponentially: in 1948, the United Nations proclaimed the Universal Declaration of Human Rights in 1948 response to World War II.[26] The Universal Declaration of Human Rights sets out, for the first time, fundamental human rights to be

[19] The German state of Bavaria has two data protection authorities, one for the public sector, chaired by state commissioner, see: https://www.datenschutz-bayern.de/, and one for the private sector, see https://www.lda.bayern.de/de/praesident.html. Retrieved September 25, 2021.

[20] Bavarian State Commissioner for Data Protection: Ausstellungseröffnung: Vom Eid des Hippokrates bis zu Edward Snowden - eine kleine Reise durch 2500 Jahre Datenschutz. Press release published March 31 2014, available at https://www.datenschutz-bayern.de/presse/20140331_Ausstellung.pdf. Retrieved September 25, 2021.

[21] Andreas Schneider: Die Datenschutz-Grundverordnung. Presentation held at the KISA forum on February 18 2018, available at https://www.kisa.it/de/datei/anzeigen/id/19667,3/datenschutzgrundverordnung.pdf. Retrieved September 25, 2021.

[22] Greg Ferenstein: The birth and death of privacy: 3000 years of history told in 46 images. Article published November 25 2015, available at https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e#.8tcuzmf86. Retrieved September 25, 2021.

[23] Samuel Warren, Louis Brandeis: The right to privacy, Harvard Law Review 1890, vol. 4, no. 5, pp. 193-220. Article available at http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Retrieved September 25, 2021.

[24] Warren and Brandeis (pp.193-195) explain how the protection of the individual developed: from the protection of property over the protection against noises, odors, dust, and smoke to the protection of the individual's intangible property and feelings and finally the protection against "unauthorized circulation of portraits of private persons" and the "evil of the invasion of privacy by newspapers".

[25] Brandeis' dissent in the case Olmstead v. United States, available at https://my.ilstu.edu/~jkshapi/Brandeis_Olmstead%20Dissent.pdf. Retrieved September 25, 2021.

[26] The Universal Declaration of Human Rights is available at http://www.un.org/en/universal-declaration-human-rights/index.html. Retrieved September 25, 2021.

universally protected, and this includes privacy.[27] Only two years later, the European Convention on Human Rights was adopted, and it included the right to respect for private and family life.[28] In addition, the EU enacted the Charter of Fundamental Rights of the European Union[29], and the specialty about this charter is that it explicitly also addresses the protection of personal data.[30] It is remarkable that the respect for private life and the right to data protection emerged much earlier than mass processing of personal data. It is also notable that even in specialist circles,[31] the Universal Declaration of Human Rights, the Charter and the Convention are sometimes better known or maybe even more recognized than the 1981 Council of Europe Data Protection Convention (108+).[32] This is not comprehensible insofar as this convention formulated several basic principles which are still valid today, for example, that personal data shall be processed lawfully, fairly and in a transparent manner and that personal data shall be accurate and kept up to date and collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes.[33] In addition, this convention is the only legally binding multilateral agreement in the field of personal data protection[34] - unlike the 1980 OECD guidelines on the protection of privacy and trans-border data flows of personal data, which are nonetheless a very important[35] contribution to the overall data protection framework. It can therefore be said that, in the time-period between World War II and the early 1980s, important (binding) international statutes have been created.

[27] UDHR Article 12 stipulates that "no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[28] The European Convention on Human Rights is available at https://www.echr.coe.int/Documents/Convention_ENG.pdf. Retrieved September 25, 2021.

[29] The Charter of Fundamental Rights of the European Union is available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Retrieved September 25, 2021.

[30] Article 8 of the Charter postulates that "everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly, for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority*"*.

[31] The German consultancy Datenschutz Nord reported on this issue on their website, published March 19 2019, available at https://www.datenschutz-notizen.de/die-konvention-nr-108-die-kleine-schwester-der-dsgvo-0222164/. Retrieved September 25, 2021.

[32] Official name: The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Convention text available at https://rm.coe.int/16808ade9d. Retrieved September 25, 2021.

[33] See Article 5 of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data, available at https://rm.coe.int/16808ade9d. Retrieved September 25, 2021.

[34] Background information on the Convention is provided by Jennifer Baker in her article: What does the newly signed 'Convention 108+' mean for UK adequacy? Article published October 30 2018, available at https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/. Retrieved September 25, 2021.

[35] A continuous contribution: information on OECD's work on information security and privacy is available at http://www.oecd.org/internet/ieconomy/oecdprivacystatementgenerator.htm. Retrieved September 25, 2021.

2.2. Development of data protection law

As far as national legislation is concerned, some sources[36] claim that the 1973 Swedish Data Act was the world's first national data protection law. However, the Hessian Data Protection Act was passed in 1970[37] and may therefore be considered the first data protection law in Europe. It can generally be said that the first generation of data protection norms appeared in the 1970s, which is also true for the U.S. as the 1970 Fair Credit Reporting Act[38] contained elements of data protection. Another example is the 1972 amendment of the Californian Constitution[39] which established an enforceable right to privacy including the ability of individuals to control the use and / or sale of their personal information, or the 1974 Privacy Act which established a code of "fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[40] This first statutory codification wave did not use terms like privacy and was rather concerned about the state sector and public authorities. Well-known concepts such as technical and / or organizational rules for processing were included.[41] Apart from security safeguards, basic concepts such as transparency and principles which govern the collection, use, and dissemination of information about individuals including the right to individual participation were introduced not only in Europe, but also in the U.S. based on the so-called Fair Information Practice Principles (FIPP).[42] Even though there is no comprehensive federal data protection act covering the private sector in the U.S. until today,[43] many FIPP principles have been fully or partially implemented in specific laws,[44] and there are important sector-specific and / or business-model relevant regulations like the 1998 Children's Online

[36] The bill text is available at https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289. Retrieved September 25, 2021.

[37] Background information on the Hessian Data Protection Act is provided by the Hessian supervisory authority, available at https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes. Retrieved September 25, 2021.

[38] Privacy International: The keys to data protection – a guide for policy engagement on data protection. Article published August 2018, available at https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf. Retrieved September 25, 2021.

[39] The International Association of Privacy Professionals provides background information in the framework of their report on the emergence of the CCPA and CPRA. Article published February 2021, available at https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/. Retrieved September 25, 2021.

[40] Details on the Privacy Act of 1974 are provided by the U.S. Department of Justice at their website, available at https://www.justice.gov/opcl/privacy-act-1974. Retrieved September 25, 2021.

[41] Background information on the history of data protection is provided by Viktor Mayer-Schönberger: Generational development of data protection in Europe in: Philip E. Agre, Marc Rotenberg (eds.): Technology and privacy – the new landscape. Massachusetts Institute of Technology Press 1998, pp. 219-241.

[42] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[43] However, businesses have to comply with certain (consumer protection) rules and standards (e.g. unfair or deceptive acts or practices) which are enforced by the Federal Trade Commission, and which quite often have an intersection with data protection law. FTC's work and mandate is explained in greater detail at https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act. Retrieved September 25, 2021.

[44] Serge Gutwirth, Ronald Leenes, Paul De Hert: Data Protection on the move – current developments in ICT and privacy / data protection. Springer Science + Media Publishing 2016, p. 181.

Privacy Protection Act[45] (COPPA) and the 1996 Health Insurance Portability and Accountability Act (HIPAA).[46] Already in 1967, the Freedom of Information Act (FOIA) came into effect in the U.S. which provides individuals with the right access documents from state agencies.[47] It is important to note, however, that the greatest difference between the U.S. and the EU approach to data protection is that, under European law, a legal basis is always required for the processing of personal data, whereas in the US, the contrary is true, because data can generally be processed unless a law specifically forbids such an activity.[48] It can therefore be said that, within the EU, the most important data protection rule is that a prohibition (of the collection, of the use) of processing applies which is subject to permission (by law, by individual consent). Further European countries passed their data protection bills in the late seventies, e.g., France in 1978, Luxembourg in 1979, and other countries like Portugal, Belgium and Spain followed later on in 1991 and 1992.[49] The second generation of data protection laws emphasized data subject rights, and the idea behind that was that the individual may be the best guarantee for successful enforcement of data protection laws.[50] In 1983, the German Federal Constitutional Court issued a decision[51] regarding the collection of personal information collected during the 1983 census. Ever since, this decision is considered a milestone of data protection as it introduced the concept of so-called "informational self-determination" and introduced a new fundamental right. In this decision, the court dealt with the question whether individuals themselves shall be able to determine collection, storage, use or disclosure of their data to others. Even though it is not the same, in this respect, the decision is similar to the concept of the "right to privacy" in the United States legal tradition. The protection of privacy, the right to a private life, the protection of personal data, or the right to public sector information all fall under the umbrella of informational self-determination.[52] The court explicitly linked these matters to constitutional rights – an idea which is one of the characteristics of the third generation of data

[45] The text of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501–6505) is available at http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim. Retrieved September 25, 2021.

[46] The text of the Health Insurance Portability and Accountability Act is available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html. Retrieved September 25, 2021.

[47] Details on the Freedom of Information Act are available at https://www.foia.gov/about.html. Retrieved September 25, 2021.

[48] Daniel Solove: Introduction – Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, vol. 126:1880, p. 1897.

[49] Herbert Burkert: Privacy - Data Protection: A German/European Perspective. 1999 Proceedings of the second symposium Max Planck project group on the law of common goods, available at http://www.coll.mpg.de/sites/www/files/text/burkert.pdf. Retrieved September 25, 2021.

[50] Viktor Mayer-Schönberger: Generational development of data protection in Europe in: Philip E. Agre – Marc Rotenberg (eds.): Technology and privacy – the new landscape. Massachusetts Institute of Technology Press 1998, pp. 219-241.

[51] Census ruling of the German Federal Constitutional Court dated December 15, 1983, available at https://openjur.de/u/268440.html. Retrieved September 25, 2021.

[52] Details on the concept of informational self-determination are provided by Wilhelm Steinmüller: Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann. Recht der Datenverarbeitung 2007, pp. 158–161.

protection norms.[53] The UK passed its data protection law in 1984, and Italy and Greece waited for the corresponding EU directive, thus avoiding the need to (re-)shape their national laws accordingly.[54] The fourth generation of data protection laws, among other things, abandoned the idea that only automated data processing requires protection[55] and introduced more detailed rules, for example for sensitive data,[56] and sector-specific regulations, for example for credit-reporting agencies.[57] The mid-nineties were the starting point of a new law regime with regards to data protection for the European Union: The Data Protection Directive[58] was created in 1995 and introduced new terms like sensitive personal data and consent. In 2002, the EU adopted a Directive on Privacy and Electronic Communication,[59] and in 2009, the EU established an electronic communications regulation[60] in response to the fact that individuals' contact details such as email addresses and mobile numbers became a prime currency in conducting marketing and sales.[61] The EU also brought forward a Directive on Data Retention[62] in 2006, however, this directive was declared invalid by the European Court of Justice in 2014 for violating fundamental rights. In the year 2014, the CJEU delivered another significant ruling:[63] the so-called Google Spain decision was about the possibility to demand that a search engine operator removes certain query results, a decision that was often quoted[64] as the right to be forgotten. Finally, after years of intensive

[53] Background information on the so-called third generation of data protection laws can be found in: Helmut Bäumler, Albert von Mutius: Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts, Luchterhand Publishing 1999.

[54] Herbert Burkert: Privacy - Data Protection: A German/European Perspective, 1999 Proceedings of the second symposium Max Planck project group on the law of common goods, available at http://www.coll.mpg.de/sites/www/files/text/burkert.pdf. Retrieved September 25, 2021.

[55] Viktor Mayer-Schönberger, Ernst Brandl, Hans Kristoferitsch: Datenschutzgesetz. Linde Publishing 2014, p. 6.

[56] For instance, former § 3 (9) of the German Federal Data Protection Law which dealt with "special personal data" such as data about ethnic origin, political belief, health, etc.

[57] For example, former § 28 b of the German Federal Data Protection Law explicitly dealt with scoring; former § 30a of the German Federal Data Protection Law dealt with market and opinion research.

[58] The Data Protection Directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046. Retrieved September 25, 2021.

[59] Directive 2002/58/EC of the European Parliament and of the Council of July 12 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058. Retrieved September 25, 2021.

[60] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services is available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140. Retrieved September 25, 2021.

[61] International Network of Privacy Professionals: A brief history of data protection: how did it all start? Blog news published June 1 2018, available at https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/. Retrieved September 25, 2021.

[62] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Retrieved September 25, 2021.

[63] The court's decision in case C-131/12 from May 13, 2014 is available at http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN. Retrieved September 25, 2021.

[64] Quoted and criticized, see Ignacio Cofone: Google v. Spain: a right to be forgotten? Chicago-Kent Journal of International and Comparative Law 2015, vol. 15, no. 1, pp. 1-11.

discussions, the General Data Protection Regulation was approved in 2016. The Internet, the growing digitalization, new techniques and (social media) platforms as well as the increasing trans-border nature of data processing made data protection more and more an international topic, which led to an increased interest in the possibility of regulating data protection at an international level.[65] Given the overall dynamics of the topic, the evolution of data protection rules cannot be considered completed.

2.3. Emergence of Big Data, Automated Decision-Making, and Artificial Intelligence

Big Data and AI both represent the search for knowledge, and they are founded on a variety of disciplines such as logic, mathematics, and statistics: logic is the foundation for understanding parameters, mathematical thinking is critical for the explanation of input and outputs, and statistics allow for interpretation and evaluation through analysis. The evolution of Big Data and AI clearly goes hand in hand with the development of computer science: obviously, the speed of processing and cost efficiency of the needed infrastructure play an important role for the development of Big Data and AI. Notwithstanding quantum leaps in the area of Artificial Intelligence in the last decade, the first concept of Machine Learning dates back to the eighteenth century when Bayes developed a framework for reasoning about the probability of events known as the Bayesian inference; in the nineteenth century, Boole worked on logical reasoning, and in 1914, the first chess-playing machine that operated without human intervention was invented.[66] The starting point of data processing was perhaps the year 1889 when the first system which could read holes punched into paper cards was introduced.[67] As regards Big Data applications, the first approaches to modern[68] Big Data analysis[69] are probably almost one hundred years old: In 1927 an Austrian-German engineer developed a means of storing information magnetically on tape,[70] and the German "Schutzgemeinschaft für Absatzfinanzierung"[71] based its decisions on a system for assessing payment behavior,[72] which became the foundation for Germany's first credit

[65] Christopher Kuner: The European Union and the search for an international data protection framework, Groningen Journal of International Law 2014, vol. 2, pp. 55-71.

[66] Gil Press: A very short history of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/. Retrieved September 25, 2021.

[67] The reason for the invention was that the previous U.S. census took years due to manual processes. Details on the "Hollerith Machine" are provided by the U.S. Census Bureau, available at https://www.census.gov/history/www/innovations/technology/the_hollerith_tabulator.html. Retrieved September 25, 2021.

[68] In contrast to accounting and the like, which was of course practiced for much longer.

[69] Not to be mixed up with the first attempts for statistical data analysis, which date back to the seventeenth century, see https://datafloq.com/read/big-data-history/239. Retrieved September 25, 2021.

[70] Keith Foote: A brief history of Big Data. Article published December 14 2017, available at https://www.dataversity.net/brief-history-big-data/. Retrieved September 25, 2021.

[71] The term can be translated as "(Protective) Association for Sales Financing".

[72] Background information is provided on SCHUFA's website, available at https://www.schufa.de/de/ueber-uns/unternehmen/geschichte-schufa/. Retrieved September 25, 2021.

agency,[73] an important use case for Big Data analytics and scoring in the financial sector.[74] The first major data project had been created in 1937 and was ordered by the Roosevelt administration in the US, because, after the Social Security Act was enacted, the government had to keep track of data of millions of employees.[75] In 1941, the world's first fully automatic, general-purpose digital computer Z3 became operational; his inventor is nowadays considered a pioneer of computer science,[76] but given the overall circumstances of the 1940s and World War II, the potential of his work was not recognized and remained largely unnoticed.[77] The 1940s saw several groundbreaking publications in the field of Artificial Intelligence: McCulloch and Pitts 1943 article "A Logical Calculus of the Ideas Immanent in Nervous Activity" that become the inspiration for neural networks, Berkeley's 1949 publication "Giant Brains Or Machines That Think" about machines that can handle information with speed and skill similar to what a brain would be if it were made of hardware and wire instead of flesh and nerves,[78] and in 1950, Turing published his famous essay "Computing Machinery and Intelligence".[79] However, at that time, Turing did not have the resources needed to translate his vision into action.[80] Not only technological progress, but political and strategic factors were reasons for the further development of computers: during World War II, the UK was intensively working to crack Nazi codes and they developed a machine called Colossus[81] which scanned for patterns in encrypted messages. Shortly after World War II, the National Security Agency was founded in the US, and they were also assigned the task of decrypting messages.[82] Many consider the 1956 Dartmouth summer research project the birth of the field of Artificial Intelligence where essential ideas behind AI have been investigated, i.e. ways in which

[73] Foundation of the federal SCHUFA-System in order to cover the whole federal territory and not only the surroundings of big German cities, see: https://www.schufa.de/de/ueber-uns/unternehmen/geschichte-schufa/ for further details. Retrieved September 25, 2021.

[74] Stefanie Eschholz, Jonathan Djabbarpour: Big Data und Scoring in der Finanzbranche, ABIDA dossier published January 2015, available at http://www.abida.de/sites/default/files/06%20Scoring.pdf. Retrieved September 25, 2021.

[75] Background information on punch cards that are used for processing is provided by the Smithsonian Institute at their website, available at https://www.si.edu/spotlight/punch-cards/punch-cards-data-processing. In this context, IBM played an important role, see https://www.ibm.com/ibm/history/ibm100/us/en/icons/punchcard/transform/. Retrieved September 25, 2021.

[76] The German engineer Konrad Zuse is often regarded as the inventor of the modern computer, see the newspaper report in Süddeutsche Zeitung published September 20 2016, available at https://www.sueddeutsche.de/digital/ausstellung-computer-pionier-konrad-zuse-seiner-zeit-voraus-1.3168630.

[77] The same is true for other pioneers, see https://famous-mathematicians.org/john-von-neumann/, an online information service about pioneer mathematicians. Retrieved September 25, 2021.

[78] Gil Press: A very short history of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/. Retrieved September 25, 2021.

[79] Alan Turing's famous essay "Computing Machinery and Intelligence" is available at https://www.csee.umbc.edu/courses/471/papers/turing.pdf. Retrieved September 25, 2021.

[80] Stanford University: One-hundred-year study on Artificial Intelligence (AI100). Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/AI100Report_MT_10.pdf. Retrieved September 25, 2021.

[81] Gregg Keizer: WWII's Colossus computer cracks codes once again. Article published November 15 2007, available at https://www.computerworld.com/article/2540136/wwii-s-colossus-computer-cracks-codes-once-again.html. Retrieved September 25, 2021.

[82] Keith Foote: A brief history of Big Data. Article published December 14 2017, available at https://www.dataversity.net/brief-history-big-data/. Retrieved September 25, 2021.

machines could be made to simulate aspects of intelligence.[83] Apart from McCarthy, many other scientists researched on the concept of engineering machines to independently execute commands in the 1950s, e.g., Samuel who coined the term “Machine Learning”; Rosenblatt who developed an early artificial neural network called “Perceptron”, or Simon and Newell who worked on one of the first AI programs called the “Logic Theorist”.[84] Computers of this time reached a point where they could operate independently and collect and process data automatically.[85] In 1950, Claude Shannon built a small remote-controlled robotic mouse called “Theseus” that could navigate within a labyrinth,[86] and in 1961, the first industrial robots[87] have been introduced.[88] In 1965, Feigenbaum and colleagues engaged in building the first knowledge repository tailored for specialized domains called “DENDRAL”, which is considered the first expert system since it automated the decision-making process and problem-solving behavior of organic chemists.[89] Also in the mid-1960s „ELIZA”, an interactive program that was capable of dialogue was developed,[90] and in the following years, further progress was made in the area of Robotics, for example with the development of the famous robots named “Shakey”[91] and “Freddy”.[92] The 1970s were the era of the personal computing revolution: the first personal computers with floppy-drives as key components emerged: in this regard, many think of IBM or Microsoft, but the first personal computers have been introduced by other companies and came as kits, e.g., the MITS Altair 8800 or the

[83] Stanford University: One-hundred-year study on on Artificial Intelligence (AI100). Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/AI100Report_MT_10.pdf. Retrieved September 25, 2021.

[84] Gil Press: A very short history of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/.

[85] Stanford University: One-hundred-year study on on Artificial Intelligence (AI100). Report published 2016, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 25, 2021.

[86] Daniel Klein: Mighty mouse. Article published December 19 2018, available at https://web.archive.org/web/20220125004420/https://www.technologyreview.com/2018/12/19/138508/mighty-mouse/. Retrieved January 10, 2023.

[87] “Robot” is derived from the word "rabota" which means work in Russian. The term was coined by Czech writer Karel Capek in his 1921 play "Rossum's Universal Robots”, which is available at the Internet Archive: https://archive.org/details/CapekRUR. Retrieved September 25, 2021.

[88] The first industrial robot called “Unimate” was used in the assembly line at a General Motors plant. Background information is provided by the Robot Hall of Fame, available at http://www.robothalloffame.org/inductees/03inductees/unimate.html. Retrieved September 25, 2021.

[89] Background information on DENDRAL and the work of Feigenbaum, Lederberg, Buchanan and Djerassi is available at Stanford University’s online library, available at https://exhibits.stanford.edu/feigenbaum/catalog?f%5Bauthor_other_facet%5D%5B%5D=DENDRAL. Retrieved September 25, 2021.

[90] Oliver Miller: A conversation with ELIZA, the electronic therapist. Article published August 1 2012, available at https://thoughtcatalog.com/oliver-miller/2012/08/a-conversation-with-eliza/. Retrieved September 25, 2021.

[91] “Shakey” was equipped with locomotion, perception and problem solving, see Gil Press: A very short history of Artificial Intelligence. Article published December 30 2016, available at https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/. Retrieved September 25, 2021.

[92] “Freddy” was one of the first general-purpose mobile robots to be able to reason about its own actions. Background information on Freddy is provided by the University of Edinburgh, School of Informatics on their website that deals with Artificial Intelligence at Edinburgh University, which is available at https://www.inf.ed.ac.uk/about/AIhistory.html. Retrieved September 25, 2021.

IMSAI 8080.[93] Despite promising ideas and approaches in previous decades, the era of the 1980s showed that there are gaps between theory and practice which resulted in little significant practical successes and lesser interest in terms of research and funding,[94] so that some describe this time as the winter of Artificial Intelligence.[95] However, another novelty paved the path forward: in 1989, the World Wide Web was invented,[96] and the 1990s saw major advancements in all relevant areas of AI, from reasoning and scheduling over data mining and natural language processing to gaming and visual reality, mainly because fundamental limits of computer storage yielded to new hardware innovations.[97] As of the mid-90s, a remarkable (exponential) growth of computing performance took place,[98] and performance and storage power as well as rate at which data is growing are key factors for Big Data, and this rate does not seem to slow down as more and more individuals[99] as well as devices[100] are interconnected. In the following years, AI applications became more sophisticated: in 2010, an early deep learning system called AlexNet, a neural network with many layers, was able to recognize images of objects near human-level,[101] and by now, image recognition capabilities of AI systems have developed very rapidly – moving from image recognition to image generation,[102] and the same is true for language generation capabilities of AI:[103] Language capabilities of AI are so advanced that AI even wrote a law for the regulation of AI regulation.[104] In late 2022 OpenAI released "ChatGPT", a language model for dialogue the company

[93] Daniel Knight: Personal computer history from 1975 to 1984. Article published June 26 2014, available at https://lowendmac.com/2014/personal-computer-history-the-first-25-years/. Retrieved September 25, 2021.

[94] Except for the Japanese government that invested millions in AI in a project aimed at improving Artificial Intelligence from 1982 to 1990, see Catherine Gallagher: 25 stunning advances in Artificial Intelligence. Article published June 23 2019, available at https://stacker.com/stories/3336/25-stunning-advances-artificial-intelligence. Retrieved September 25, 2021.

[95] Daniel Fagella: Will there be another Artificial Intelligence Winter? Article published January 2 2019, available at https://emerj.com/ai-executive-guides/will-there-be-another-artificial-intelligence-winter-probably-not/. Retrieved September 25, 2021.

[96] Details on the World Wide Web are provided by the World Wide Web Foundation, available at https://webfoundation.org/about/vision/history-of-the-web/. Retrieved September 25, 2021.

[97] Catherine Gallagher: 25 stunning advances in Artificial Intelligence. Article published June 23 2019, available at https://stacker.com/stories/3336/25-stunning-advances-artificial-intelligence. Retrieved September 25, 2021.

[98] Pawel Sysiak: Exponential growth of computing. Article published March 21 2016, available at https://medium.com/ai-revolution/exponential-growth-of-computing-a836fce8b907. Retrieved September 25, 2021.

[99] A phenomenon arising from social media platforms like Facebook, Instagram and the like.

[100] A concept that describes the idea of everyday physical objects being connected to the Internet and being able to identify themselves to other devices, see https://www.techopedia.com/definition/28247/internet-of-things-iot. Retrieved September 25, 2021.

[101] Max Roser: The brief history of artificial intelligence: The world has changed fast – what might be next? Article published December 6 2022, available at https://ourworldindata.org/brief-history-of-ai. Retrieved January 10, 2023.

[102] For example, free AI Art generators, see https://aiseo.ai/products/ai-image-generator.html. Retrieved January 10, 2023.

[103] Background information is provided by Jonathan Vanian: Why tech insiders are so excited about ChatGPT, a chatbot that answers questions and writes essays. Article published December 13 2022, available at https://www.cnbc.com/2022/12/13/chatgpt-is-a-new-ai-chatbot-that-can-answer-questions-and-write-essays.html. Retrieved January 10, 2023.

[104] Kate Sandaliz, Julie Tsirkin: AI wrote a bill to regulate AI. Now Rep. Ted Lieu wants Congress to pass it. Article published January 26 2023, available at https://www.nbcnews.com/politics/congress/ted-lieu-artificial-intelligence-bill-congress-chatgpt-rcna67752. Retrieved January 29, 2023.

considers to be the most advanced AI chabot.[105] ChatGPT has recently been extended to control robots based on speech, whicih eliminates the need for programming skills.[106] While the tool amazed the general public, others claim that ChatGPT is "nothing revolutionary,"[107] and some stress the risk this AI may involve due to its potential for harm – from simple cheating at school or college, disclosure of company-internal or personal information[108] to misinformation on a large scale because the program can convincingly mix false information between correct information.[109] The developments in this area shall be closely monitored since ChatGPT could become the first example of an AI application whose developers promptly reacted to the criticism in the context of potential harms as they introduced AI classifier, a software with the ability to identify AI generated text, however, with little success because the recognition rate at present is only as low as 26 %.[110] In 2019, the world's first integrated Quantum Computing system for commercial use[111] was introduced, and one of the special things about Quantum Computing[112] is that, despite the fact that the idea behind Quantum Computing is not new,[113] we are only now in the position to develop computers which are able to increase computational power far beyond what is achievable by conventional computers. Quantum Computers would be able to exponentially speed up the rate of Machine Learning operations and that is why the further development of Quantum Computing is followed with great interest, including from a cybersecurity preparedness

[105] OpenAI released ChatGPT on November 30, 2022. Background information on ChatGPT is provided on the company's website, available at https://chatgpt.pro/. Retrieved January 29, 2023.

[106] Andreas Donath: ChatGPT in der Robotik soll Sprachsteuerung ermöglichen. Article published February 22 2023, available at https://www.golem.de/news/kuenstliche-intelligenz-chatgpt-in-der-robotik-soll-sprachsteuerung-ermoeglichen-2302-172080.html?utm_source=nl.2023-02-22.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter. Retrieved February 22, 2023.

[107] Tiernan Ray quotes the opinion of Meta's chief AI scientist, Yann LeCun in his article: The public perceives OpenAI's ChatGPT as revolutionary, but the same techniques are being used and the same kind of work is going on at many research labs, says the deep learning pioneer. Article published January 23 2023, available at https://www.zdnet.com/article/chatgpt-is-not-particularly-innovative-and-nothing-revolutionary-says-metas-chief-ai-scientist/. Retrieved January 29, 2023.

[108] Christiane Schulzki-Haddouti: Wenn der stochastische Papagei sich verplappert. Article published February 28 2023, available at https://www.golem.de/news/chatgpt-und-datenschutz-wenn-der-stochastische-papagei-sich-verplappert-2302-172227.html?utm_source=nl.2023-02-28.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter**.** Retrieved February 28, 2023.

[109] Ingo Pakalski: OpenAI veröffentlicht Tool zur Erkennung von KI-Texten. Article published February 1 2023, available at https://www.golem.de/news/ai-classifier-chatgpt-erfinder-wollen-texte-von-maschinen-erkennen-2302-171582.html?utm_source=nl.2023-02-01.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter. Retrieved February 5, 2023.

[110] Fionna Agomuoh: ChatGPT has a new way to detect its own plagiarism. Article published February 1 2023, available at https://www.digitaltrends.com/computing/chatgpt-new-way-to-detect-plagiarism/. Retrieved February 5, 2023.

[111] Background information on "IBM's Q System One", the "world's first integrated Quantum Computing system for commercial use" is provided on IBM's website, available at https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use. Retrieved September 25, 2021.

[112] Characteristics and differences of Quantum Computers are summarized by Varun Kumar: 22 Most Interesting Facts About Quantum Computers. Article published January 2 2023, available at https://www.rankred.com/interesting-facts-about-quantum-computers/. Retrieved January 22, 2022.

[113] Theoretical foundations of this technology were already discussed in the mid-70s, e.g., by Roman Ingarden: Quantum Information Theory. Reports on Mathematical Physics 1976, vol. 10, issue 1, pp. 43-72.

perspective.[114] Research has pushed so far as to store information in DNA:[115] "DNA molecules can store up to 215 petabytes, or 215 million gigabytes, of data in a single doubled stranded molecule, making it one of the highest storage density mediums in the world (… which is much more) than we can currently create, so there has been a lot of focus in trying to harness the power and data storage capabilities of DNA for our (…) data storage systems."[116] Scientists are even working on "Organoid Intelligence" by creating AI that uses real human cell brains.[117] While AI may help to solve challenges in science and reshape medicine,[118] it may also be used to keep the world under watch.[119]

This chapter elaborated on the history of the right to privacy, it explained that the first data protection laws have already been enacted more than fifty years ago, and illustrated relevant legislative developments in recent decades in in Europe and in the U.S. Even though there is no comprehensive federal data protection law in the U.S.A., Fair Information Practice Principles have been formulated and implemented in sector-specific laws such as the 1998 Children's Online Privacy Protection Act or the 1996 Health Insurance Portability and Accountability Act, which are laws that are still in force today. This chapter furthermore dealt with the emergence of Artificial Intelligence whose foundations date back to the 1950s when first attempts have been made to create machines that could simulate aspects of intelligence. As of the 1990s, the substantial growth of computing performance paved the way for Big Data and AI as we know it today, resulting in both, fascinating technology such as Quantum Computing or frightening types of Artificial Intelligence such as Deep Fakes.

3. Definitions

This chapter deals with definitions of relevant legal terms. The examination of the legal terminology is essential because the definition of legal terms is decisive for the scope and applicability of laws. The challenge already starts with the broad definition of the term personal information which tempts some to speak of data protection law as the law of everything. Since terms like pseudonymous and anonymous

[114] Alexander Berengaut, Jayne Ponder, Jorge Ortiz: President Biden signs Quantum Computing Cybersecurity Preparedness Act. Article published January 10 2023, available at https://www.insidetechmedia.com/2023/01/10/president-biden-signs-quantum-computing-cybersecurity-preparedness-act/. Retrieved January 10, 2023.

[115] Deoxyribonucleic acid (abbreviated DNA) is the molecule that carries genetic information for the development and functioning of an organism, see: National Human Genome Research Institute, available at https://www.genome.gov/genetics-glossary/Deoxyribonucleic-Acid. Retrieved October 2, 2021.

[116] Liam Critchey: Storing information and data with DNA. Article published August 11 2020, available at https://www.electropages.com/blog/2020/08/storing-information-and-data-dna. Retrieved October 2, 2021.

[117] Hannah Docter-Loeb: Scientists now want to create AI using real human brain cells. Article published February 28 2023, available at https://www.vice.com/en/article/qjkgap/scientists-now-want-to-create-ai-using-real-human-brain-cells. Retrieved February 28, 2023.

[118] Pranav Rajpurkar, Emma Chen, Oishi Banerjee, Eric Topol: AI in health and medicine. Article published January 20 2022, available at https://www.nature.com/articles/s41591-021-01614-0. Retrieved January 10, 2023.

[119] A report from the National Endowment for Democracy: The global struggle over AI surveillance. Report published June 2022, available at https://www.ned.org/global-struggle-over-ai-surveillance-emerging-trends-democratic-responses/. Retrieved January 10, 2023.

data, consent as well as profiling, automated decision-making or scoring are part of the existing legal framework, the regulation of novel technologies may not be in its infancy as some claim, meaning that existing data protection laws address Big Data, ADM, and AI. This section furthermore illustrates the discussion around the terms data protection and privacy, which are often used interchangeably. The debate is highly valuable to examine the question what data protection and data privacy protect and to determine whether present definitions are future-proof. The chapter concludes with challenges of legal terminology, including interpretation, and translation issues as well as background on the terms risk and harm which are important for the legal approach: rights-based, risk-based, or control-based.

3.1. Definition of privacy

As opposed to the "protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data",[120] there is no appearance of the term privacy in GDPR. It is hence unclear what exactly is meant by privacy, so to speak the essence of what is to be protected: is data protection a subset, an expression of the right to privacy, or does it provide additional protection?[121] Existing legal bases are not helpful: the term privacy appears frequently, e.g., in the United Nations Universal Declaration of Human Rights[122] or the OECD Privacy Guidelines as well as various other resolutions and guidelines at international level. Other norms operate with terms such as private and family life,[123] but there is no universal definition or privacy. Current legislation does not offer a conclusive definition of the term privacy or private data; data protection is thus rather achieved through the regulation of the conditions under which personal data may be processed.[124] If privacy is about the right to keep personal matters and relationships secret[125] and being apart from company or observation,[126] then privacy is about separating private from public life. Given that this depends on the era, the degree of technical development as well as the social and cultural environment of the individual, it is comprehensible that the concrete idea of privacy differs and develops, and the notion of privacy as we know it has only emerged in the past 150 years.[127] Perhaps a suitable and catchy definition of privacy

[120] See GDPR Article 1 (2).

[121] Juliane Kokott and Christoph Sobotta examine this question: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law 2013, vol. 3, Issue 4, pp. 222–228, available at https://academic.oup.com/idpl/article/3/4/222/727206. Retrieved September 26, 2021.

[122] See GDPR Article 12.

[123] Article 8 of the European Convention on Human Rights.

[124] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law, Computers and Technology 2009, vol. 23, no. 1, p. 13.

[125] Cambridge Dictionary definition, available at https://dictionary.cambridge.org/de/worterbuch/englisch/privacy. Retrieved September 26, 2021.

[126] Merriam-Webster definition, available at https://www.merriam-webster.com/dictionary/privacy. Retrieved September 26, 2021.

[127] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved September 26, 2021.

would be “control over knowledge about oneself”,[128] but the problem is that data subjects do not exercise control as the so-called privacy paradox shows, and moreover, it is quite often not possible to predict in advance which personal information will be claimed as private, since such claims are made on an ex post facto basis and also depend on contextual factors.[129] Social media is a good example for the shift of private life to public as, some years ago, it would have been unimaginable to share so many private details with so many people. The unanimity with which the claim for privacy is represented stands in contrast to the diversity of answers to the question of which value(s) should actually be protected.[130] In this regard, some pursue the idea of data ownership, others stress informational self-determination or emphasize defense against surveillance or the instrumental character of data protection as risk prevention, while others are primarily concerned with combating power asymmetries between organizations (state, companies, service providers) and individuals (citizens, customers, patients, clients).[131] Numerous attempts to define privacy failed because the definitions were too narrow or too broad or because they focused on certain aspects, but some authors developed characteristics of privacy such as the right to be let alone, the control of personal information, limited access to the self, as well as secrecy and intimacy.[132] Others discussed levels that affect privacy such as the political, the socio-cultural and the personal level:[133] they defined the right to privacy as the right of individuals to determine for themselves when, how, and to what extent information about themselves is communicated to others, including when such information will be obtained and what uses will be made of it by others. Some bills[134] identify privacy as a fundamental right – and “an essential element of freedom”, meaning that individuals’ freedom is core of the legislative intent. Moreover, technology must be taken into consideration as well to grant protection not only by the state or authorities, but also by businesses which process personal data: GDPR embraces this idea by setting standards for data protection by design and

[128] Charles Fried: Privacy. Yale Law Journal 1968, vol. 77, p. 482, available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5894&context=ylj. Retrieved September 26, 2021.

[129] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law. Computers and Technology 2009, vol. 23, no. 1, p. 22.

[130] Rainer Stentzel: Das Grundrecht auf ...? Auf der Suche nach dem Schutzgut des Datenschutzes in der Europäischen Union, Privacy in Germany, issue 5, pp. 185-191, available at https://www.pingdigital.de/ce/das-grundrecht-auf/detail.html. Retrieved September 26, 2021.

[131] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved September 26, 2021.

[132] Daniel Solove: Conceptualizing Privacy. California Law Review 2005, vol. 90, no. 4, pp. 1132-1140, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview. Retrieved September 26, 2021.

[133] Alan Westin: Social and political dimensions of privacy. Journal of Social Issues 2003, vol. 59, no. 2, pp. 431-434, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.4866&rep=rep1&type=pdf. Retrieved September 26, 2021.

[134] For example, New York’s new privacy bill which defines privacy as a fundamental right and essential element of freedom. The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S00365&term=2023&Summary=Y&Actions=Y&Text=Y. Retrieved January 7, 2023.

by default in GDPR Article[135] 25. Perhaps a contemporary definition of privacy is the absence of harmful use[136] with regards to the individuals concerned with the data processing – an idea that is consistent with the Regulation's risk-oriented approach and the fact that the production, collection, and use of data is growing at fast pace, which is why some declare the regulation of data collection to be a losing battle.[137] The difference between privacy and data protection needs to be clarified, because these terms cannot be considered identical even though they are quite often used interchangeably. The terms can have different meanings depending on context, industry, or jurisdiction: There are two systems which ensure the protection of fundamental human rights in Europe, the European Convention on Human Rights (Convention) and the Charter of Fundamental Rights of the European Union (Charter). The protection of personal data and privacy are closely linked in the jurisprudence of both, the European Court of Human Rights (ECtHR)[138] and the Court of Justice of the European Union (CJEU), but their personal and substantive scopes diverge:[139] Article 8 of the Convention and Article 7 of the Charter stipulate that everyone has the right to respect for private and family life, home and communications, and Article 8 of the Charter specifically deals with protection of personal data. This shows that privacy and data protection are not the same. The General Data Protection Regulation is, as the name says, about data protection, and given the numerous duties processors must implement,[140] one may say that data protection is about a (management) system of data processing practices for the protection of privacy, meaning that companies ensure protection whereas individuals ensure privacy by controls to which they are entitled as data subjects. Privacy includes private and family life, home and correspondence. It is a recognized fundamental human right and as such addresses the state and its bodies; data protection addresses the state[141] as well as companies and, depending on the case, even individuals as they may also be controllers or processors.[142]

3.2. Definition of Artificial Intelligence

Big Data is based on algorithms, and algorithms are best described as step-by-step procedures for the calculation, evaluation and automated reasoning as well as decision-making which are based on data

[135] Unless otherwise specified, Article always refers to GDPR articles.
[136] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law. Computers and Technology 2009, vol. 23, no. 1, p. 23.
[137] Karen McCullagh: Protecting privacy through control of personal data processing – a flawed approach, International Review of Law. Computers and Technology 2009, vol. 23, no. 1, p.22.
[138] The final arbitrator on the Convention.
[139] Juliane Kokott, Christoph Sobotta: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law 2013, vol. 3, issue 4, pp. 222–228, available at https://academic.oup.com/idpl/article/3/4/222/727206. Retrieved September 26, 2021.
[140] Winfried Veil: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs. Zeitschrift für Datenschutz 2018, vol. 1, pp. 9-16, available at https://rsw.beck.de/rsw/upload/ZD/ZD_01-2018_-_Beitrag_Veil_1.pdf. Retrieved September 26, 2021.
[141] See GDPR Article 2 (2) which names exceptions.
[142] See GDPR Article 4 (7) and (8): controller or processor means a natural or legal person.

processing.[143] The difference between Artificial Intelligence and former Big Data analytics is that AI programs do not rely on a linear data analysis; instead they learn from the data which allows them to respond intelligently and to adapt their outputs accordingly.[144] A prominent definition of AI is that Artificial Intelligence is the "activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment"[145]. John McCarthy who is believed to be the father of AI coined the term Artificial Intelligence as "the science and engineering of making intelligent machines."[146] Others define AI as a "set of techniques that seek to approximate cognitive tasks" or as "systems that act rationally to achieve goals via perception, planning, reasoning, communicating, decision making and acting."[147] Other definitions distinguish general and narrow Artificial Intelligence, the latter refers to AI systems "that addresses specific application areas such as playing strategic games, language translation, self-driving vehicles and image recognition", whereas general AI means "a notional future artificial intelligence system that exhibits apparently intelligent behavior at least as advanced as a person across the range of cognitive, emotional, and social behaviors."[148] Big Data, Artificial Intelligence and so-called Machine Learning are often used interchangeably, but there are important differences: Big Data is about innovative forms of high-volume, high-velocity and high-variety information processing which is cost-effective and enables enhanced insight and decision making.[149] Artificial Intelligence refers to systems which perceive their environment and which are able to perform various tasks with some degree of autonomy to achieve specific goals.[150] Apart from autonomy, another important characteristic of AI is the adaptiveness of the technology.[151] There is no single or generally accepted definition of AI, but the term Artificial Intelligence is used to describe computer systems that are able to learn from own experiences and solve

[143] European Union Agency for Fundamental Rights: Handbook on European Data Protection Law 2018, p. 351, available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law. Retrieved September 26, 2021.

[144] ICO: Big Data, Artificial Intelligence, Machine Learning and data protection 2017, p. 6, available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Retrieved September 26, 2021.

[145] Nils Nilsson, The Quest for Artificial Intelligence: A History of Ideas and Achievements, Cambridge University Press 2010.

[146] Andy Peart: Homage to John McCarthy, the father of Artificial Intelligence. Article published October 29 2020, available at https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence. Retrieved September 26, 2021.

[147] Valerie Thomas: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved September 26, 2021.

[148] For instance, section 3 of H.R.4625 of the Future of Artificial Intelligence Act of 2017, available at https://www.congress.gov/bill/115th-congress/house-bill/4625/titles. Retrieved September 26, 2021.

[149] Definition of Big Data provided by the Gartner IT glossary, available at http://www.gartner.com/it-glossary/big-dataA. Retrieved September 26, 2021.

[150] European Commission's factsheet on Artificial Intelligence, published July 4 2019, available at https://digital-strategy.ec.europa.eu/en/library/factsheet-artificial-intelligence-europe. Retrieved September 26, 2021.

[151] Marcus Evans, Anj Merchant: UK AI – UK consults on non-statutory cross-sectoral guidance principles for regulating AI – final approach still some way off. Article published July 27 2022, available at https://www.insidetechlaw.com/blog/uk-consults-on-non-statutory-cross-sectoral-guidance-principles-for-regulating-ai. Retrieved July 30, 2022.

complex problems in different situations.[152] Scientists speak of AI whenever a non-biological system mimics cognitive functions and this way shows behaviors which were thought to be unique to natural persons.[153]

3.3. Definitions of relevant legal terms

Since (changes to) definitions effect the material scope of the regulation as defined in GDPR Article 2, a series of terms has to be examined.[154] The same applies to eventual restrictions which may apply to special categories of data as well as potential limitations that may be applicable to certain methods of data processing, namely automated individual decision-making and profiling. Many of the core definitions under the Data Protection Directive were not changed,[155] whereas GDPR expanded the scope of some terms[156] and added new definitions, for example for profiling. GDPR covers all of the terms explained in the below definitions. However, privacy and artificial intelligence (AI) are not mentioned, but as they are needed to complete the picture of Big Data, this section will also explain what is meant by privacy and how AI and underlying algorithms shall be interpreted.

3.3.1. Personal data

The Data Protection Directive defined personal data as “any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.[157] There was controversial discussion on whether, e.g., IP addresses fall within this definition of personal data.[158] GDPR Article 4 (1) states that, “for the purposes of this regulation, personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

[152] Norwegian Data Protection Authority: Artificial intelligence and Privacy 2018, p. 5, available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf. Retrieved September 26, 2021.

[153] FRA’s Handbook on European Data Protection Law 2018, p. 351, available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law. Retrieved September 26, 2021.

[154] As regards the relationship between GDPR’s Articles and Recitals, the 2015 “Joint practical guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation” makes it clear that Recitals are drafted in such a way that their non-binding character becomes clear. The guide is retrieved from https://publications.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732. Retrieved September 25, 2021.

[155] For instance, the terms “controller” and “processor”.

[156] Such as personal data and sensitive personal data.

[157] Article 2 (a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[158] See the corresponding judgment on IP-addresses by the European Court of Justice in in Case C-582/14, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0582&from=EL. Retrieved September 25, 2021.

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". GDPR thus contains a broad definition of personal data and makes clear that online identifiers and location data are also considered personal data. As a result, GDPR's material scope is also broader than the scope of the Data Protection Directive.[159] Other laws define personal data differently, e. g. the new California Consumer Privacy Act[160] according to which any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"[161] is considered personal information. Despite obvious similarities, CCPA's definition of personal information is not identical to GDPR's definition of personal data, and it's a good example that terminology can only be the starting point of discussions.[162]

3.3.2. Anonymous data

Unlike pseudonymization,[163] GDPR does not define anonymization. From a data protection perspective, anonymization of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates:[164] data can be considered effectively and sufficiently anonymized if they have been treated in such a manner that the data subject is no longer identifiable.[165] The application of data privacy laws therefore stands and falls with anonymization. Anonymization is moreover valuable from a compliance point of view as it may be considered equal to the deletion of personal data,[166] which is important with regards to data retention and deletion periods. Anonymity is interpreted differently[167] as some refer to so-called computational anonymity, where a data controller (even in collaboration with

[159] The same is true for the territorial scope: the Data Protection Directive only applied to European Union Member States and non-EU members which are a part of the European Economic Area.
[160] The California Consumer Privacy Act (CCPA) was signed into law on June 28 2018, and went into effect on January 1 2020. Background information including a rulemaking fact sheet are available at https://www.oag.ca.gov/privacy/ccpa#:~:text=CCPA%20was%20signed%20into%20law%20on%20June%2028%2C,sale%20of%20personal%20information%20that%20businesses%20collect%2C%20. Retrieved September 25, 2021.
[161] CCPA, Section 1798.140(o)(1).
[162] The examination of relevant definitions will focus on the GDPR because of its broad scope, see GDPR Articles 2 and 3, and because GDPR can be considered a role model law.
[163] GDPR Article 4 (5).
[164] AEPD-EDPS's joint paper on 10 misunderstandings related to anonymization clarifies what shall be considered anonymization, and what not. Paper published April 27 2021, available at https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en. Retrieved February 28, 2023.
[165] Definition provided by the Irish Data Protection Authority, available at https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation. Retrieved September 25, 2021.
[166] The Austrian Data Protection Authority decided correspondingly in their decision dated December 5 2018, which is available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html. Retrieved September 25, 2021.
[167] Detailed background information is provided by the Article 29 Working Party in their 2014 opinion (05/2014) on anonymization techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Retrieved September 25, 2021.

third parties) would have difficulties to directly, or indirectly identify data subjects, while others tend to refer to so-called perfect anonymity where such an endeavor would be impossible. The problem of re-identification is often also described as relative anonymity whose main criterion may be summarized as disproportionality of assignment to a person vs. absolute anonymity whose main criterion may be summarized as the impossibility of assignment to a person.[168] The Data Protection Directive dealt with anonymous data[169] to exclude such data from the scope of data protection legislation, and the same is true for GDPR:[170] Recital 26 (6) is also important for Big Data applications as it makes clear that GDPR "does not concern the processing of (…) anonymous information (…) for statistical or research purposes". This exception for statistical purposes is tempting to businesses but must be matched against the (rather absolute) definition of personal data as set forth in GDPR Article 4 (1). Furthermore, anonymization of data is anything but easy to achieve,[171] many data sets shall therefore rather be classified as pseudonymous data, meaning that it is still possible to single out individuals and / or to link records to them:

3.3.3. Pseudonymous data

GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".[172] As a result, personal data which has been subjected to technological measures to make them pseudonymous shall still be considered personal data[173] as long as information can be attributed[174] to an identifiable person. This definition stresses GDPR's broad scope, which is a fact many may not welcome in view of the implementation effort, however, there is a variety of advantages for businesses when they process pseudonymous data: pseudonymization is explicitly mentioned[175] as an appropriate technique

[168] An overview on the discussion is provided by Nico Härting: DSGVO – gibt es Regelungen für anonyme Daten? Article published May 3 2016, available at https://www.cr-online.de/blog/2016/05/03/dsgvo-gibt-es-regelungen-fuer-anonyme-daten/. Retrieved September 25, 2021.

[169] Recital 26 of Directive 95/46/EC.

[170] GDPR Recital 26.

[171] MIT researchers published a study in December 2018 explaining that anonymous data can be re-identified. The corresponding press release is available at https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized. Retrieved September 25, 2021.

[172] See GDPR Article 4 (5).

[173] The EU General Court determined in Case T-557/20 that pseudonymized data is not inherently considered personal data. Decision published April 16 2023, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=272910&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=641166. Retrieved April 26, 2023.

[174] ICO believes that personal data that has been pseudonymized fall within the scope of the GDPR. depending on how difficult it is to attribute the pseudonym to a particular individual, see ICO's overview of the General Data Protection Regulation, available at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/. Retrieved September 25, 2021.

[175] See GDPR Article 25: Pseudonymization is mentioned as an example of an appropriate technical measure in correspondence with the principles of data protection by design and data protection by default.

for data controllers to comply with GDPR's data protection principles; restrictions to data subjects' rights apply;[176] breach notification requirements may be impacted.[177] What is particularly interesting for Big Data applications is that profiling on the basis of pseudonymous data may be possible[178] without data subjects' consent as processing of such data is unlikely to significantly affect individuals, which is one of the admissibility criteria under GDPR Article 22 (1). As a result, it can be assumed that the GDPR shows strong incentives to employ data pseudonymization technologies.

3.3.4. Special categories of data

GDPR does not address or define all types of personal data that would generally be considered sensitive or worthy of protection. GDPR covers and defines special categories of data such as genetic,[179] biometric[180] or health[181] data and states that, as a basic rule, sensitive personal data must not be processed.[182] In comparison to the Data Protection Directive, the protection of genetic and biometric data is new. As a result, GDPR has a broader definition of so-called sensitive personal data. Moreover, GDPR Article 22 (4) prohibits automated individual decision-making including profiling if it is based on special categories of personal data referred to in GDPR Article 9 (1), so that numerous categories of data[183] are generally not suitable for this type of data processing. If pseudonymous data is a good example for the possibility to conduct Big Data analyses, sensitive data may serve as an example for restrictions in this area.[184] But there are exceptions to this rule as GDPR Article 22 (4) also says that automated individual decision-making including profiling is admissible if it is based on explicit consent or if it is necessary for reasons of substantial public interest.[185]

3.3.5. Processing

GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

[176] GDPR Article 11 (2) affects individuals' rights of access, the right to correct and erase data as well as requests for data portability.
[177] See GDPR Article 34 (3a) .
[178] Subject to a successful assessment of legitimate interests, GDPR Article 4 (1) lit. f.
[179] See GDPR Article 4 (13) and Recital 34.
[180] See GDPR Article 4 (14), for instance, fingerprints, facial recognition, etc.
[181] See GDPR Article 4 (15) and Recital 35.
[182] Unless there is a justification, for example individuals' explicit consent: GDPR Article 9 (2a).
[183] Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; data concerning health; data concerning a natural person's sex life or sexual orientation; biometric data for the purpose of uniquely identifying a natural person: GDPR Article 9 (1).
[184] Moreover, large scale processing of sensitive personal data triggers the need to undertake data protection impact assessments, see GDPR Article 35.
[185] In addition, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be in place.

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[186] If even erasure and deletion of personal data is considered as a data processing activity under the GDPR, these related data processing activities in the life cycle of personal information raise the question of the appropriate legal basis, which underlines that GDPR is about finding the right legal basis: just like the Data Protection Directive, GDPR works with prohibitions that are subject to permission, and the processing of special categories of data is a perfect example in this regard. The definition of processing is also very broad and makes it clear that the applicability of GDPR is not limited to so-called automated processing as handwritten records may also fall under GDPR. While any use of computers, smartphones, cameras, scanners or Internet and e-mail can lead to the applicability of the GDPR if personal data are concerned, non-automated processing of personal data is only covered by the scope of application if the data are (or are to be) stored in a filing system as defined in GDPR Article 4 (6).[187]

3.3.6. Profiling

The Data Protection Directive did not contain a definition of profiling; the GDPR introduced a new definition of profiling: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements".[188] Profiling means massive processing of personal data in order to identify patterns that allow for the automatic categorization of individuals and aims at predictive data mining.[189] Profiling moves away from the use of personal data as we know it, because, instead of collecting personally identifiable data, a digital persona is created which is based on information algorithms created with the help of attributes which are not directly related to individuals.[190] While the probabilistic nature of profiles is desired, their inherent opacity[191]

[186] See GDPR Article 4 (2).

[187] Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

[188] See GDPR Article 4 (4).

[189] Gloria Gonzalez Fuster, Serge Gutwirth, Eriak Ellyne: Profiling in the European Union – a high-risk practice, Inex Policy Brief no. 10, published June 2010, available at https://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf. Retrieved September 25, 2021.

[190] Serge Gutwirth, Paul De Hert: Regulating profiling in a democratic constitutional state, in: Profiling the European citizen, Springer Publishing 2008, p. 300. The article is also available at http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_365_restricted.pdf. Retrieved September 25, 2021.

[191] Tal Zarsky: The Trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making. Article published October 14 2015, available at https://journals.sagepub.com/doi/abs/10.1177/0162243915605575. Retrieved September 25, 2021.

together with their potential for discrimination[192] is considered problematic.[193] An important legal development in this regard is that many countries are coming up with privacy laws of their own[194] and these laws foresee, amongst other things, rules on automated decision making and profiling which are similar to the ones set forth in the GDPR.[195]

3.3.7. Automated decision-making

Even though GDPR combines both topics in the same Article, profiling and automated individual decision-making must be distinguished: Profiling is based on automated processing with the objective to evaluate personal aspects about a natural person, however, only automated decision-making has the ability to make decisions by technological means without human involvement. GDPR stipulates that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[196] Automated decision-making presupposes that there is no human intervention[197] at all, so that mere pre-selection processes (decision support systems) do not fall under the rule.[198] The problem is where to draw the line between (generally admissible) pre-selection and (potentially inadmissible) decision-making: the question is which (interim) results[199] can be considered to have the quality of a decision in the sense of the Regulation, i.e. a decision "which produces legal effects concerning him or her or similarly significantly affects him or her". There is consensus that this question can only be answered on a case-by-case-basis since all circumstances have to be considered, but there are dissenting opinions[200] as to whether or not marketing activities similarly significantly affect data subjects.[201]

[192] This problem was reviewed by the Article 29 Working Party in their 2017 guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, published August 22 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Retrieved September 25, 2021.

[193] And consequently, mentioned in the GDPR, see Recital 71.

[194] For instance, Brazil, see Renato Leite Monteiro: GDPR matchup – Brazil's general data protection law. Article published October 4 2018, available at https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Retrieved September 25, 2021.

[195] For example, Virginia, see Sarah Rippy: Virginia passes the Consumer Data Protection Act. Article published March 3 2021, available at https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/. Retrieved September 25, 2021.

[196] See GDPR Article 22 (1).

[197] To qualify as human intervention, the controller must ensure that the decision is carried out by someone who has the competence to change the decision: Peter Gola: Bundesdatenschutzgesetz 2012, para. 6 a BDSG, note 6.

[198] Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Stiftung Publishing 2018, p. 19.

[199] Any such decision must be the result of automated processing: Spiros Simitis: Bundesdatenschutzgesetz 2006, para. 6 a BDSG, note 26.

[200] Some believe that the economic and practical significance of the decision play a role as well as the sustainability of the impairment, whereas annoying or uncomfortable consequences of an automated decision should not be regarded as a significant impairment: Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Publishing 2018, p. 20.

[201] According to the Commission, sending out advertising material does not have a significant adverse effect on data subjects. However, it should not be overlooked that this view dates to 1992, a time when it was not at all foreseeable what the extent of targeted advertising would be like some years ago: Spiros Simitis: Budesdatenschutzgesetz 2006, para. 6 a, note 24.

Recital[202] 71 names two typical examples of automated individual decision-making: e-recruitment processes and (refusal) of an online credit application, which shows that automated individual decision-making is relevant whenever dynamic (real-time) results are needed.[203] In addition, there are several exceptions[204] to the above rule that individuals have the right not to be subject to a decision based solely on automated processing, e.g., if such processing is based on data subjects' explicit consent, or if the processing is necessary for entering into or performance of a contract between the data subject and a data controller, or if it is allowed by Union or member state law to which the controller is subject.[205] Each of these exceptions is problematic, for the following reasons: consent seems problematic due to factors like lack of transparency and / or information asymmetries and imbalance of powers. As regards the necessity of processing for entering into or performance of a contract between the data subject and a data controller, the problem is that the exception actually applies to scenario which Recital 71 considers a typical use case of the norm, namely credit applications.[206] The permissibility of national rules[207] dilutes GDPR's overall goal to harmonize the legal framework, it increases legal uncertainties caused by the necessary interpretation of national laws in the light of higher-ranking EU law, and it makes compliance more difficult for those controllers who do not merely fall under one jurisdiction. At first sight, the Regulation also foresees for a limit for the admissibility of automated decision-making as GDPR Article 22 (4) prohibits the use of special categories of personal data within the meaning of GDPR Article 9 (1) for automated decision-making. But this does not apply if the data subject has given explicit consent or when processing is necessary for reasons of substantial public interest.[208] GDPR Article 9 (2) names a whole catalogue of exemption clauses, and from an entrepreneurial point of view, it is likely that the following two exceptions will arouse interest: processing of sensitive data is admissible if it relates to personal data which are manifestly made public by the data subject,[209] and processing of special categories of data is admissible if it is "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued (and) respect the essence

[202] Unless otherwise specified, Recital always refers to GDPR Recitals.

[203] For instance in the area of differential pricing, which is considered a significant effect if prohibitively high prices effectively bar someone from certain goods or services: Article 29 Working Party in their 2017 guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Retrieved September 25, 2021.

[204] All of them are, according to Recital 71 "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."

[205] Provided that such a law also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, see GDRP Aarticle 22 (2b).

[206] Stephan Dreyer, Wolfgang Schulz: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Stiftung Publishing 2018, p. 21.

[207] For example, the new German BDSG provides a corresponding exception for insurance contracts in § 37 (1).

[208] Datenschutzkonferenz Kurzpapier Nr. 17, pp. 2 and 3. Paper published March 27 2018, available at https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_17_Besondere-Kategorien.pdf. Retrieved September 25, 2021.

[209] See GDPR Article 9 (2) lit. e.

of the right to data protection".[210] It can therefore be assumed that companies may concentrate on the investigation of and focus on scientific and statistical purposes in connection with Big Data applications and automated decision-making. In any event, in order to perform automated decision-making in a compliant manner, the controller has to implement suitable measures[211] to safeguard data subjects' rights and freedoms and interests and to assess and document[212] the endeavor. Finally, it should be noted that with regard to GDPR Article 22, there is controversy about the ambiguity of the norm, as to whether or not the rule shall be interpreted as a prohibition[213] in the sense that the controller must respect legal limitations, or if it shall be considered an individual right.[214] The difference being that, exercising a right requires action of the data subject, while a prohibition offers protection by default. The latter seems favorable and is supported by the EDPB,[215] because otherwise, automated decisions could perhaps be legitimized based on implicit consent, which does not comply with the idea of consent as a specific, freely given and informed indication of a data subject's choices.[216] Therefore, the concept of consent must be examined as well:

3.3.8. Consent

Consent generally plays an important role in data protection and is frequently used to justify the processing of personal data.[217] Recital 32 describes conditions for consent as set forth in GDPR Article 7: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement". Consequently, Recital 32 explains that inactivity cannot constitute consent; consent can only be given unambiguously. Like the Data Protection Directive, GDPR requires explicit consent for sensitive

[210] See GDPR Article 9 (2) lit. j.

[211] See GDPR Article 22 (4).

[212] See GDPR Article 35 (1, 3, 7).

[213] For instance, Isak Mendoza and Lee Bygrave: The right not to be subject to automated decisions based on profiling. University of Oslo Legal Studies Research Paper Series no. 2017-20, available at https://ssrn.com/abstract=2964855. Retrieved September 25, 2021.

[214] Some authors stress that Article 22 and its predecessors do not prohibit the use of automated individual decisions: Bettina Berendt, Sören Preibusch: Toward accountable discrimination-aware data mining- the importance of keeping the human in the loop. Big Data. 2017, vol. 5, Nr. 2, pp. 135-152, available at https://www.ncbi.nlm.nih.gov/pubmed/28586238. Retrieved September 25, 2021.

[215] Sebastiao Barros Vale, Gabriela Zanfir-Fortuna for the Future of Privacy Forum: Automated decision-making under the GDPR: practical cases from courts and data protection authorities. Report published May 17 2022, available at https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/. Retrieved December 29, 2022.

[216] Even though the authors refer to the Data Protection Directive and not to GDPR, their argument is still valid: Servge Gutwirth, Paul De Hert: Regulating profiling in a democratic constitutional state, in: Profiling the European citizen, Springer Publishing 2010, p. 283, available at http://www.vub.ac.be/LSTS/pub/Dehert/Dehert_365_restricted.pdf. Retrieved September 26, 2021.

[217] In May 2020, the EDPB adopted Guidelines 05/2020 on consent under Regulation 2016/679. The guidelines are available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

personal data,[218] and consent can generally be distinguished by differentiating between explicit and implicit as well as written versus orally given consent[219]. GDPR also brought some changes with regards to consent, beginning with seemingly simple topics like form requirements: GDPR does not insist on a written form requirement; the contrary is true, but Recital 42 makes it clear that there is a burden of proof that consent exists, and that is why controllers have to think about how to best comply with the challenge of demonstrating that the data subject has given consent to the processing operation. The issue of form requirements also led to sector- and scenario-specific variations in national jurisdictions:[220] For example,[221] former § 4a (1) of the German Federal Data Protection Law as a general rule required written form for consent. However, § 13 (2) of the German Tele-Media Act[222] allowed for electronic consent, for example, by clicking a checkbox. In addition, § 26 (2) of the new German Federal Data Protection Law again stipulates the written form in an employment context. Another particularity is that GDPR introduced special conditions applicable to child's consent in relation to information society services.[223] Consent may be an important legal basis when it comes to marketing activities, unless so-called soft opt-in rules apply. The GDPR does not have specific provisions that address marketing activities, but Recital 47 deals with marketing by explaining that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". GDPR is furthermore not silent on various topics that are highly relevant for Big Data, ADM, and AI, e.g., automated decision-making and profiling,[224] admissible re-use of personal information,[225] international data transfers,[226] transparency,[227] data subject rights,[228] data security[229] or requirements that apply to special categories of personal information[230] - all of which might play a role in the context of valid consent as the basis of admissible data processing. Consent is key when the exercise of control over own data is in question, and an

[218] Explicit consent is needed for the processing of special categories of personal data, see GDPR Article 9 (2 a).

[219] However, providing proof or such consent might be challenging, see GDPR Article 7 (1): "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

[220] In comparison (and as a rule), former § 4 a (1) of the German Federal Data Protection Law required written form for consent (with exceptions depending on the circumstances of the individual case). However, § 13 (2) of the German Tele-Media Act allowed for electronic consent, e.g., by clicking a checkbox and the like.

[221] With exceptions depending on the circumstances of the individual case. It is questionable how a deviation from the written form requirement could be argued in the employment environment when in fact employees are either permanently present or can be reached via Intranet, Email, by post. If time pressure was to serve as an argument, this fails due to fact that this way, the voluntary nature of consent is in doubt.

[222] The German Telemedia Act (TMG) will soon to be replaced with the "Telecommunications Telemedia Data Protection Act" (TTDSG). This new law is intended to bundle the parts of the German Telecommunications Act (TKG) and the German Telemedia Act (TMG) that are relevant to data privacy into one central law. Background information on this legal development is provided by the consultancy bITs in their blog "TTDSG passiert Bundesrat – endlich verbindliche Regelungen für Cookies" published June 3 2021, available at https://www.bits.gmbh/ttdsg-passiert-bundesrat-endlich-verbindliche-regelungen-fuer-cookies/. Retrieved September 26, 2021.

[223] See GDPR Article 8 and Recital 38.

[224] See GDPR Article 22.

[225] See GDPR Article 6 (4).

[226] See GDPR Chapter 5.

[227] For example, GDPR Articles 12, 13, 14.

[228] See GDPR Chapter 3.

[229] For example, GDPR Article 32.

[230] See GDPR Article 9.

important condition to exercise control is transparency.[231] That is why a data subject requires all necessary information to make a free decision, and this seems difficult when automated decision-making is applied. Consequently, one of the major issues regarding consent in the framework of automated decision-making, especially when it is based on profiling, is the question whether sufficient information was provided to the data subject: Given the complex matter, even if the data controller fulfills existing transparency requirements and provides the data subject with information concerning the logic involved in making the decision, it remains questionable whether the fulfillment of this legal obligation is enough for the data subject to realize how an automated decision may (and will) affect him.[232] It is difficult to imagine valid consent as consent must be intelligible in order to be specific; clear reference has to be made to the scope and the consequences of the data processing.[233] From a business perspective it must be considered that, for reasons of intellectual property and competitive advantage, functionality and logic of an algorithm are often kept secret and therefore not or only partially disclosed. [234] Moreover, Recital 43 explicitly stresses that “in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller”. This is most probably the case for all Big Tech players such as Meta (formerly known as Facebook)[235] or Google. Recital 43 also underlines that consent is presumed not to be freely given if the performance of a contract or the provision of a service is made conditional on the consent of the data subject to the processing of personal data. Another factual problem arises from the fact that automated decision-making which is based on profiling does not have to cover exclusively the personal data of the data subject that consented to this type of data processing, but that it might also involve personal data of other individuals.[236] Consent can neither cover other people’s personal data not can it be applied in an open-ended set of processing activities. Furthermore, consent can be revoked at any time, and in the framework of automated individual decision-making, additional data subject rights apply.[237] As a result, using consent as legal grounds for data processing is sometimes

[231] Detailed background information is provided by the Article 29 Working Party in their opinion on consent. Paper (15/2011) published July 13 2011, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. Retrieved September 26, 2021.

[232] Laurens Nauds: The right not to be subject to automated decision-making: the role of explicit consent. Article published August 2 2016, available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/. Retrieved September 26, 2021.

[233] The requirements of consent are explained in opinion 15/2011 of the Article 29 Working Party on consent. Paper published July 13 2011, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. Retrieved September 26, 2021.

[234] In Germany, a popular example was the case of SCHUFA, one of the main credit bureaus. The issue was how their score is calculated and displayed. Background information is available at https://www.internet-law.de/2014/02/das-urteil-des-bgh-zum-schufa-scoring-im-volltext.html. Retrieved September 26, 2021.

[235] Salvador Rodriguez: Facebook changes company name to Meta. Article published October 28 2021, available at https://www.cnbc.com/2021/10/28/facebook-changes-company-name-to-meta.html. Retrieved January 22, 2022.

[236] Veleria Ferraris et al: The impact on profiling on fundamental rights. Article published December 22 2013, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753. Retrieved September 26, 2021.

[237] The data subject has the right to contest the decision, to express his or her point of view and to obtain human intervention on the part of the controller, see Laurens Nauds: The right not to be subject to automated decision-making: the role of explicit consent. Article published August 2 2016, available at

much more difficult and much less recommendable than many businesses might assume. However, many companies still opt for consent[238] as they believe this is both, a legally admissible and safe way to obtain legal grounds for the desired data processing.

3.3.9. Other relevant terms including risk and harm

Apart from the above definitions, GDPRs furthermore defines other important terms such as controller, processor, recipient and third party. These terms are important for assigning responsibility: a controller is a natural or legal person (…) which, alone or jointly with others, determines the purposes and means of the processing of the personal data.[239] A processor is a natural or legal person (…) which processes personal data on behalf of the controller.[240] A third party is a natural or legal person (…) other than the data subject, controller, processor or persons who, under the direct authority of the controller or processor are authorized to process personal data.[241] A recipient, on the other hand, is a natural or legal person to which the personal data are disclosed.[242] Joint controllership is given when two or more controllers jointly determine the purposes and means of the processing.[243] Given the complexity of modern data processing activities and the variety of service providers involved, the differentiation needed to identify and distinguish these players is not always easy to accomplish. Due to the fact that Big Data, automated decision making and Artificial Intelligence may involve risk from a data subject perspective, it is important to know what GDPR says about risk: Recital 75 deals with risks to the rights and freedoms of natural persons and explains that "the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic

https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/. Retrieved September 26, 2021.

[238] Nico Härting describes this as consent fetishism during his presentation in the framework of the 2012 annual DSRI academy summit (DSRI Herbstakademie) that was held September 12-15 2012. The presentation is available at https://rsw.beck.de/cms/?toc=ZD.60&docid=338853. Retrieved September 26, 2021.

[239] See GDPR Article 4 (7).

[240] See GDPR Article 4 (8).

[241] See GDPR Article 4 (10).

[242] See GDPR Article 4 (9).

[243] See GDPR Article 26 (1).

situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects." GDPR as such does not define risk, it only provides interpretative guidance on what may constitute risk and lists examples, and the fact that privacy violations may be given without privacy harms[244] and the fact that relevant terms like risk, threat, harm, injury or violation are often used interchangeably or evaluated in a different context (e.g., regulator perspective as opposed to the individual's or court perspective) adds to the problem. Regulators dealt with the issue of informational injuries[245] and various scholars tried to explain risk and provide a typology of privacy harms,[246] e.g., by distinguishing privacy harms as follows: physical, economic, reputational, emotional; due to disturbance, vulnerability, loss of autonomy, control, informed choice or based on thwarted expectations, chilling effects, or discrimination. Another approach was to explain which risks exist in which stages of data processing,[247] starting with information collection: surveillance (e.g., monitoring) and interrogation (e.g., questioning) and during data processing: aggregation (e.g., combining of datasets), identification (e.g., linking of information), secondary use (e.g., using data for other purposes), insecurity (e.g., carelessness in protecting information from leaks), exclusion (e.g., failure to let the individual know about information others have about them) and in the event of information dissemination, where the following risks have been identified: breach of confidentiality (e.g., breaking the promise to keep information confidential), disclosure (e.g., revealing truthful information), distortion (e.g., disseminating false or misleading information about an individual), blackmail (e.g., threatening to disclose information), increased accessibility (e.g., amplifying the accessibility of personal information) and appropriation (e.g., using an individual's identity to serve the aims and interests of another), and finally invasion where intrusion (e.g., disturbing an individual's tranquility) can be distinguished from decisional interference (e.g., interfering with an individual's decision making). One further aspect to consider is that Big Data, ADM and AI do not only involve potential risks for individuals but may also lead to societal harms,[248] e.g., by accelerating growth and prosperity for some, and at the same time leading to significant changes in the employment sector for others or by leading to greater connectivity on the one hand but also greater vulnerability on the other owing to a much larger "cyber-physical attack

[244] Ryan Calo: The boundaries of privacy harm. Indiana Law Journal 2011, vol. 86, no. 3.

[245] Maureen Ohlhausen for the Federal Trade Commission: Painting the Privacy Landscape: Informational Injury in FTC privacy and data security cases. Article published September 19 2017 and is available at https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf. Retrieved September 26, 2021.

[246] See Daniel Solove's famous book: Understanding Privacy. Harvard University Press 2008.

[247] Taxonomy of Privacy infographic provided by Enterprivacy Consulting Group, published August 3 2017, available at https://enterprivacy.com/2017/08/03/taxonomy-of-privacy-infographic/. Retrieved September 26, 2021.

[248] Danielle Keats Citron, Daniel Solove: Privacy harms. George Washington Law School Public Law and Legal Theory Paper no. 2021-11 published February 18, 2021, last revised April 14, 2022.

surface."[249] Risk generally depends on the context, the operational environment as well as the type of data, the device in question as well as access and data location, retention and preservation.[250] In addition, risk may also be based on (weak) business processes and governance, miscommunication and conflict of interest as well as resource and project management, and issues of stewardship, values and ethics.[251] Finally, Big Data and AI applications also have a political dimension and human rights implication.[252] One definition of risk the privacy community came up with is that "privacy risk equals the probability that a data processing activity will result in an impact, threat to or loss of (in varying degrees of severity) a valued outcome (for example rights and freedoms)."[253] GDPR takes a risk-based approach, for example by saying that technical and organizational measures must match the processing with regards to "the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,"[254] and GDPR also deals with high risk since impact assessments are needed for high risk data processing activities.[255] However, it is difficult to draw the line between (i.e. low) risk and high (or unacceptable) risk, but the fact that many European supervisory authorities issued guidance in accordance with GDPR Article 35 (4) and provided "list(s) about which (…) processing operations (…) are subject to the requirement for a data protection impact assessment" helps in practice when it comes to defining and documenting high-risk processing activities based on general criteria such as large-scale processing, systematic monitoring, or the use of new technology.[256]

3.3.10. Challenges with definitions and terminology

Risk is a good example of challenges as regards definitions and terminology since these seemingly simply questions raise issues in relation to scope and applicability: the notion of risk is a key element when it comes to assessing potential consequences of data processing activities. While it is clear that risk can be manifold, GDPR's comprehensive protective purpose which is laid down in the above-

[249] National Intelligence Council: Global Trends 2040 – a more contested world. Paper published March 2021, available at https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf. Retrieved September 26, 2021.

[250] Mike Dutch: A data protection taxonomy, paper for the Storage Networking Industry Association. Paper published June 2010, available at https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf. Retrieved September 26, 2021.

[251] Government of Canada: Guide to risk taxonomies. Paper published March 29 2016, available at https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html#toc2. Retrieved September 26, 2021.

[252] Catelijne Muller: The impact of Artificial Intelligence on human rights, democracy, and the rule of law. Report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Article published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved September 26, 2021.

[253] Centre for Information Policy Leadership: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. Paper published December 2016 and is available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf. Retrieved September 26, 2021.

[254] See GDPR Article 32 (1).

[255] See GDPR Article 35.

[256] GDPR Recital 91 provides background on the "necessity of a data protection impact assessment".

mentioned detailed catalogue of examples for potential risks is viewed critically for many reasons: some say that “no life risk of this world remains unmentioned in Recital 75”[257] and that this ultimately leads to the question where data protection ends. This is all the more true given the fact that more and more data qualify as personal information, because combining of data sets and the like may lead to linkability of information and identifiability of natural persons, meaning that literally any handling of data would become subject to data protection laws.[258] Others stress that data protection law, unlike other areas of law, does not dispose of limiting, restrictive criteria to help balance rights and freedoms and interest[259] and this way, allow for legal certainty. Most importantly, GDPR uses a variety of terms, and it is questionable if that means that those terms can be used interchangeably. It also leads to the question which concept is behind that terminology in the sense of what exactly is to be protected by GDPR: rights, freedoms, interests, privacy, data protection, informational self-determination, informational integrity or a combination?[260] GDPR mentions rights and freedoms fifty times, and fundamental rights and freedoms around a dozen times, whereas other terms like vital or legitimate interests, human dignity or compelling legitimate grounds are used in specific scenarios. The list of protected interests seems erratic, and it appears that literature has not yet taken the time to examine GDPR’s wording to define protected interest.

This chapter focused on the GDPR owing to its scope[261] and illustrated that the GDPR defines and thus governs the use of personal, pseudonymous as well as special categories of data. The GDPR also defines data processing, automated decision-making, and profiling as well as consent, and deals with further relevant terms including risk. However, when it comes to definitions and terminology, there are numerous challenges, be it interpretation or translation issues or the fact that GDPR uses certain terms without providing definitions, for example, freedoms and interests. A core issue that seems truly difficult to resolve is the definition and relationship between data protection and data privacy, which are terms that are often used interchangeably, even though they are not the same. In addition, further legal

[257] Niko Härting: Wann ist eine Datenverarbeitung eigentlich „erforderlich“? Article published February 1 2019, available at https://www.cr-online.de/blog/2019/02/01/wann-ist-eine-datenverarbeitung-eigentlich-erforderlich/. Retrieved September 26, 2021.

[258] Omer Tene, Jules Polonetsky: Privacy in the age of Big Data – a time for big decisions. Stanford Law Review 2012, vol. 64:63, p. 66.

[259] Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved September 26, 2021.

[260] Winfried Veil: Zum Schutzgut der DSGVO – eine naive Wortlautanalyse. Article published April 22 2021, available at https://www.cr-online.de/blog/2021/04/22/zum-schutzgut-der-ds-gvo-eine-naive-wortlautanalyse/. Retrieved September 26, 2021.

[261] Multinationals must adjust their global operations to EU standards to be compliant with provisions that are applicable to them due to the scope of certain EU laws. Some authors call this the Brussels Effect, see Anu Bradford: The Brussels Effect - How the European Union rules the world, Oxford University Press 2020.

initiatives around the globe add new terminology and definitions[262] which result in further complexity und uncertainty.

4. Characteristics, types, benefits and risks of Big Data and AI

Rather than discussing various definitions, this chapter describes Big Data and Artificial Intelligence by explaining their characteristics and the most relevant Data and Artificial Intelligence types and use cases, including their benefits to provide an overview over the impressive capabilities of these novel technologies. On the one hand, real-time analytics and the like are truly valuable from a business perspective, on the other hand, Big Data and AI may involve serious risks, and that is why this chapter explains in detail the challenges that may be involved when this technology is used, for example, data aggregation, secondary use of data, opaqueness, information mismatch, loss of human oversight as well as liability and security issues. AI's potential for discrimination, surveillance, intrusion, or manipulation, it's potential impact on privacy self-management show how important it is to investigate these effects and match to them against the present and proposed or recommended future legal framework.

4.1. Characteristics of Big Data

There are numerous definitions of Big Data, but rather than searching for the perfect definition, it makes more sense to turn to the characteristics of Big Data and to understand the value chains:[263] It can generally be said that Big Data is about the analysis[264] of vast amounts of data at high speed (ideal: 'real-time') with the aim of making it economically viable. The reason for that is that, in today's business landscape, data management can be a major determinant of success. Big data applications are characterized by large and growing amounts of data (e.g. sensor, log, clickstream, transaction or location data, search queries, social network interactions), data diversity (types, sources, formats), the speed of the evaluation (ideal: real time) and the quality of the results and forecasts obtained out.[265] Big Data lives on a large, diverse, complex and growing and pool[266] which can only be addressed with new (corresponding) techniques and a suitable infrastructure to cope with such datasets. Big Data is therefore different from old school data management, particularly because nowadays, the performance of

[262] For example, consent is defined differently in various jurisdictions, see Securiti's Q1 2023 publication: State of global consent requirements, available at https://securiti.ai/whitepapers/cookie-consent-global-heat-map/. Retrieved March 10, 2023.
[263] Nikolaus Fargo, Stefanie Hänold, Benjamin Schütze: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Fargo (eds.): New Technology, Big Data and the Law: Springer Publishing 2017, p. 21.
[264] Analyses are the second step since Big Data applications can be divided into the following stages and steps: acquisition, data processing / evaluation: Fargo et al.: The principle of purpose limitation and Big Data, p. 21.
[265] Helbing, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, Kunst und Recht 2015, vol. 3, pp. 145-150.
[266] Mario Martini: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten. Nomos Publishing Baden Baden 2015, pp. 99-169.

computational tasks place in an affordable and convenient way as processing of data is much cheaper and sharing of data is much easier.[267] It became popular to characterize Big Data by volume, variety and velocity,[268] terms which are all commencing with the initial letter "*V*", and ever since, the number of terms grew from the initial three "*Vs*" to more than forty.[269] However, only the most common vectors shall be presented in the framework of this paper:

Volume – size of data: The volume of data is increasing at a staggering rate[270] as more people use data-collecting devices and more devices are connected to the Internet, which results in the generation of billions of terabytes of (man-human, man-machine, and machine-machine) data per day.

Variety – type of data: Databases were designed to process a smaller volume of structured data, and the challenge with Big Data is that it includes various sources and formats of (un-)structured data, audio, video, social media information,[271] and that the level of completeness differs.

Velocity – speed of data: Not only the volume of data is increasing, but also the rate at which data is generated.[272] The rapidly increasing speed at which new data is being created[273] also affects the need for that data to be digested and analyzed in near real-time.

Veracity – quality of data: Veracity is about how truthful a data set may be. It has to do with improving the accuracy of Big Data by removing undesired factors like duplication, inconsistencies, abnormalities or bias. It is therefore very important[274] from a decision and intelligence viewpoint.

[267] Christopher Kuner, Fred Cate, Christopher Millard, Dan Svantesson: The challenge of Big Data for data protection. International Data Privacy Law 2012, vol. 2, no. 2, p. 47.

[268] Doug Laney (2001) for Gartner in: 3D Data Management – controlling data volume, velocity, and variety. Article published February 2001, available at http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Retrieved September 26, 2021.

[269] Tom Shafer: The 42 V's of Big Data and data science. Article published April 1 2017, available at https://www.elderresearch.com/blog/42-v-of-big-data. Retrieved September 26, 2021.

[270] Figures and background information provided by Gary Price who refers to the EMC Digital Universe Study. Study published April 16 2014, and is available at https://www.infodocket.com/2014/04/16/how-large-is-the-digital-universe-how-fast-is-it-growing-2014-emc-digital-universe-study-now-available/. Retrieved September 26, 2021.

[271] David Gewirtz: Volume, velocity, and variety - understanding the three V's of Big Data. Article published March 21 2018, available at https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/. Retrieved September 26, 2021.

[272] Tom Shafer: The 42 V's of Big Data and data science. Article published April 1 2017, available at https://www.elderresearch.com/blog/42-v-of-big-data. Retrieved September 26, 2021.

[273] For instance, in the framework of online gaming where millions of users operate concurrently or the large amount of photo material which is uploaded daily to social media platforms, or stock exchange operations where trading movements are reflected within microseconds, etc.

[274] Cassandra McNeill: Veracity – the most important "V" of Big Data. Article published August 29 2019, available at https://www.gutcheckit.com/blog/veracity-big-data-v/. Retrieved September 26, 2021.

Variability – meaning of data: Variability is different from variety as variability focuses on properly understanding and interpreting the correct meanings of raw data. This is particularly important in the framework of natural language processing.[275]

Volatility – **duration of usefulness of data:** Volatility refers to how long data is available, how long it is valid and how long it should be stored.[276] In a world of real-time data, the point at which data is no longer relevant to the current analysis has to be determined.[277]

Value – importance of data: Big Data is about turning volume to value, other characteristics seem rather meaningless if businesses cannot derive economic value and competitive advantage[278] from Big Data. Value is the return resulting from data management by using Big Data and AI: it is predicted that only China will make US$600 billion annually with the help of AI and machine learning technology.[279]

The above characteristics do not represent an exhaustive description of Big Data applications. To complete the above enumeration to a certain extent, below is an overview of the most used features in large data applications:[280]

Volume	Quantity of collected and stored data
Velocity	The transfer rate of data between source and destination
Value	Business value to be derived from Big Data
Variety	Different type of data (pictures, videos, audio) are returned
Variability	Differentiation between noisy data and important data
Veracity	Analysis of captured data is virtually worthless if it's not accurate

[275] For example, the word "great" is associated with something positive whereas "greatly" (disappointed) has a negative meaning, see Eileen McNulty: Understanding Big Data - the Seven V's, the article was published on May 22 2014 and is available at https://dataconomy.com/2014/05/seven-vs-big-data/. Retrieved September 26, 2021.

[276] Nancy Tai: Dimensions of Big Data. Article published July 27 2018, available at http://www.klarity-analytics.com/2015/07/27/dimensions-of-big-data/. Retrieved September 26, 2021.

[277] In this regard, storage limitations and legal requirements also play a role.

[278] Husam Barham: Achieving competitive advantage through Big Data – a literature review. Conference paper for the 2017 International Conference on Management of Engineering and Technology. The paper is available at https://www.researchgate.net/publication/318351614_Achieving_Competitive_Advantage_Through_Big_Data_A_Literature_Review. Retrieved September 26, 2021. Retrieved September 26, 2021.

[279] Daniel Ren: AI, Machine Learning tech promises US $600 billion annually for China economy as it pervades industries, says McKinsey. Article published July 25 2022, available at https://www.scmp.com/business/banking-finance/article/3186409/ai-machine-learning-tech-promises-us600-billion-annually?utm_source=Twitter&utm_medium=share_widget&utm_campaign=3186409. Retrieved July 25 2022.

[280] The overview is based on an article by Arockia Panimalar, Varnekha Shree and Veneshia Kathrine who describe the evolution of the vectors in their article: The 17 V's of Big Data, International Research Journal of Engineering and Technology 2017, vol. 4, issue 9, pp. 329-333, available at https://www.irjet.net/archives/V4/i9/IRJET-V4I957.pdf. Retrieved September 26, 2021.

Validity	Accuracy of data used to extract result in the form of information
Volatility	Question of how long the stored data is useful for the user
Virality	Rate at which the data is spread and received by different users
Viscosity	Time difference when the event occurred and when it was described
Vagueness	Ambiguity about data found; interpretation issues with results found

Even though it is still very common to link Big Data and AI to large volumes of data, some scientists believe that the future of Artificial Intelligence will be about less data, not more:[281] they claim that the training on mountains of data will soon be replaced since such systems have serious limitations, for example in cases in which little data exists or in instances where computers can be easily stumped.[282] They believe that companies will rely less on bottom-up data and more on top-down reasoning which resembles the way humans approach problems and tasks, e.g., by using common sense and ready expertise.

4.2. Types of Big Data analytics

As regards Big Data analytics, a general distinction can be made between three dominant types of analytics, each of them offering different findings: descriptive, predictive and prescriptive analytics.[283] Descriptive analytics use data aggregation and data mining to create reports, dashboards or scorecards in order to provide insight into the past. Predictive analytics use statistical models and forecasts techniques to discover explanatory patterns, and that is why such tools can predict an outcome with a significant probability of accuracy and provide businesses the ability to forecast future developments. Prescriptive analytics use optimization and simulation algorithms to provide advice on possible outcomes. The possibilities to make use of Big Data applications are countless, however, Big Data applications can roughly be divided in the following groups:[284] customer analytics, operational analytics, analytics which are used to (further) develop data-driven products and services as well as tools which are used for compliance purposes and fraud detection. These objectives are often grouped in a different

[281] James Wilson, Paul Daugherty, Chase Davenport: The future of AI will be about less data, not more. Article published January 14 2019, available at https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more. Retrieved September 26, 2021.

[282] At present, smart phone facial recognition systems are sometimes unable to recognize "morning faces", i.e., a puffy, haggard look on first awakening; autonomous driving is tricky as such cars have difficulties to recognize children or pedestrians wearing costumes; so-called CAPTCHAs are easy for humans, but hard for computers.

[283] Explanations and definitions of these terms can be found in James Blackman's 2018 article: Operational intelligence, three ways – descriptive, predictive and prescriptive. Article published December 11 2018, available at https://enterpriseiotinsights.com/20181211/channels/fundamentals/descriptive-predictive-prescriptive-analytics. Retrieved September 26, 2021.

[284] A summary on Big Data use cases is provided by Datameer in their 2016 E-book: Top five high-impact use cases for Big Data Analytics. E-book published 2016, available at http://orcp.hustoj.com/wp-content/uploads/2016/01/eBook-Top-Five-High-Impact-UseCases-for-Big-Data-Analytics.pdf. Retrieved September 26, 2021.

manner, depending on whether or not transactional data are in question, such as: decision science to improve the decision-making process; performance management which is typically done by business intelligence tools using dashboards, reports; data exploration which makes use of statistics to allow for predictive modeling as well as (social) analytics to measure awareness, engagement and word of mouth, the success of (online) campaigns, etc.[285]

4.2.1. Operational analytics and forecasting

Operational analytics refers to business analytics which focus on improving existing operations and to get more transparent information for business planning purposes.[286] As such, the idea of improving of business operations is anything but new. The difference nowadays is that Big Data allows for a more detailed and timely insight into operations, which is important for monitoring and maintenance of systems or supply chain management etc. A higher level of operational analytics can be achieved when so-called data warehouse optimization is used: A data warehouse[287] is a data-service platform, a repository for all data an enterprise holds in various operational systems with the aim to capture data from diverse sources to allow for access and analysis rather than for transaction processing. The advantage[288] of such a unified database is that it allows for a unified approach for organizing and representing data; that is has a robust infrastructure; ideally with a high level of security and scalability; that it is accessible across the company for all divisions and that it enables contingency plans in terms of business continuity.

4.2.2. Customer analytics and marketing

There is a myriad of uses cases when customer analytics are in question: the segmentation of customers based on behavior patterns, the creation of 360-degree customer views, the analysis of customer sentiments, the delivery of personalized customer services based on customer profiles in real time, e.g., by so-called robo-advisor services or chat-bots,[289] the recommendation of next-best products to buy or

[285] Salvatore Parise, Bela Iyer, Dan Vesset: Four strategies to capture and create value from Big Data, published in Ivey Business Journal, July/August issue 2012, available at http://www.iveybusinessjournal.com/topics/strategy/four-strategies-to-capture-and-create-value-from-big-data#.Uwm-L4XHjWh. Retrieved September 26, 2021.

[286] Definition provided by Technopedi at their website, available at https://www.techopedia.com/definition/29495/operational-analytics. Retrieved September 26, 2021.

[287] Background information on the term enterprise data warehouse is provided by Jamens Kobielus: The enterprise data warehouse – defined, refined, evolving with the times. Article published April 8 2008, available at https://go.forrester.com/blogs/08-04-08-the_enterprise_data_warehouse_edw_defined_refined_evolving_with_the_times/. Retrieved September 26, 2021.

[288] Features provided by Technopedia at their website, available at https://www.techopedia.com/definition/26204/enterprise-data-warehouse. Retrieved September 26, 2021.

[289] Examples provided by Karsten Egetoft: Data-driven analytics: practical use cases for financial services. Article published published January 29 2019, available at https://www.digitalistmag.com/customer-

the prevention of customer churn,[290] The prevention of customer churn is good example of how Big Data analytics are used as a basis for follow-up measures: an organization conducts a data analysis and identifies potentially critical moments in the customer relationship, for example by analyzing the ratio between the term and the amount of a loan in relation to the time at which loans were repaid in advance. The analysis is the first step for the creation of an efficient marketing mix as only those customers will be contacted where data indicated that there is a risk of early repayment, resulting in financial loss for the bank. As far as data protection is concerned, the first step may well work with aggregated data without the need to process personal data, but the second step is legally much more demanding as customer contacts are covered not only by data protection, but also by competition law.[291] Another important use case is social media – from advertising to speech and content moderation.

4.2.3. Data-driven products and services

A prominent example of analytics which are used for data-driven products and services is pricing. Average Internet users are not aware that neither the content[292] which a website displays nor the prices it indicates are the same to every user. Online shops are technically capable to offer each website customer a different price, a practice called personalized pricing:[293] customers can be recognized with the help of so-called cookies[294] which can categorize customers in order to group them as an either price-sensitive or a price-insensitive person. It can be argued that European data protection law applies to personalized pricing, meaning that companies are required to inform people about the specific purpose of processing their personal data.[295] The lawfulness of price personalization under the GDPR on the basis of consent, the necessity for pre-contractual or contractual measures, and the data controller's

experience/2019/01/29/data-driven-analytics-practical-use-cases-for-financial-services-06195123/. Retrieved September 26, 2021.

[290] An exhaustive overview over Big Data use cases is provided by Alexander Bekker: Twenty Big Data use cases. Article published March 6 2018, available at https://www.experfy.com/blog/twenty-big-data-use-cases. Retrieved September 26, 2021.

[291] And, depending on the case and the jurisdiction in question, further laws might apply, for example, in the framework of unsolicited telephone calls or commercial e-mails. Such communications, as opposed to postal advertising which was priviledged under German data protection law, always required specific legal checking.

[292] So-called "responsive web-design", see http://blog.freedomscientific.com/responsive-web-design-why-one-site-can-behave-differently-on-different-pcs-and-browsers/ for background information. Retrieved September 26, 2021.

[293] Frederik Zuiderveen Borgesius, Joost Poort: Online price discrimination and EU data privacy Law. Journal of Consumer Policy 2017, vol. 40, issue 3, pp. 347-366, available at https://www.researchgate.net/publication/318511438_Online_Price_Discrimination_and_EU_Data_Privacy_Law. Retrieved September 26, 2021.

[294] ICO describes cookies as "a small file of letters and numbers that is downloaded on to your computer when you visit a website. Cookies are used by many websites and can do a number of things, e.g. remembering your preferences, recording what you have put in your shopping basket, and counting the number of people looking at a website", see https://ico.org.uk/your-data-matters/online/cookies/. Retrieved September 26, 2021.

[295] Frederik Zuiderveen Borgesius, Joost Poort: Online price discrimination and EU data privacy law, Journal of Consumer Policy 2017, vol. 40, issue 3, pp. 347-366.

legitimate interests has been the subject of numerous publications.[296] Moreover, the Privacy and Electronic Communications Regulation (PECR) also covers cookies and the use of similar technologies for storing or accessing information, including technologies like device fingerprinting.[297] As a result, such an approach is as tempting as it is legally demanding.

4.2.4. Fraud prevention and compliance issues

Fraud prevention is a good example of how Big Data applications can help businesses to achieve legal compliance as, e.g., the banking sector is obliged to perform background checks and to permanently screen transactions to fulfill requirements which arise from various sanction lists.[298] Big Data analytics can also be very helpful when companies want to detect suspicious activities to prevent and fight fraud. This is especially important to e-commerce as there are specific challenges in the area of distance selling, for example, the identification of the customer, address verification, credit assessment and the like.[299] Because companies do not want to risk customer dissatisfaction through service delays or payment rejections, they turn to device or geo-location or even social media data analysis to perform real-time-checks for suspicious activities[300] so that the (online) customer journey is neither interrupted nor disturbed. This approach is comprehensible from a business point of view in terms of protection from possible financial risks arising from fraud.[301] But it should not be forgotten that such procedures are questionable[302] with regard to transparency requirements vis-à-vis data subjects; an average buyer does not suspect that a simple online order leads to a variety of background checks including devices and online activities, and it might therefore not cross his mind to read (extensive) privacy notices prior to the purchase.

4.2.5. Sense-making

In the context of Big Data analytics, a new class of analytic capability emerged which may be characterized as (general purpose) sense-making. This approach relates to a new type of technology

[296] For instance, Richard Steppe: Online price discrimination and personal data: a General Data Protection Regulation perspective. Computer Law & Security Review 2017, vol. 33, issue 6, pp. 768-785.

[297] See ICO at https://ico.org.uk/your-data-matters/online/cookies/. Retrieved September 26, 2021.

[298] Ernst & Young: Effective screening controls for sanctions and AML risk management. Paper published April 12 2018, available at https://vdocuments.net/effective-screening-controls-for-sanctions-and-aml-risk-screening-controls-for.html Retrieved September 26, 2021.

[299] Examples of retail use cases are provided by Igor Bobriakov: Top 10 data science use cases in retail. Article published July 22 2018, available at https://medium.com/activewizards-machine-learning-company/top-10-data-science-use-cases-in-retail-6483accc6042. Retrieved September 26, 2021.

[300] For instance, the German company named RiskIdent. Background information on their services and the way they work is available at https://riskident.com/de/technologie/. Retrieved September 26, 2021.

[301] Also offered by the German company Arvato Financial Solutions as explained on their website https://finance.arvato.com/de/financial-solutions/fraud-management/fraud-detection.html. Retrieved September 26, 2021.

[302] The question is also whether or consent or legitimate interests shall serve as legal basis.

which helps organizations to make decisions faster and better. Unlike master data management which helps businesses to gain control over information in order to have consistent and reliable master data records, sense-making is about making sense of “their diverse observational space, ranging from data they own and control (e.g. structured master data) to data they do not or cannot control (e.g. externally-generated and less structured social media”.[303] Sense-making suggests that an organization can only be as smart as the sum of its observations collected across various enterprise systems,[304] and this is where Artificial Intelligence comes into play:

4.3. Types of Artificial Intelligence

4.3.1. Rule-based Artificial Intelligence

There are many forms of Artificial Intelligence; traditional algorithmic AI is rule-based, and therefore often compared to a recipe, including more or less of ingredients, and therefore leading to more or less accurate results. Rule-based Artificial Intelligence is the simplest form of AI[305]: knowledge is achieved by applying a set of rules.

4.3.2. Search and planning Algorithms

In the age of Internet, probably the most prominent examples of Artificial Intelligence are algorithms that are used frequently to search for all kinds of goods, items, hints or suggestions. Search algorithms are very useful type of AI, but their problem-solving capacities can be limited depending on their ability to take constraints into account. That is why search algorithms are often combined with planning (and / or scheduling) algorithms.[306]

[303] Background information on the issue is provided by Jeff Jonas: Master data management vs. sensemaking, Article published November 11 2011, available at http://jeffjonas.typepad.com/jeff_jonas/2011/11/master-data-management-mdm-vs-sensemaking.html. Retrieved September 26, 2021.

[304] Ann Cavoukian, Jeff Jonas: Privacy by Design in the age of Big Data. Article published June 8 2012, available at https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf. Retrieved September 26, 2021.

[305] Background information on various types of Artificial Intelligence is provided by Tricentis at their website, available at https://www.tricentis.com/artificial-intelligence-software-testing/ai-approaches-rule-based-testing-vs-learning/. Retrieved September 26, 2021.

[306] Debby Nirwan: Using forward-search algorithms to solve AI Planning Problems. Article published September 19 2020, available at https://ai.plainenglish.io/using-forward-search-algorithms-to-solve-ai-planning-problems-361ad4910239. Retrieved September 26, 2021.

4.3.3. Symbolic Artificial Intelligence including Expert Systems

Symbolic Artificial Intelligence was the main area of interest in the early decades of AI research[307] and the first important step to design computers to assist humans in with complex decisions. This approach is also known as classical Artificial Intelligence and encompasses all AI methods that are based on symbolic, i.e., human-readable representations of problems, logic, and search.[308] Since this type of AI helps experts in various professional domains to make their decisions, such symbolic AI systems are called Expert Systems. Expert Systems are knowledge repositories used to gather human expertise and to replicate that knowledge[309]. The first such system was already introduced in 1965.[310] Even though Symbolic Artificial Intelligence led to significant advances in the understanding of cognition, symbolic AI has fallen by the wayside as Neural Networks gained traction.[311]

4.3.4. Knowledge Engineering

Knowledge Engineering is a field of Artificial Intelligence that aims at imitating the way humans think and approach problems; Knowledge Engineering is used in decision support software and similar to Expert Systems[312], it imitates the judgment of human experts by codifying knowledge as rules and relationships between data,[313] but is specific insofar as it tries to provide solutions for today’s information explosion: e.g., in the area of taxation[314], it is hard to keep pace with ever-changing rules and regulations. This is a where Knowledge Engineering could help by using various algorithms, from

[307] Ranjeet Singh: The rise and fall of Symbolic AI. Article published September 14 2019, available at https://towardsdatascience.com/rise-and-fall-of-symbolic-ai-6b7abd2420f2. Retrieved September 26, 2021.

[308] Eleni Ilkoua and Maria Koutrakia provide background information on Symbolic AI in their 2020 paper: Symbolic vs. sub-symbolic AI methods: friends or enemies? Proceedings of the CIKM 2020 workshops held October 19-20 in Galway, Ireland. The paper is available at http://ceur-ws.org/Vol-2699/paper06.pdf. Retrieved September 26, 2021.

[309] Indranil Das: How to implement Expert Systems in Artificial Intelligence? Article published September 18 2019, available at https://www.edureka.co/blog/expert-system-in-artificial-intelligence/#ExpertSystemInArtificialIntelligence. Retrieved September 26, 2021.

[310] The first Expert System that used AI to solve problems within a specialized domain that normally requires human expertise was developed in Stanford by Edward Feigenbaum and colleagues. Background information on Feigebaum’s role for expert systems is provided by Stanford University at their website, available at https://cs.stanford.edu/people/eaf/wordpress/. Retrieved September 26, 2021.

[311] Sebastian Bader, Pascal Hitzler explain the differences of Symbolic AI and Neural Networks: Dimensions of neural-symbolic Integration - A Structured Survey. Article published November 10 2005, available at https://arxiv.org/pdf/cs/0511042.pdf. Retrieved September 26, 2021.

[312] Background information is provided by Nathalie Aussenac-Gilles, Jean Charlet, Chantal Reynaud: Knowledge Engineering. A Guided Tour of Artificial Intelligence Research. Springer Publishing 2020, pp.733-768.

[313] Michael Radwin: Knowledge Engineering demystified, expert paper for the Future of Privacy Forum issued February 8 2021.

[314] Gang Wang: Tech Talk: Intuit’s AI-powered tax knowledge engine boosts filers’ confidence. Article published March 6 2019, available at https://www.intuit.com/blog/social-responsibility/tech-talk-intuits-ai-powered-tax-knowledge-engine-boosts-filers-confidence/?q=knowledge+engineering++taxation&qs=n&form=QBRE&sp=-1&pq=knowledge+engineering+taxation&sc=0-30&sk=&cvid=C86F17EA921A4662B0AEE8187B558298. Retrieved September 26, 2021.

Natural Language Processing to interpret laws to graph representations to find the relationships of new rules to previous instances. However, a challenge in the field of Knowledge Engineering is the capture of tacit knowledge[315]: it was soon discovered that human experts also rely on collateral data and that the interaction between explicit and tacit knowledge is vital for the creation of new knowledge.

4.3.5. Robotics

Robotics are used in various domains: they can be used in the industry to handle material, they can be used in the medical sector able to perform complex surgeries, and they can be used or for exploration purposes or even for the military as robots (including drones) can reach inaccessible, hazardous zones or to identify and destroy life-threatening objects. Especially these military use cases show the ethical implications of certain types of Artificial Intelligence; data protection is a lesser issue here, and there are further legal issues, for example the handling of machine data, non-personal information, data ownership or questions of own legal personality. It can be generally said that Robotics heavily rely on electrical and mechanical engineering and given the fact that robots in many industrial use cases must be capable of using vision to locate and assemble goods, advances in Robotics will very likely rely on progress in the field of Computer Vision and other forms of machine perception:

4.3.6. Computer sensing and vision

Another form of Artificial Intelligence is Computer Sensing where computers are designed with a range of sensors to enable them to see, listen or taste to assess their environment and, e.g., measure distance or acceleration and speed, temperature as well as light. This type of AI is thus used for augmented machine perception, and at present, Computer Vision is probably the most prominent form of Computer Sensing: computers are able to perform certain tasks like image and video captioning much better than humans could, and far beyond human perception[316]. Owing to the fact that the application domains of this type of AI include biometrics and face recognition[317], Computer Vision is one of the most

[315] Dag Prawitz: Tacit knowlege - an impediment for AI? in: Göranzon et al.: Artifical Intelligence, culture and language: on education and work. Springer Publishinng 1990, available at https://doi.org/10.1007/978-1-4471-1729-2_7. Retrieved September 26, 2021.

[316] Stanford University: One-hundred-year Study on AI (AI100) 2016, Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 26, 2021.

[317] Facial and character recognition techniques generally have a potential for bias and discrimination, and the ClearView case showed how easy it has become to use a single piece of information to identify and track individuals: the company scraped more than three billion facial images from social media sites. The scope of the matter and the lack of legal basis cause the European Commission to consult with national data protection authorities on how to proceed in the case: Samuel Stolton: After Clearview AI scandal, Commission 'in close contact' with EU data authorities. Article published February 12 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/. Retrieved September 26, 2021.

problematic forms of Artificial Intelligence from a privacy perspective: while truly promising medical advancements seem possible by iris diagnostics with the help of AI which even go beyond diagnosing mere ocular diseases,[318] one and the same AI could cause serious challenges when used in a different setting, for example in the employment context, allowing for the collection of employees' biometric data – like the example of Metaverse, the digital future Mark Zuckerberg is steering shows:[319] Metaverse[320] is a collective virtual shared space where users can interact, a digital reality that combines social media, augmented and virtual reality, online gaming, and cryptocurrencies.[321] Metaverse adds a more complex dimension to today's privacy challenges[322] if employees were forced to use the Metaverse. Computer Vision is also one of the most challenging disciplines from a technical point of view, and that is why Computer Sensing is often combined with other types of AI, including rule-based and symbolic Artificial Intelligence as well as so-called Machine Learning:

4.3.7. Machine Learning

The emergence of Machine Learning (ML) is the reason why millions of users globally enjoy their smart devices and specialized (fitness, banking, weather, etc.) apps without really being able to tell what this type of AI is about. In fact, many people use the terms Machine Learning and Artificial Intelligence interchangeably. But ML is a new form of AI that can be distinguished from traditional Artificial Intelligence since it gives computers the ability to learn from and improve with experience by focusing on learning through patterns and building rules a from examples.[323] Some describe AI as the intelligence and Machine Learning as the implementation of the compute methods which support it.[324] One could therefore speak of Machine Learning as the art of having computers perform without being programmed

[318] Ursula Schmidt-Erfurth, Amir Sadeghipour, Bianca Gerendas, Sebastian Waldstein, Hrvoje Bogunović: Artificial Intelligence in retina. Article published August 1 2018, available at https://pubmed.ncbi.nlm.nih.gov/30076935/. Retrieved September 26, 2021.

[319] Claudio Müller: Leben im Metaverse: Was, wenn Zuckerberg gewinnt? Article published November 19 2021, available at https://www.giga.de/news/leben-im-metaverse-was-wenn-zuckerberg-gewinnt/. Retrieved July 22, 2022.

[320] The term Metaverse was coined by author Neal Stephenson in his 1992 science-fiction novel "Snow Crash" in which envisions a virtual reality-based successor to the Internet. Tom Huddleston reports on the novel in his article: This 29-year-old book predicted the Metaverse – and some of Facebook's plans are eerily similar. Article published November 3 2021, available at https://www.cnbc.com/2021/11/03/how-the-1992-sci-fi-novel-snow-crash-predicted-facebooks-metaverse.html. Retrieved July 25 2022.

[321] Jean Folger: What is the Metaverse? Article published July 6 2022, available at https://www.investopedia.com/metaverse-definition-5206578. Retrieved July 25, 2022.

[322] Kate Beioley: Metaverse vs employment law: the reality of the virtual workplace. Article published February 21 2022, available at https://www.ft.com/content/9463ed05-c847-425d-9051-482bd3a1e4b1. Retrieved July 25, 2022.

[323] Ben Dickson: Why the difference between AI and machine learning matters. Article published October 8 2018, available at https://bdtechtalks.com/2018/10/08/artificial-intelligence-vs-machine-learning/. Retrieved September 26, 2021.

[324] Statement provided by Intel's head of machine learning, Nidhi Chappell, quoted in Lee Bell's article: Machine learning versus AI: what's the difference? Article published December 1 2016, available at https://www.wired.co.uk/article/machine-learning-ai-explained. Retrieved September 26, 2021.

in a specific way.[325] Introduced in 2014[326], so-called Generative Adversarial Networks (GANs) are the newest variation of Machine Learning: two neural networks contest with each other, i.e. the second neural network (discriminator) evaluates the other network (generator) in a game to create and refine data (results).

4.3.8. Supervised and Unsupervised Learning

Machine Learning can be roughly separated into supervised and unsupervised (predicted) learning[327] as there are several ways to train algorithms: in a supervised learning model, the algorithm is provided with and learns from a labeled dataset for which the correct outcome is provided so that the network can learn to map inputs to observations and make necessary adjustments to learn for the future. An unsupervised model works with no or minimal human supervision and computers must look for patterns within an unlabeled (unclassified) dataset. Another name for unsupervised learning is knowledge discovery because unsupervised learning is used to find hidden patterns. Between these two main methodological types of Machine Learning lies so-called semi-supervised learning where a system is provided with a small set of labeled examples, and also uses unlabeled information within the same dataset for evaluation and analyzing purposes.

4.3.9. Reinforcement Learning

Alongside with supervised learning and unsupervised learning, Reinforcement Learning is one of three basic Machine Learning paradigms and has been around for some time already: Reinforcement Learning is built on observation[328] to allow for making optimal decisions and complete tasks within an uncertain environment using experiences. The focus of Reinforcement Learning is thus rather experience-driven decision-making than pattern recognition[329]: Reinforcement Learning aims at independent learning and performance of human-like goal-oriented tasks. There are more and more practical use cases in this area, and it is likely that Reinforcement Learning will play a vital role in future Robotics.

[325] UK House of Lords 2018 report on AI: AI in the UK: ready, willing and able? Report published April 16 2018, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf. Retrieved September 26, 2021.

[326] Ian Goodfellow et al.: Generative Adversarial Networks, Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), pp. 2672-2680, available at https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf. Retrieved September 26, 2021.

[327] Isha Salian: SuperVize Me: What's the difference between supervised, unsupervised, semi-supervised and Reinforcement Learning? Article published August 2 2018, available at https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/. Retrieved September 26, 2021.

[328] Diana Borsa, Bilal Piot, Rémi Munos, Olivier Pietquin: Observational learning by reinforcement learning. Article published June 20, 2017, available at https://arxiv.org/abs/1706.06617. Retrieved September 26, 2021.

[329] Stanford University: One-hundred-year study on Artificial Intelligence (AI100), Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 26, 2021.

4.3.10. Neural (Connectionist) Networks

An Artificial Neural Network (ANN) is inspired by the idea of imitating the human brain: computers are built in a manner suggestive of the connections between neurons in a human brain by using silicon and wires which act similar as dendrites and neurons:[330] Neural Networks use processors which are interconnected and are able to learn by a process of trial and error. One of the pioneers in this area defined a neural network as a computing system made up of a number of simple but highly interconnected processing elements that process information by their dynamic state response to external inputs.[331] The emergence of Artificial Neural Networks was a crucial aspect for the advancement of Artificial Intelligence.

4.3.11. Deep Learning

Deep Learning is part of Machine Learning[332] and uses Neural Networks that work with artificial neurons.[333] This area of Artificial Intelligence uses Neural Networks that are layered in a manner that allows for interaction between input and output values, i.e., passing back and forth input and output data with the help of mathematical functions so that new information is generated. This type of processing has helped with object and activity recognition and enabled progress in specific areas of perception, e.g., audio or speech.[334]

4.3.12. Natural Language Processing

Natural Language Processing (NLP), which is often combined with automatic speech recognition, is one of the most common forms of Artificial Intelligence: “Siri”, “Alexa”, “Cortana” are prominent examples of (home-based) assistants, and the growing Internet connectivity of devices and appliances (Internet of Things) will further reinforce this. “DeepL” is a good example of how far machine translation has come

[330] Background information about ANN is provided by Oludare Abiodun et al.: State-of-the-art in artificial neural network applications. Heliyon 2018, vol. 4, issue 11, available at https://www.sciencedirect.com/science/article/pii/S2405844018332067. Retrieved September 26, 2021.

[331] The University of California at San Diego published an article about the life-time achievements of Dr. Hecht-Nielsen. Article published July 1 2019, available at https://qi.ucsd.edu/news-article.php?id=3089. Retrieved September 26, 2021. Dr. Hecht-Nielsen authored the first textbook on the subject, Neurocomputing, in 1989 (see https://www.semanticscholar.org/paper/Theory-of-the-backpropagation-neural-network-Hecht-Nielsen/f4457792a247c0eb6c6fb11a1d92f6f45b82acc1 for details).

[332] Connor Shorten: Machine Learning vs. Deep Learning. Article published on September 7 2018, available at https://towardsdatascience.com/machine-learning-vs-deep-learning-62137a1c9842. Retrieved September 26, 2021.

[333] Nagesh Singh Chauhan: Introduction to artificial neural networks. Article published October 13, 2019, available at https://towardsdatascience.com/introduction-to-artificial-neural-networks-ann-1aea15775ef9. Retrieved September 26, 2021.

[334] Stanford University: One-hundred-year study on Artificial Intelligence (AI100). Report published September 2021, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf. Retrieved September 26, 2021.

in the recent years, and the debut of "ChatGPT" has recently drawn a great deal of attention due to the fact that it can generate high-quality responses. The shift in NLP is to move away from systems that allow for real-time interaction with, e.g., customers to genuine dialogue.

The above-mentioned instances do not represent an exhaustive description of all types of Artificial Intelligence. To summarize the above enumeration to a certain degree, below is an overview of the most used types of Artificial Intelligence:[335]

Symbolic AI	Human-readable logic problems
Rule-based AI	Deductions based on curated rules
Search	Steps from initial state to goal
Planning & Scheduling	Multi-dimensional strategies and action sequences
Computer Sensing	Using human sense-based inputs
Robotics	Mobile AI and multi-sensing
Expert Systems	Complex solutions through reasoning
Knowledge Engineering	Technology behind expert systems
Machine Learning	Improvements through experience
Deep Learning	Using multiple layers of neural networks
Reinforcement Learning	Learning to a complex task
Natural Language Processing	Understanding and interpreting language
Neural Networks	Learning by making connections

4.4. Use cases of Artificial Intelligence

There are countless use cases of Artificial Intelligence:[336]

Retail	Virtual mirrors, cashless stores
Mobile	Voice to text, smart personal assistants
Hospitality	Predictive supply chain, concierge services
Media	Automated journalism, identification of fake news
Insurance	Risk identification, client support, personalized pricing

[335] The overview is based on a document provided by Brenda Leong of the Future of Privacy Forum called "The spectrum of Artificial Intelligence". Infographic published December 14, 2020, available at https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool/. Retrieved September 26, 2021.

[336] An overview on use cases is provided by BITKOM, the German Association for Information Technology, Telecommunications and New Media in their 2019 guideline: Konkrete Anwendungsfälle von KI & Big-Data in der Industrie. Guideline published 2019, available at https://www.bitkom.org/sites/default/files/2020-02/200203_lf_ki-in-der-industrie_0.pdf. Retrieved September 26, 2021.

Cyber-security	Incident detection and accelerated incident response
Gaming	Improved visual quality, 3D-Avatars, thought-controlled gaming
Education	Plagiarism detection, digital learning interfaces, virtual teachers
Banking & Finance	Fraud prevention, credit decision making, client segmentation
Smart homes	Personal assistants, home security, automated good ordering
Transport	Travel time reduction through traffic analytics, autonomous vehicle
Agriculture	Robot harvesting, computer vision to monitor soil health and needs
Real Estate	Market and price analysis, client segmentation, targeted advertising
Entertainment	Music and TV suggestions, search optimization, personalization
Defense	Target identification, autonomous weapons, simulations, training
Communications	Spam filters, real-time translation, emotion analysis, text suggestions
Online Shopping	Search recommendations, customer services and sales chat-bots
Social Networks	Photo recognition, chat-bots, friendship suggestions, personalization
Workplace	Robotics, automated checks in factories, enhanced recruitment
Healthcare	Virtual doctors, surgery robots, drug discovery, enhanced diagnostics
Politics & government	Targeted campaigning, public opinion monitoring, predictive policing

4.5. Benefits and challenges of Big Data and Artificial Intelligence

Big Data and AI applications are attractive for companies since they allow for analytics, customer insights, forecasting, decision-making, and the optimization of processes, products, quality and services.[337] Big Data and AI can help to better understand market conditions and customer needs and such applications are therefore valuable for product development and overall innovation to achieve the desired competitive advantage; the same applies to necessary adjustments to reflect external and internal developments that can be better monitored with corresponding tools, even for reputation control.[338] From a company perspective, Big Data and AI are particularly useful for increasing productivity, managing inventory manufacturing, delivery and distribution and fostering preventive maintenance.[339] This technology can thus improve operational efficiency and optimize business outcomes.[340] Big Data and

[337] Pricewaterhouse Cooper's 2021 AI predictions survey published October 2020, available at https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html. Retrieved September 26, 2021.

[338] Background information on social media sentiment analysis is provided by New Generation Applications Ltd. in their August 29 2017 news, available at https://www.newgenapps.com/blog/the-secret-way-of-measuring-customer-emotions-social-media-sentiment-analysis. Retrieved September 26, 2021.

[339] Alexander Bekker provides a comprehensive overview over Big Data use cases in his article: Twenty Big Data use cases. Article published May17 2021, available at https://www.experfy.com/blog/twenty-big-data-use-cases. Retrieved September 26, 2021.

[340] Further details are provided by Karsten Egetoft: Data-driven analytics – practical use cases for financial services. Article published January 29 2019, available at https://www.digitalistmag.com/customer-

AI have proven to be valuable: so-called smart grids, traffic management as well as the medical sector as well as mobile and online applications are further important uses,[341] and based on existing experience thus far, it can generally be said that the use of Big Data and AI typically goes along with time reductions and cost savings.[342] In the last years, there has been an increased awareness with regards to these benefits, and this resulted in corresponding investments in the relevant infrastructure. Consequently, retail and insurance companies as well as financial institutions and governments use Big Data for various purposes, e.g., for the improvement and tailoring of products and services, for the assessment of churn rates, creditworthiness or other risks including detection of potential fraud and abuse, and they all follow their own Big Data value chain, from data collection to storage and analysis and the use of the results.[343] The maturation of Big Data and AI software was also an important factor for the growing success of such applications. It can therefore be concluded that Big Data and AI drive growth for those companies that know how to take advantage of "data-driven decision-making"[344] for their business. Conversely, the inability of an organization to benefit from the information it possesses can result in what is called "enterprise amnesia".[345] Despite of the existing potentials of Big Data and Artificial Intelligence in terms of analytics, mining, reporting, simulation and visualization, it should not be forgotten that evaluations that are based on Big Data and AI do not automatically lead to correct or meaningful results: e.g., a correlation was proven between the rise in stock market prices and Superbowl results; the same applies to the correlation between the susceptibility of Angina Pectoris and the individuals with the zodiac sign Aquarius.[346] It is difficult to capture meaningful results as algorithms do not dispose of social skills[347] or the intuition to discard patterns if need be. This is especially true for behavioral analytics since human behavior is not only guided by reason, but often driven by emotions. To provide a very simple example, it cannot necessarily be assumed that the frequency of clicking on certain messages is in an indicator for

experience/2019/01/29/data-driven-analytics-practical-use-cases-for-financial-services-06195123. Retrieved September 26, 2021.

[341] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[342] Pricewaterhouse Cooper's 2021 AI predictions survey published October 2020, available at https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html. Retrieved September 26, 2021.

[343] International Working Group on Data Protection in Telecommunications: Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics, p.18. Paper published May 6 2014, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf. Retrieved September 26, 2021.

[344] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[345] Ann Cavoukian, Jeff Jonas: Privacy by Design in the age of Big Data. Article published June 8 2012, available at https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf. Retrieved September 26, 2021.

[346] Mario Martini: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten. Nomos Publishing Baden Baden 2015, pp. 99-169.

[347] Niko Härting: Internetrecht. Dr. Otto Schmidt Publishing 2014, p. 626.

their importance to the user.[348] And there are always two sides of the medal, while Big Data and AI may be beneficial businesses, there seems to be a price tag for individuals: health data management is valuable, but dependent on very sensitive data; traffic management is desirable but could lead to seamless tracking of motion patterns based on geo-location data, and the same is true for data collected from mobile devices. There have been reports that operating systems are transmitting a lot of user data even if users deliberately switch off certain services such as location-based services.[349] So-called smart meters electricity suppliers started using some years ago are very useful for billing purposes. But smart meters are able to transmit power consumption levels within short intervals, and a result, suppliers have detailed information about the intensity of the usage of household devices – sensors work so precisely that they can even capture which TV channels have been watched.[350] Smart meters thus allow for a detailed at customer usage behavior, and that implies privacy risks.[351] In addition, smart meters are also a good example for unexpected results: consumption data clearly show whether and how many people have been present in certain premises for a certain period of time. Therefore, smart meter data could be used in tax matters and may serve as evidence if a taxable (primary) residence is in question. Big Data and Artificial Intelligence can generally only create value if the delivered results and conclusions are meaningful. However, the problem is that any decision-making process is based and dependent on a high number of other, underlying decisions, and that makes the process vulnerable to errors which vary in complexity, their consequences and in the extent to which they can be influenced. It is important to note that various errors can occur in every single phase of the design and decision process:[352] errors can already occur during the design phase of algorithms or when the automatic decision-making system is constructed; operationalization errors can lead to results which cannot be interpreted in a meaningful manner. Finally, errors may occur when users fail to recognize poor data and / or when they misinterpret results. The factual challenge is that, on top of a multitude of legal questions that arise when Big Data and Artificial Intelligence are in question, there is a high potential for failure as every single phase of the automatic decision-making process is theoretically error-prone: even correct data may lead to wrong decisions, because users' conclusions may be wrong, and because users can influence results by the way

[348] Niko Härting: Internetrecht. Dr. Otto Schmidt Publishing 2014, p. 627.

[349] A corresponding study was conducted by Douglas Schmidt: Google Data Collection, Article published August 2018, available at https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf. Retrieved September 26, 2021.

[350] Researchers confirmed this result in the framework of the Data Privacy Management project funded by the federal government. They summarized their findings in a working paper which was published in 2011: Hintergrund und experimentelle Ergebnisse zum Thema Smart Meter und Datenschutz. Münster University of Applied Sciences, available at http://1lab.de/pub/smartmeter_sep11_v06.pdf. Retrieved September 26, 2021.

[351] Jens-Matthias Bohli, Christoph Sorge and Osman Ugus offer an overview on the problem in their 2010 paper: A Privacy Model for Smart Metering, 2010 IEEE International Conference on Communications Workshops, Capetown, 2010, pp. 1-5.

[352] Katharina Zweig, Sarah Fischer, Konrad Lischka: Wo Maschinen irren können – Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung. Bertelsmann Stiftung Publishing, pp. 21-28. Report published February 2018, available at https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WoMaschinenIrrenKoennen.pdf. Retrieved September 26, 2021.

the dataset is defined or by the way the algorithm is written.[353] After all, decision-making with the help of Big Data and AI in many cases still means interpretation of results by individuals, and this is where (human) mistakes come into play. In this context, it is important to note that some authors[354] claim that next generation smart information management systems can reduce false positives and false negatives because they are able to deal with plausible variations and that context-accumulating systems will automatically determine if new observations reveal something of sufficient interest to provoke a reaction rather than data scientists asking questions to the system. Businesses will for sure welcome such developments, but from a data protection perspective, responsible innovation including privacy-enhancing elements should be applied to prevent harms for individuals.

4.6. Potential risks of Big Data and Artificial Intelligence

4.6.1. Data aggregation and maximization

Since Big Data lives on processing of large and growing datasets, the principle of data minimization as set forth in GDPR Article 5 (1) lit. c may well be affected since Big Data is about turning volume to value.[355] Fact is that more and more data is being generated and processed: 2.5 quintillion bytes of data are created each day, and that pace is accelerating with the growth of the Internet of Things.[356] Big Data and AI are on the rise: 77 percent of the devices we use today feature one form of AI or another; owing to AI, global GDP may grow to $ 15 trillion by 2030 and the overall AI market is expected to be almost

[353] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics, Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[354] Lisa Sokol and Jeff Jonas: Data finds data in: Beautiful Data – the stories behind elegant data solutions, published July 27 2009, available at https://jeffjonas.typepad.com/jeff_jonas/2009/07/data-finds-data.html. Retrieved September 26, 2021.

[355] Nikolaus Fargo, Stefanie Hänold, Benjamin Schütze: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Fargo (eds.): New Technology, Big Data and the Law: Springer Publishing 2017, p. 21.

[356] Bernard Marr: How much data do we create every day? The Mind-Blowing Stats Everyone Should Read. Article published on May 21, 2018, available at https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2152235f60ba. Retrieved October 22, 2021.

$ 60 billion by 2025.[357] In the next ten years, almost 70 percent of all companies will adopt at least one type of AI.[358] AI's potential is so broad that some speak of it as the fourth industrial revolution.[359]

4.6.2. Secondary use and use of collateral data

(Compatible) reuse of personal data is admissible[360] to the extent the conditions of GDPR Article 6 (4) are met,[361] i.e. considering the nature of the data in question, the context in which the data were collected, the relationship between the purposes for which the data have been collected and the purposes of further processing, the impact of the envisaged data processing on the data subjects, and the safeguards applied by the controller. Since a major characteristic of many AI applications is a certain degree of autonomy with systems being able to perform in an unsupervised manner, it is questionable whether such data processing operations meet all these requirements. Another problem of Big Data applications is that, quite often, external data are processed.[362] The upload of address books to social media platforms is a simple, but good example of this risk: whenever a user uploads his individual contacts to a social media platform, the platform receives a full set of contact data, and the concerned individuals behind those data do not know anything about this, not to mention that they never consented to such information sharing. This type of data processing is not transparent and can hardly be considered lawful: it is true that users upload the data; the platform was not actively collecting or harvesting data, but the platform as the controller acted as an enabler since it was the platform which implemented and activated the corresponding functionality – while another useful feature, (at least) information of concerned data subjects through communication channels the platform can dispose of, is not a default. However, some platforms used e-mail addresses which were uploaded by other users for other (own) purposes, which

[357] Background information is provided by Techjury: AI Statistics About Smarter Machines on January 28 2019, available at https://techjury.net/stats-about/ai/. Retrieved October 22, 2021.

[358] McKinsey Global Institute: Notes from the AI Frontier – Modeling the Impact of AI on the World Economy. Paper published September 2018, available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx. Retrieved October 22, 2021.

[359] EDPS: EU Guidelines on Ethics in Artificial Intelligence, p. 2, published September 2019, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf, Retrieved October 22, 2021.

[360] Article 6 of the former EU Data Protection Directive was also stressing compatibility, and according to the United Nations Guidelines Concerning Computerized Personal Data Files, personal data collected must remain relevant and adequate to the purposes specified at the time the data was collected. The Guidelines are available at https://www.refworld.org/pdfid/3ddcafaac.pdf. Retrieved October 22, 2021.

[361] The Directive on open data and the re-use of public sector information provides the legal framework for government-held data (public sector information), available at https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information. Retrieved October 22, 2021.

[362] Jay Choi, Doh-Shin Jeon, Byung-Cheol Kim: Privacy and personal data collection with information externalities. Journal of Public Economics 2019, vol. 173, pp. 113-124, available at https://www.sciencedirect.com/science/article/abs/pii/S0047272719300131.

courts considered to be illegal advertising.[363] Mergers & acquisitions are also a typical example of how companies may end up breaching data protection[364] (and / or consumer protection, competition or anti-trust) laws.

4.6.3. Opaqueness

One problem in the field of AI is that quite often, important parameters are unknown, e.g., details of the processing, the decisive (set of) operators behind the algorithm, etc. Some argue that there are three distinct types of opaqueness which can be distinguished:[365] intentional opacity when the inner workings of the system are deliberately concealed; illiterate opacity when the inner workings are opaque since only those with expert knowledge understand how it works; intrinsic opacity due to a fundamental mismatch between how humans and how algorithms understand the world. The ability of AI to act autonomously and in unforeseeable ways adds to the fear that decisions about individuals may made by a "Kafkaesque system of unreviewable decision-makers".[366] Another imminent problem is that the outcome of AI applications is often based on statistical correlations, not causality, and that is why some believe that AI shall attempt to identify causal relationships.[367] However, some companies engage in the "fight against black box algorithms"[368] with a new set of open source software to help understand how Artificial Intelligence is making decisions.

[363] On January 14, 2016, the German Federal Supreme Court has ruled that the "find friends" feature of Facebook, which is also used to email people who are not registered on Facebook, constitutes unlawful (harassing) advertising: decision Az. I ZR 65/1, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=73328&linked=pm. Retrieved October 22, 2021.

[364] As regards the transfer of data from WhatsApp to Facebook, the administrative court in Hamburg ruled that Facebook Germany must not use personal information from WhatsApp users, see Peter Sayer: German court upholds WhatsApp-Facebook data transfer ban. Article published April 26 2017, available at https://www.computerworld.com/article/3192613/german-court-upholds-whatsapp-facebook-data-transfer-ban.html. M&As have already been subject to national fines: press release of the Bavarian SA published August 30 2015, available at https://www.lda.bayern.de/media/pm2015_10.pdf. Retrieved October 22, 2021.

[365] Jenna Burrell How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society 2016, pp. 1-12, available at https://doi.org/10.1177/2053951715622512. Retrieved October 22, 2021.

[366] Neil Richards and Jonathan King: Three paradoxes of Big Data, Stanford Law Review Online 2013, vol. 66:41, p. 42, available at http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data (Retrieved October 22, 2021). The autors quote Daniel Solove who uses the term Kafkaesque in his book "The digital person: technology and privacy in the information age". New York University Press 2004.

[367] Matt Kusner, Joshua Loftus, Chris Russell, Ricardo Silva: Counterfactual fairness, presented and published at the 31st Conference on Neural Information Processing Systems (NIPS 2017), available at https://papers.nips.cc/paper/6995-counterfactual-fairness.pdf. Retrieved October 22, 2021.

[368] IBM introduced a "Fairness 360 Kit" to help AI developers to see inside their AI creations via a set of dashboards: Introducing AI Fairness 360, published in IBM's Research Blog on September 19 2018, available at https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/. Retrieved October 22, 2021.

4.6.4. Human oversight

A variety of factors contribute to the problem that human oversight is an issue in the framework of Big Data, ADM, and AI applications: the specialty about AI is that systems are able to autonomously perform certain tasks to achieve specific goals,[369] that they can recognize meanings by extracting characteristics and patterns[370] and learn (and teach) themselves without being programmed in a specific way. Processing operations may therefore lead to decisions which are opaque since they lack transparency and reproducibility, and that also questions the fairness and reliability of results which may be incorrect or even inappropriate (biased). If data is merged from various datasets, traceability is yet another issue to consider which conflicts with controllers' accountability.[371] A worst case scenario would be that unknown (secret) processing takes place and that the controller lost control or is simply not aware of what is going on. The fact that many services are outsourced to a multitude of specialized vendors further contributes to the potential risk that human oversight may be threatened; in many cases, it may therefore be difficult to define the true operators.

4.6.5. Information mismatch

Companies must be transparent about the processing of personal data,[372] but they are not obliged to provide detailed information about the data processing. For example, GDPR Article 13 (2) lit. f limits the transparency obligation to information about "the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". Details about the significance as well as envisaged consequences of the processing are relative insofar as dynamic processing may perhaps not allow for foreseeing all relevant consequences.[373] Details about the underlying logic are relative insofar as meaningful information is not the same as comprehensibility or reproducibility of decisions and insofar as businesses may refer to

[369] European Commission's 2018 factsheet on Artificial Intelligence, available at https://ec.europa.eu/digital-.single-market/en/artificial-intelligence. Retrieved October 23, 2021.

[370] Isha Salian: SuperVize Me: What's the difference between supervised, unsupervised, semi-supervised and reinforcement learning? Article published on August 2, 2018, available at https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/. Retrieved October 23, 2021.

[371] See GDPR Article 5 (2).

[372] See GDPR Article 12, 13, 14. See also the new California Consumer Privacy Act (CCPA), which creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. Background information on CCPA can be found on the website of the State of California Department of Justice, Office of the Attorney General at https://oag.ca.gov/privacy/ccpa. Retrieved October 23, 2021.

[373] Whenever processing operations are subject to ongoing change, data protection risk assessments will be an on-going process, and not a one-time exercise, Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679 (WP 248), p. 13.

trade secrets in order not to disclose underlying algorithms they use.[374] Another point that adds to the mismatch is the dilemma of information asymmetry between users and (Internet) service providers.[375] Information requirements are not only common to European law but are also part of so-called Fair Information Practice Principles (FIPP) which have been adopted in many US-laws.[376] FIPPs and many other privacy frameworks[377] have in common that individuals must be able to know which information is held about them and correct records of personal information if need be. Even if lack of transparency is not the problem, transparency as such is problematic since the ineffectiveness of transparency requirements seems to be proven by now: people are as badly informed as they are overtaxed with long and complex privacy notices;[378] people routinely turn over their data for small benefits;[379] people care much more about price-sensitive information than about data protection information;[380] people are much more concerned about social privacy than about institutional privacy,[381] and if people are about to decide about their privacy preferences, they tend to make their lives easy and accept all default settings[382] rather than taking their time to really comprehend and decide on relevant settings.

4.6.6. Privacy self-management

Lack of transparency is also related to data subject rights: there is good reason why GDPR Article 12 covers both, transparent information, and modalities for the exercise of data subject rights, because being aware who holds which data is a prerequisite for exercising individual rights. GDPR stresses the right

[374] German SCHUFA, one of the countries' leading credit agencies that bases its decisions on scoring successfully filed a law suit: the German Federal High Court of Justice ruled in 2014 that SCHUFA cannot be forced to explain in detail how scores are determined: Gerrit Hornung reports on the decision in his article: Datenverarbeitung der Mächtigen bleibt intransparent. Article published January 19 2014, available at https://www.lto.de/recht/hintergruende/h/bgh-urteil-vizr15613-schufa-scoring-ermittlung-kreditwuerdigkeit-algorithmus-geschaeftsgeheimnis-auskunft/. Retrieved October 23, 2021.

[375] Masooda Bashir, Carol Hayes, April Lambert, Jay Kesan: Online privacy and informed consent: The dilemma of information asymmetry. Proceedings of the Association for Information Science and Technology 2015, vol. 52, issue 1, pp. 1-10, available at https://doi.org/10.1002/pra2.2015.145052010043. Retrieved October 23, 2021.

[376] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[377] For example Paragraph 12 and 13 of OECD's Privacy Guidelines, available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf or Principle 23 of APEC's Privacy Framework, available at https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework. Retrieved October 23, 2021.

[378] Fred Cate, Viktor Mayer-Schönberger: Notice and consent in a world of Big Data. International Data Privacy Law 2013, vol. 3, no. 2, p. 67.

[379] Daniel Solove: Introduction: privacy self-management and the consent dilemma. Harvard Law Review 2013, vol. 126:1880, p. 1886.

[380] Daniel Solove: Introduction: privacy self-management and the consent dilemma. Harvard Law Review 2013, vol. 126:1880, p. 1898.

[381] Alison Young, Anabel Quan-Haase: Privacy protection strategies on Facebook – the Internet privacy paradox revisited, Information, Communication & Society 2013, p. 201.

[382] Lokke Moerel summarizes situations in which people are least likely to make good choices in: Big Data protection – how to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, p. 48, available at https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf. Retrieved October 23, 2021.

to information in the framework of multi-purpose processing since GDPR Article 13 (3) requires that individuals be (repeatedly) informed if the controller “intends to further process personal data for a purpose other than that for which the personal data were collected”. A draft version of the ePrivacy Regulation pursues the same goal by introducing the duty to remind users of their right to withdraw their consent unless users decide not to receive such reminders.[383] The idea of privacy self-management has been further developed into a fundamental right that is also known as “informational self-determination”: In Germany for example, the federal constitutional court dealt with a case regarding the collection of personal information during the 1983 census, and whether or not individuals shall determine the collection, storage, use or disclosure of their data.[384] In this decision, the court introduced the concept of “informational self-determination” for the first time. This concept deals with the right to a private life, and the protection of privacy and personal data.[385]

4.6.7. Potential for manipulation and addiction

Connected to the problem of privacy self-management is the potential for manipulation and addiction[386] which may reduce (risk-)awareness and this way, further reinforce loss of control.[387] While people are aware that companies have a strong interest to make their products and services attractive, many people may not be aware that certain apps take advantage of psychological patterns:[388] so-called behavioral engineering consists of features like a never-ending stream of irresistible content, gamification that encourages users to contribute their own content, infinite scroll that ensures users never break their attention, or real-time information that results in a constant fear of missing out.[389] Applications may be designed in a manner that can lead to digital addiction, a serious phenomenon that caught the World Health Organization’s attention since it may result in the inability to manage time, attention, and

[383] Kristof Van Quathem: New draft ePrivacy regulation released. Article published October 14, 2019, available at https://www.insideprivacy.com/international/european-union/new-draft-eprivacy-regulation-released/. Retrieved October 23, 2021.

[384] Census ruling of the German Federal Constitutional Court dated December 15 1983, available at https://openjur.de/u/268440.html. Retrieved September 25, 2021.

[385] Details on the concept of informational self-determination are provided by Wilhelm Steinmüller: Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann. Recht der Datenverarbeitung 2007, pp. 158-161.

[386] Hilary Andersson: Social media apps are deliberately addictive to users. Article published July 4 2018, available at https://www.bbc.com/news/technology-44640959. Retrieved July 25, 2022.

[387] Sometimes even to the point of addiction, see Jan-Keno Janssen, Sylvester Tremmel: Die Psycho-Tricks der App-Entwickler. Article published October 15 2019, available at https://www.heise.de/ct/artikel/Die-Psycho-Tricks-der-App-Entwickler-4547123.html?seite=all. Retrieved October 23, 2021.

[388] Nancy Cheever, Larry Rosenblatt, Mark Carrier and Amber Chavez: Out of sight is not out of mind: The impact of restricting wireless mobile device use on anxiety levels among low, moderate and high users. Computers in Human Behavior 2014, vol. 37, pp. 290-297.

[389] Kalev Leetaru: Why do we blame social media instead of blaming us? Article published April 21 2019, available at https://www.forbes.com/sites/kalevleetaru/2019/04/21/why-do-we-blame-social-media-for-being-addictive-instead-of-ourselves/. Retrieved July 25, 2022.

energy.[390] Moreover, research on pathological Internet use shows that digital addiction often leads to anxiety, depression,[391] and loneliness – a problem that should not be underestimated as the lack of real life contacts up to complete social isolation already became a mass phenomenon, an epidemic[392] with its own name in some countries,[393] and its own ministry in others[394] – because it was identified as a serious risk for public health. It is therefore questionable whether it is fair to say that individuals make a conscious choice to spend a lot of time on social media.[395] Last, but not least, the lack of (pay-per-view) fees shows that there is no financial incentive to minimize the amount of time people spend on social platforms, and that the collection of personal information provided and / or generated by users may serve as the basis for the monetization of individuals' behaviors.[396] Given the implications for consumer privacy, various laws have been enacted to address the potential for manipulation by explicitly prohibiting manipulative design, mostly with a focus on consent: if consent is obtained through manipulation, it is neither informed nor freely-given.[397]

4.6.8. Increase of paradoxes

There is much enthusiasm around Big Data as it is believed to be a powerful tool which enables detailed insight into many different economically valuable aspects of life. However, this seems to be only true for Big Data users since Big Data applications, pools and sensors are predominantly in the hands of powerful intermediary institutions, meaning that large corporate entities[398] are privileged at the expense

[390] Birgitta Dresp-Langley, Axel Hutt: Digital addiction and sleep. Article published June 5 2022, available at https://pubmed.ncbi.nlm.nih.gov/35682491/#:~:text=In%202020%2C%20the%20World%20Health%20Organization%20formally%20recognized,produce%20disturbed%20sleep%20patterns%20or%20insomnia%20during%20nighttime. Retrieved July 25, 2022.

[391] Erik Peper, Richard Harvey: Digital Addiction – increased loneliness, anxiety, and depression. Article published March 30 2018, available at https://www.neuroregulation.org/article/view/18189. Retrieved July 25, 2022.

[392] Alexander Voiskunsky, Galilna Soldatova: The loneliness epidemic in the digital society: Hikikomori as a cultural and psychological phenomenon. Journal for Consultative Psychology and Psychotherapy 2019, vol. 27, no. 3, pp. 22-43. An English translation of the article is available at https://translated.turbopages.org/proxy_u/ru-en.ru.01322d87-62e6acea-b532bfdd-74722d776562/https/psyjournals.ru/files/108495/cpp_2019_n3_Voiskunskii_Soldatova.pdf. Retrieved July 25, 2022.

[393] Mihai Andrei: Japanese phenomenon of extreme social isolation – and why it seems to be spreading. Article published January 22 2021, available at https://www.zmescience.com/science/hikikomori-loneliness/. Retrieved July 25, 2022.

[394] UK government press release: Prime Minister Theresa May launches government's first loneliness strategy. Press release published October 15 2018, available at https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users. Retrieved July 30, 2022.

[395] Kalev Leetaru: Why do we blame social media instead of blaming us? Article published April 21 2019, available at https://www.forbes.com/sites/kalevleetaru/2019/04/21/why-do-we-blame-social-media-for-being-addictive-instead-of-ourselves/. Retrieved July 25, 2022.

[396] See Shoshanna Zuboff's book: The age of surveillance capitalism – the fight for human future at the new frontier of power. Profile Books 2019.

[397] Felicity Slater: The future of manipulative design regulation. Article published January 19 2022, available at https://fpf.org/blog/the-future-of-manipulative-design-regulation/. Retrieved January 20, 2022.

[398] Or governments: For instance, the Syrian government lifted restrictions on the usage of Facebook, Twitter, and the like only to secretly profile, track, or even round up dissidents, see Stephan Faris: The hackers of

of individuals.[399] This "power paradox" is accompanied by the "transparency paradox": Big Data lives on small data inputs which, when viewed in isolation, appear unimportant and unsuspicious. The problem is that especially online data collection is much more far reaching and much more detailed than users would expect, and that underlying tools and techniques that are used for decision-making are opaque.[400] Therefore, some compare interactions with Big Data platforms with a poker game "where one of the players has his hand open and the other keeps his cards close".[401] Transparency is a topic GDPR explicitly stresses,[402] but transparency and consent seem to be an unfortunate issue since privacy self-management in many instances is about a take-it-or-leave-it-approach[403] or a mere click-mechanism.[404] Even though the EDPB[405] and the Court of Justice of the European Union clarified some questions regarding the use of cookies,[406] the ePrivacy Regulation is yet to come[407] so that there is still a lack of clarity with regard to consent requirements.[408] The described phenomenon is summarized under the term "control paradox" which also deals with the problem that affording more control to users does not help them to better protect their privacy.[409] The opposite effect is true:[410] not only does affording more control to users not lead to better protection of their data – this may even induce them to reveal

Damascus. Article published November 14 2012, available at http://www.businessweek.com/articles/2012-11-15/the-hackers-of-damascus. Retrieved October 23, 2021.

[399] Some authors call this the power paradox, see Neil Richards and Jonathan King: Three paradoxes of Big Data. Stanford Law Review 2013, vol. 66:41, p. 44, available at http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data. Retrieved October 23, 2021.

[400] Cookie information practices are a prominent example: often available, but rarely meaningful.

[401] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[402] See GDPR Article 5 (1) lit. a.

[403] Giovanni Buttarelli: We need to talk about terms and conditions. Article published April 29 2019, available at https://edps.europa.eu/press-publications/press-news/blog/we-need-talk-about-terms-and-conditions_en. Retrieved October 23, 2021.

[404] Daniel Solove discussed the issue in his publication: Privacy Self-Management and the Consent Dilemma. Harvard Law Review 2013, pp. 1880-1903.

[405] In addition, the EDPB adopted a letter in reply to letters calling for a consistent interpretation of cookie consent on January 19 2022, available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-french-associations-cookie-consent-requirement_en. Retrieved February 20, 2022.

[406] The court ruled that storing cookies requires Internet users' active consent. The corresponding press release no. 125/19 dated October 1 2029 is available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf. Retrieved October 23, 2021.

[407] Nicloas Herrmann: ePrivacy-Verordnung in der Krise – Die Suche nach einem Plan B. Article published November 25 2019, available at https://www.datenschutzbeauftragter-info.de/eprivacy-verordnung-in-der-krise-die-suche-nach-einem-plan-b/. Retrieved October 23, 2021.

[408] The draft ePrivacy Regulation faced much criticism: Ingo Dachwitz and Alexander Fanta: EU-Staaten wollen Verlagen einen Blankoscheck für Online-Tracking gewähren. The article provides background information on the draft ePrivacy regulation. Article published November 18 2019, available at https://netzpolitik.org/2019/eu-staaten-wollen-verlagen-einen-blankoscheck-fuer-online-tracking-gewaehren/. Retrieved October 23, 2021.

[409] Lokke Moerel: Big Data protection: How to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, p. 43, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[410] Susanne Barth, Menno de Jong: The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior: a systematic literature review. Journal of Telematics and Informatics, vol. 34, issue 7, pp. 1038-1058.

more sensitive information: if people feel that they have control over their data, they tend to provide more data about themselves.[411] Similar effects are known from other fields, e.g., in the framework of the introduction of the safety belt legislation: people felt more secure with safety belts and drove less carefully.[412] Another effect may be described as the "trust paradox": people are nowadays so used to relying on all kinds of Apps as "single source of truth" that they there does not seem to be any more room left for own decision making,[413] and that has a direct impact on how we deal with both, our own responsibility and others' trustworthiness in the event that an App's decision is challenged. The control paradox goes hand in hand with the so-called "security paradox":[414] data protection and data security are inseparable, and that is why security measures such as access controls are principally indispensable from both, a controller and user perspective. But any such measures require the processing of log-in data, and the general risk is that the more data are processed, the larger the risks that data are somehow compromised. Depending on the case, only name and password are required, but more and more often, users are required to provide a fingerprint in the framework of the authentication process, and that may lead to severe risks: nowadays many devices require the use of biometric data,[415] but the problem is that, unlike a password, there is no reset process for a unique fingerprint, and what is worse: such data can be manipulated very easily.[416] For instance, access to a used object is sufficient to reproduce a fingerprint, and if fingerprints are a mandatory part of official ID-documents,[417] then the individual concerned has a serious problem when such data is abused. Consequently, supposed security mechanisms themselves may lead to further risks. Even the COVID-19-pandemic is an example of such potential paradoxes when people "give up private information (… and) weigh up the costs and benefits in a "Privacy Calculus"."[418] The paradox at implementation level is that, even if stakeholders are

[411] Laura Brandimarte, Alessandro Acquisti, George Loewenstein: Misplaced confidences – Privacy and the control paradox. Article published August 9 2012, available at http://www.futureofprivacy.org/wpcontent/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf. Retrieved October 23, 2021.

[412] Wiel Janssen: Seat-belt wearing and driving behavior – an instrumented-vehicle study. Accident Analysis and Prevention 1994, vol. 26, issue 2, p. 261. A summary of the study is available at http://www.ncbi.nlm.nih.gov/pubmed/8198694?dopt=Abstract. Retrieved October 23, 2021.

[413] Steven Tanimoto writes about how the loss of user responsibility is linked to users getting lazy and losing own problem-solving capacities when they trust "system judgments" in his 2010 book: The elements of Artificial Intelligence. Computer Science Press 2010, p. 478.

[414] Lokke Moerel: Big Data protection: How to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, p. 43, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[415] Given the sensitivity of biometric data and the insufficiency of investigating alternatives, the Amsterdam District Court ruled that a company cannot require its employees to log in to the cash register system through fingerprint scanners. Decision published August 15 2019, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005. Retrieved October 23, 2021.

[416] An election poster of former German chancellor Dr. Angela Merkel was enough to present how easily an iris scan can be manipulated, see Stefan Krempl: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck. Article published December 28 2014, available at https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html. Retrieved October 23, 2021.

[417] The EU Commission proposed making fingerprints mandatory in ID cards, see Nicole Goebel: All EU ID cards to include fingerprints. Article published April 16 2018, available at https://www.dw.com/en/all-eu-id-cards-to-include-fingerprints-eu-commissioner/a-43401789. Retrieved October 23, 2021.

[418] Paul Garrett et al: Privacy and health: the lesson of COVID-19. Article published

determined to comply with privacy standards, the introduction of an AI system may lead to privacy problems since there is a risk for potential trade-offs between different data protection principles. In this regard, the UK's Information Commissioner's Office[419] explains that such tensions may arise between accuracy and fairness vs. privacy, and fairness vs. accuracy as well as explicability vs. accuracy and security, e.g., more data may lead to more accuracy, but at the expense of individual's privacy; if AI is tailored to avoid discrimination (if certain indicators are removed to that AI is fair), this may have an impact on accuracy; if AI is tested to see if it may be discriminatory, it needs to be tested by using data that is labeled by protected characteristics, but that may be restricted under privacy laws that govern the processing of special category data; providing detailed explanations about the underlying logic of complex AI systems may lead to disclosure of information that can be used to infer private information about the individuals whose personal data was used to build the AI system.

4.6.9. (Re-)Identification and identity

Even though one single piece of information may not very telling,[420] combined datasets tell more about the person and enable to form a picture of the individual; therefore, aggregated information can reveal new facts about a person the individual did not expect to be known when the original (isolated) data was collected.[421] It is frightening to see how little information is needed to associate information to an individual: a study of credit card records showed that only four spatiotemporal points are enough to uniquely re-identify 90 percent of individuals and that knowing the price of the underlying transaction increases the risk of re-identification by 22 percent.[422] Identification of a person is not necessarily a risk, but if one thinks of the importance of the protection of witnesses[423] and whistleblowers[424] and the relevance of anonymous speech,[425] this shows that the issue of identification may be linked to fundamental rights. The predictive nature of Big Data applications may lead to individuals being identified, and the trouble in this regard is that individuals face difficulties to control the access and use

February 4 2021, available at https://pursuit.unimelb.edu.au/articles/privacy-and-health-the-lessons-of-covid-19. Retrieved October 23, 2021.

[419] Reuben Binns, Valeria Gallo: Trade-offs. Article published July 25 2019, available at https://ico.org.uk/about-the-ico/news-and-events/ai-blog-trade-offs/. Retrieved October 23, 2021.

[420] The Clearview case has already proven the opposite: the App can identify individuals based on a single photo, see Jannis Brühl and Simon Hurtz: Eine Software schockiert Amerika. Article published January 20 2020, available at https://www.sueddeutsche.de/digital/gesichtserkennung-clearview-app-polizei-gesicht-1.4764389. Retrieved October 23, 2021.

[421] Daniel Solove: Understanding Privacy, p. 118. Harvard University Press 2008.

[422] Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex Pentland: Unique in the shopping mall: On the re-identifiability of credit card metadata, Science 2015, vol. 347, issue 6221, pp. 536-539.

[423] And the related right not to incriminate oneself, a generally recognized international standard which is key part of a fair procedure: https://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf. Retrieved October 23, 2021.

[424] The Council of the European Union adapted new rules for the protection of whistleblowers. Press release published October 7 2019 and is available at https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/better-protection-of-whistle-blowers-new-eu-wide-rules-to-kick-in-in-2021/ (Retrieved October 23, 2021). Member states will have two years to transpose the new rules into their national law.

[425] Daniel Solove: Understanding Privacy, p. 125. Harvard University Press 2008.

of their personal data and that they thus do not have sufficient autonomy to determine, maintain and develop their identity.[426] Big Data and AI can make individuals' identities potentially more vulnerable, simply because more and more data is available, shared with service providers around the world, and stored in various tools – and any of these systems could be hacked, which may, e.g., enable identity theft. Identity[427] theft is a growing issue since advances in digital technology have aggravated the problem. Identity threats and the potential for discrimination are interconnected: in many instances, individuals can neither know nor influence the outcome of evaluations in relation to their preferences, performance, or creditworthiness. Consequently, some authors address the problem[428] and some institutions call for a prohibition of so-called secret profiling.[429] The core problem is that the outcome of any such evaluation is based on correlations rather than causes,[430] and therefore, some speak about data protection as protection against probability.[431]

4.6.10. Potential for discrimination

The probabilistic nature of individual decision-making and profiling is highly desired, but their inherent opacity[432] together with their potential for discrimination[433] is problematic: price discrimination by online-shops is just one rather simple example,[434] which can be judged from various perspectives, from data protection and consumer protection up to competition law.[435] But there are far more examples of

[426] Jacques Bus, Carolyn Nguyen: Personal Data Management – A Structured Discussion in: Mireille Hildebrandt, Kieron O'Hara, Michael Waidner, eds.: The value of personal data, Digital Enlightenment Yearbook, IOS Press Amsterdam 2013, p. 272, available at https://www.academia.edu/6325541/Personal_Data_Management_A_Structured_Discussion. Retrieved October 23, 2021. Retrieved October 23, 2021.

[427] The term identity is used as a reference to the self and in the technical sense of the complete set of attributes that defines a person.

[428] Daniel Solove: Understanding Privacy, p.133. Harvard University Press 2008.

[429] For instance, the Universal Guidelines on AI issued 2018 by the Public Voice, available at https://thepublicvoice.org/ai-universal-guidelines/. Retrieved October 23, 2021.

[430] Mireille Hildebrandt: Slaves to Big Data. Or are we? Keynote during the 9th Annual Conference on Internet, Law & Politics on June 25 2013 in Barcelona, available at http://works.bepress.com/mireille_hildebrandt/52. Retrieved October 23, 2021.

[431] Lokke Moerel: Big Data protection: How to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, p. 43, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[432] Tal Zarsky: The Trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making. Science, Technology, & Human Values 2016, vol. 41(1), pp. 118-132, available at https://pdfs.semanticscholar.org/9b4d/bc901010a790d88c8be2370f8c9557895956.pdf?_ga=2.57485485.60694232.1562929501-1933874839.1562929501. Retrieved October 23, 2021.

[433] This problem was reviewed by the Article 29 Working Party in their 2017 guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 published August 22 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Retrieved October 23, 2021.

[434] Ira Rubinstein: Big Data: The end of privacy or a new beginning? International Data Privacy Law 2013, vol. 3, no. 2, p. 77. Rubinstein explores on more types of discrimination. Apart from price discrimination, he also discusses threats to autonomy and covert discrimination.

[435] Non-discrimination is a fundamental right according to Article 21 of the EU Charter of Fundamental Rights. The bill text is available at https://fra.europa.eu/en/charterpedia/article/21-non-discrimination. Retrieved October 23, 2021.

the potential for discrimination and bias in practice with a much greater impact on people's lives, and there are various forms of bias: from implicit bias (discrimination or prejudice against a person or group that is unconscious to the person with the bias, which is dangerous because the person is unaware of the bias) over sampling bias (a statistical problem where random data selected from the population do not reflect the distribution of the population), or temporal bias (when a machine-learning model works well at this time but fails in the future because certain factors / possible future changes had not been considered when building the model), over-fitting to training data (when the AI model can accurately predict values from the training dataset but cannot predict new data accurately), and edge cases and outliers (refers to data outside the boundaries of the training dataset).[436] Nowadays, employers are able to turn down job candidates based on social media information without providing candidates with an opportunity to comment on their findings: a study showed that a Meta profile is better at predicting job performance than an IQ test;[437] other examples are more severe, for example, biometric identification systems that lead to racial profiling:[438] as regards discrimination in the recruitment and / or employment context, it shall be noted that human rights provisions to protect individuals from discrimination exist,[439] for example: the International Covenant on Economic, Social and Cultural Rights,[440] the Revised European Social Charter,[441] the Additional Protocol to the American Convention on Human Rights,[442] or the African Charter on Human and Peoples' Rights.[443] Under the GDPR, any data subject has the right to request information and, under certain conditions, the right to object[444] "on grounds relating to his or her particular situation", but the key problem is that individuals unlike businesses do not dispose of enough information to defend themselves not just against the data processing as such (which may be legitimate under GDPR Article 6 (1) lit. f, but against "being sorted in the wrong bucket,"[445] resulting in individuals not succeeding at their jobs or their mortgage. And there are even more dramatic examples

[436] Background information is provided by the World Economic Forum: Research shows AI is often biased. Here's how to make algorithms work for all of us. Article published July 19 2021, available at https://www.weforum.org/agenda/2021/07/ai-machine-learning-bias-discrimination/. Retrieved July 30, 2022.

[437] Donald Klümper, Peter Rosen, Kevin Mossholder: Social networking websites, personality ratings and the organizational context - more than meets the eye? Journal of Applied Social Psychology 2012, vol. 42, issue 5, pp.1143-1172.

[438] Through a joint statement, various NGOs are calling on the European Union to ensure the AI Act, amongst other things, respects the rights of migrants, and prohibits certain AI systems. Background information on the initiative is available at AccessNow: EU AI Act must protect all people, regardless of migration status. Article published December 6 2022, available at https://www.accessnow.org/eu-ai-act-migration-status/. Retrieved January 7, 2023.

[439] Caragh Aylett-Bullock: Automating insecurity – decision making in recruitment. Article published March 13 2022, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment. Retrieved January 20, 2023.

[440] See ICESCR Article 6. The bill text is available at https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx. Retrieved January 22, 2023.

[441] The bill text is available at https://rm.coe.int/168007cf93. Retrieved January 20, 2023.

[442] The bill text is available at https://www.oas.org/juridico/english/treaties/a-52.html. Retrieved January 20, 2023.

[443] The bill text is available at https://www.achpr.org/legalinstruments/detail?id=49. Retrieved January 20, 2023.

[444] See GDPR Article 21 (1).

[445] Omer Tene: Privacy: For the rich or for the poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html. Retrieved October 23, 2021.

such as facial recognition bias,[446] bias in recidivism scoring systems,[447] bias in welfare[448] or bias in healthcare – detected years after the algorithm had been used.[449] The potential of information injustice and information inequality leads to the problem that the right to data protection does not help against certain risks and effects of the new economy.[450] Even if individual automated decision-making would be completely prohibited, this only refers to decisions which have been taken by tools and applications without any human intervention at all. Consequently, the 2019 expert opinion of the German Data Ethics Commission distinguishes between algorithm-based (suggestion-only), algorithm-driven (limited leeway) and fully automated decisions.[451]

4.6.11. Potential for surveillance

The potential for surveillance is another important factor to consider when AI technology is used.[452] Facial recognition is a prominent example in this context and a very sensitive topic;[453] the case of Clearview demonstrated how easy it is to identify[454] individuals. Owing to growing concerns from users and regulators even Meta, the company formerly known as Facebook, announced it will be putting an end to its face recognition system and delete more than 1 billion people's individual facial recognition

[446] National Institute of Standards and Technology: NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. Demographics study on face recognition algorithms could help improve future tools. Background information on the study has been published on December 19, 2019, available at https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Retrieved October 23, 2021.

[447] Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner: Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. Article published May 23 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Retrieved October 23, 2021.

[448] John Henley, Robert Booth: Welfare surveillance system violates human rights, Dutch court rules. Article published February 5 2020, available at https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules. Retrieved October 23, 2021.

[449] Heidi Ledford: Millions of black people affected by racial bias in health-care algorithms. Article published October 24 2019 (updated October 26 2019), available at https://www.nature.com/articles/d41586-019-03228-6. Retrieved October 23, 2021.

[450] Lokke Moerel: Big Data protection: How to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, p. 43, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[451] Expert opinion of the Data Ethics Commission of the German Federal Government's Ministry of the Interior, for Building and Home Affairs (Gutachten der Datenethikkommission der Bundesregierung) 2019, p. 24. Paper published October 12 2019, available at https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=3D63214EEC7EB10049F7C59E63B89F53.1_cid287?__blob=publicationFile&v=4. Retrieved October 23, 2021.

[452] FTC issued a report which also dealt with commercial surveillance. Report published June 2022, available at https://www.ftc.gov/reports/combatting-online-harms-through-innovation. Retrieved October 5, 2022.

[453] The EU had been considering a temporary ban in public places for up to five years until safeguards to mitigate the technology's risks are in place, see Anthony Spadafora: EU calls for five-year ban for facial recognition. Article published January 20 2020, available at https://www.techradar.com/news/eu-calls-for-five-year-ban-on-facial-recognition. Retrieved October 23, 2021.

[454] See the company statement on their website: "ClearView have built a reputation for meeting the stringent demands of police and law enforcement agencies", available at https://clearview-communications.com/products/law-enforcement. Retrieved October 23, 2021.

templates.[455] The fact that some countries introduced so-called social scoring that tracks and evaluates all aspects of life[456] shows the societal and political dimension such techniques may involve, and some fear that "AI technologies fit into wider systems of over-surveillance, criminalization, structural discrimination" with serious consequences for marginalized people and communities and vulnerable individuals.[457] Apart from obvious forms of surveillance like CCTV, other techniques may have much more impact on people's lives, but people are sometimes not really aware of that: the discussion around cookie consent[458] shed some light to the fact that tracking users' behavior is of economic interest, but there is little consciousness about the fact that a considerable part of today's digital economy is not simply about advertising, but about "surveillance capitalism", i.e., "using human experience as free raw material for translation into behavioral data and usage for hidden commercial practices,"[459] and the concentration of data[460] and knowledge may enforce surveillance powers. The fact that AI can not only be used for commercial practices, but for repression purposes led some to conclude that the surveillance industry is out of control because it is selling its products to human rights abusers.[461] The issue of is of such importance that organizations like Amnesty International who campaign against abuses of human rights[462] dealt with the topic:[463] the issue is to protect minorities, marginalized communities or victims of violence, discrimination, or patriarchal structures, which often applies to women[464] and particularly

[455] Salvador Rodriguez: Facebook plans to shut down its facial recognition program. Article published November 2 2021, available at https://www.cnbc.com/2021/11/02/facebook-will-shut-down-program-that-automatically-recognizes-people-in-photos-and-videos-delete-data.html#:~:text=Facebook%20on%20Tuesday%20announced%20it%20will%20be%20putting,recognition%20templates%20as%20a%20result%20of%20this%20change. Retrieved February 2, 2022.

[456] Nicole Kobie: The complicated truth about China's social credit system. Article published June 7 2019, available at https://www.wired.co.uk/article/china-social-credit-system-explained. Retrieved October 23, 2021.

[457] AccessNow provides background information on this topic: EU AI Act must protect all people, regardless of migration status. Article published December 6 2022, available at https://www.accessnow.org/eu-ai-act-migration-status/. Retrieved January 7, 2023.

[458] The latest draft of the ePrivacy Regulation was again rejected, see Jennifer Baker: How the ePrivacy Regulation talks failed ... again. Article published November 26 2019, available at https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/. Retrieved October 23, 2021.

[459] Shoshanna Zuboff: The age of surveillance capitalism – the fight for human future at the new frontier of power. Profile Books 2019.

[460] The German Facebook case showed that antitrust issues may be a factor to consider, however, the antitrust authority's ruling that social-media giant abused its dominance was reversed, see Sara Germano: Facebook Wins Appeal Against German Data-Collection Ban. Article published August 26 2019, available at https://www.wsj.com/articles/facebook-wins-appeal-against-german-data-collection-ban-11566835967. Retrieved October 23, 2021.

[461] Merel Koning: EU companies selling surveillance tools to China's human rights abusers. Article for Amnesty International published September 21 2020, available at https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/. Retrieved October 23, 2021.

[462] Amnesty International provides background information on secretive cyber surveillance on their website, available at https://www.amnesty.org/en/. Retrieved October 23, 2021.

[463] Amnesty International, Privacy International, and the Centre for Research on Multinational Corporations published a report "Operating from the shadows" in which they want to draw attention to the human rights risks of the global surveillance industry. Report published 2021, available at https://www.privacyinternational.org/sites/default/files/2021-06/DOC1041822021EN.pdf. Retrieved February 28, 2023.

[464] For example, to fight stalking or monitoring, or to protect individuals from violence.

women human rights defenders.[465] Therefore, the European Parliament and EU Member States started discussing agreements to toughen export rules for European tech companies that sell technology which could be used for espionage and surveillance.[466] However, some still believe that it is "misleading to assume that all applications of AI can be made compatible with European values, when some applications inherently threaten human rights."[467] What is worse, in many cases surveillance is not imposed on people, they buy into it willingly which some describe as the phenomenon of luxury surveillance:[468] people buy expensive tech products that enable "ambient intelligence,"[469] a technology where devices slip into the background but are "always on", meaning that they constantly collect (sensitive) information, or they buy expensive cars that are equipped with multiple internal cameras that allow for constant monitoring of their behavior and actions.[470]

4.6.12. Intrusion

Closely connected to the potential for surveillance is the risk of intrusion, and mobile health apps or virtual / augmented reality may serve as examples of this risk: It can generally be said that health and fitness apps are data-invasive[471] by nature, simply because the performance of such apps is dependent on good data quality, and this is inconceivable without the permanent collection of relevant, i.e., granular data. On the one hand, health applications may be truly beneficial for users by providing them with up-to-date information, analytics, and recommendations on their sleeping rhythm, blood pressure, glucose level, or weight loss progress. On the other hand, a lot of sensitive and intimate[472] information needs to be constantly processed to deliver these metrics. In the context of mobile health apps, the European

[465] Shmyla Khan: Surveillance as a feminist issue. Article published November 21 2017, available at https://www.privacyinternational.org/news-analysis/3376/surveillance-feminist-issue. Retrieved February 28, 2023.

[466] Laurens Cerulus: Europe to crack down on surveillance software exports. Article published October 15 2020, available at https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/. Retrieved October 23, 2021.

[467] AccessNow: Europe's approach to artificial intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 23, 2021.

[468] Chris Gilliard: The rise of luxury surveillance. Article published October 18 2022, available at https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/. Retrieved October 18, 2022.

[469] Wired reported on this topic at their website. Article published September 28 2022, available at https://www.wired.com/story/amazon-wants-to-cocoon-you-with-ambient-intelligence/. Retrieved October 18, 2022.

[470] Matthew Beedham: Why Tesla's in-car monitoring camera is a major privacy risk. Article published March 24 2021, available at https://thenextweb.com/news/teslas-driver-monitoring-cameras-privacy-risk. Retrieved October 18, 2022.

[471] Chris Stokel-Walker: The most data-invasive health and fitness apps. Article published May 13 2022, available at https://cybernews.com/privacy/the-most-data-invasive-health-and-fitness-apps/. Retrieved October 18, 2022.

[472] Lesley Fair: Health app broke its privacy promises by disclosing intimate details about users. Article published January 13 2021, available at https://www.ftc.gov/business-guidance/blog/2021/01/health-app-broke-its-privacy-promises-disclosing-intimate-details-about-users. Retrieved October 23, 2021.

Commission has been facilitating an industry-led Code of Conduct[473] with the objective of raising awareness, fostering users' trust in mHealth apps, and facilitating compliance with EU data protection rules. The code has been prepared against the background of the Commission's mobile health consultations which revealed that people often do not trust mobile health apps because of privacy concerns.[474] Given the psychological and physiological aspects of immersive technologies of virtual and augmented reality, some authors consider such technologies to have the potential for a completely new class of privacy-related harms: the Metaverse, a collective digital reality where users can interact that combines social media, augmented and virtual reality, online gaming, and cryptocurrencies,[475] may serve as an example in this regard. The massive collection of individuals' biometric data and behavioral information adds to the complexity of privacy challenges, because such data may pave the way to "connect your identity to your innermost thoughts, wants, and desires" and this way, be used for biometric psychography.[476] To some, this may sound like music of the future, however, applications like Neuralink[477] show that use cases of brain-machine interfaces in which humans do not need to talk any more, but can transmit their thoughts directly already exist. Some authors name this development the "artificialization of the human."[478]

4.6.13. Human Rights and democracy

The case of Cambridge Analytica is probably the best example of the political dimension[479] the use of Artificial Intelligence may have. The data mining company Cambridge Analytica had been hired in the 2016 presidential campaign in the U.S. and collected personal information of a large number of users

[473] The European Commission's Privacy Code of Conduct for mobile health applications consists of practical guidance on data protection principles for developers of mobile health apps, and covers the following topics: user's consent, data subjects' rights and information requirements, purpose limitation and data minimization, Privacy by Design and by Default, security measures, data retention and data transfers, use of personal data for secondary purposes, disclosing data to third parties for processing operations, principles on advertising in mHealth apps, personal data breach as well as data gathered from children. The code is available here: https://digital-strategy.ec.europa.eu/en/library/code-conduct-privacy-mhealth-apps-has-been-finalised. Retrieved December 29, 2022.

[474] Background information on the European Commission's consultations on mobile health applications, including the Green Paper on mobile health is available at the Commission's website https://digital-strategy.ec.europa.eu/en/library/green-paper-mobile-health-mhealth. Retrieved December 29, 2022.

[475] Jean Folger: What is the Metaverse? Article published July 6 2022, available at https://www.investopedia.com/metaverse-definition-5206578. Retrieved July 25, 2022.

[476] Brittan Heller coined the term in her article: Reimagining Reality – Human rights and immersive technology. Article published June 12 2020, available at https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology. Retrieved December 29, 2022.

[477] Background information on Neuralink is provided by Ernest Hamilton: The future of Neuralink: does it affect our private lives? Article published December 8 2020, available at https://www.sciencetimes.com/articles/28562/20201208/the-future-of-neuralink-does-it-affect-our-private-lives.htm. Retrieved December 29, 2022.

[478] Eric Fourneretis: The dangers of Musk's Neuralink. Article published April 1 2022, available at https://iai.tv/articles/the-dangers-of-musks-neuralink-auid-2092. Retrieved December 29, 2022.

[479] The issue is addressed in ICO's guidance for the use of personal data in political campaigning. Guidance published October 14 2022, available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/. Retrieved December 29, 2022.

and their extensive friend networks under false pretenses as a research-driven application.[480] Facebook transferred 87 million user profiles to Cambridge Analytica, which was one of the largest unlawful data transfers that resulted in investigations by lawmakers and regulators: Mark Zuckerberg, founder and CEO of Meta, had to testify publicly before Congress,[481] and Facebook agreed to pay $725 million to resolve a class-action lawsuit accusing the social media giant of allowing third parties, including Cambridge Analytica, to access users' personal information.[482] It is very problematic that AI may be exploited for manipulative purposes or to enhance operations that automate disinformation,[483] because people do not realize that troll factories may be used to manufacture specialized (dis-)information,[484] and that AI could be used to significantly influence voters and this way, the outcome of elections. The so-called BREXIT looks like an important precedent in this context, and Aggregate IQ is the example of yet another data company that played a crucial role in the Vote Leave's campaign – a fact that has been underlined by the chief strategist for Vote Leave.[485] Phenomena like fake news and hate speech show that it is worthwhile examining AI use cases from a human rights and democracy perspective. The impact of hate speech shall not be underestimated since millions of people use social media every day, and the constant repetition of hate news has the potential to serve as a fire accelerate and cause massive harm since: "When our environment consists of information that polarizes, that enrages, it leads to a loss of trust in each other. This version of Facebook is tearing our society apart and causing violence."[486]

[480] Background information on the case is available at the website of the Electronic Privacy Information Center https://epic.org/privacy/facebook/cambridge-analytica/. Retrieved October 23, 2021.

[481] Alfred Ng: Facebook's Mark Zuckerberg to appear before Senate and House committees to answer questions about privacy and user data. Article published April 4 2018, available at https://www.cnet.com/news/politics/mark-zuckerberg-will-testify-to-congress-on-april-11/. Retrieved December 29, 2022.

[482] Nate Raymond: Facebook parent Meta to settle Cambridge Analytica scandal case for $725 million. Article published December 23 2022, available at https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/. Retrieved December 29, 2022.

[483] Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi, Ido Wulkan: AI and the future of disinformation campaigns. Center for Security and Emerging Technology Policy brief published December 2021, available at https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/. Retrieved July 25, 2022. The report describes the stages and techniques used by human operators to build disinformation campaigns.

[484] Darren Linvill, Patrick Warren: Troll factories – Manufacturing specialized disinformation on Twitter. Article published February 5 2020, available at mhttps://www.tandfonline.com/doi/abs/10.1080/10584609.2020.1718257?journalCode=upcp20. Retrieved December 29, 2022.

[485] Background information on the Vote Leave campaign is provided by Carole Cadwalladr: Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica. Article published March 24 2018, available at https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions. Retrieved December 29, 2022.

[486] Frances Haugen: Facebook makes money with hate and anger. Headline of her interview with German television October 4 2021, available at https://www.tagesschau.de/ausland/amerika/facebook-whistleblowerin-101.html. Retrieved December 29, 2022.

Consequently, organizations like Human Rights Watch,[487] ARTICLE 19,[488] Amnesty International and AccessNow[489] as well as Data & Society[490] dealt with the analysis of AI and governance from a human rights standpoint and stressed the importance of political participation and freedom of expression. There is good reason why the issue of human rights is part of literally all national Artificial Intelligence strategies and either mentioned explicitly in the framework of the concept of trustworthy AI or referenced because "human rights are often assumed to form the foundation of policy whether or not it is explicitly stated".[491] At European level, various institutions dealt with human rights implications AI may have and issued corresponding papers, for example, the Council of Europe provided a recommendation regarding human rights impacts of algorithmic systems,[492] and a study on human rights dimensions of automated data processing techniques and possible regulatory implications.[493] In addition, the Council of Europe established an ad hoc Committee on Artificial Intelligence (Committee on Artificial Intelligence of the Council of Europe: CAHAI) whose mission is to engage in broad multi-stakeholder consultations to examine the feasibility of a legal framework for the development, design, and application of Artificial Intelligence, based on Council of Europe's standards on human rights, democracy, and the rule of law.[494] CAHAI's 2020 report[495] focused on the impact on AI various human-rights-related aspects embedded in ECHR such as liberty, security and fair trial,[496] private and family life as well as physical, psychological and moral integrity,[497] freedom of expression,[498] freedom of

[487] Human Rights Watch: UK – Automated benefits system failing people in need – the government's flawed Universal Credit Algorithm pushing people into poverty. Article published September 29 2020, available at https://www.hrw.org/news/2020/09/29/uk-automated-benefits-system-failing-people-need. Retrieved October 23, 2021.

[488] Details on privacy and freedom of expression in the age of Artificial Intelligence are provided by Article 19 on their website, available at https://www.article19.org/resources/privacy-freedom-expression-age-artificial-intelligence/. Retrieved October 23, 2021.

[489] Amnesty International and Access Now issued the "Toronto Declaration" in 2018 which is available at https://www.torontodeclaration.org/. Retrieved October 23, 2021.

[490] Mike Latonero: Governing Artificial Intelligence – upholding human rights & dignity. Paper for Data & Society published 2018, available at https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf. Retrieved October 23, 2021.

[491] Global Partners Digital: National Artificial Intelligence strategies and human rights: a review. Paper published April 15 2020, available at https://www.gp-digital.org/publication/national-artificial-intelligence-strategies-and-human-rights-a-review/. Retrieved October 23, 2021.

[492] The recommendation on human rights impacts of algorithmic systems was published April 8 2020, and is available at https://rm.coe.int/09000016809e1154. Retrieved October 23, 2021.

[493] The study on human rights dimensions of automated data processing techniques and possible regulatory implications was published December 2017, and is available at https://www.coe.int/en/web/freedom-expression/algorithms-and-human-rights#{%2234578668%22:[0]}. Retrieved October 23, 2021.

[494] AccessNow: Europe's approach to artificial intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 23, 2021.

[495] Catelijne Muller: The impact of Artificial Intelligence on human rights, democracy, and the rule of law. Report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Paper published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 23, 2021.

[496] ECHR Art. 5 and 6.

[497] ECHR Art. 8.

[498] ECHR Art. 10.

assembly and association[499] as well as prohibition of discrimination.[500] CAHAI's report also dealt with red lines such as AI-enabled (personal, physical or mental) tracking, assessment, profiling, scoring or nudging through biometric or behavior recognition, AI-powered mass surveillance, Deep Fakes and human-AI interfaces. It also addresses potential new human rights and the need for:

- *"A right to human autonomy, agency, and oversight over AI,*
- *A strengthened right to privacy to protect against AI-driven mass surveillance,*
- *A separate right to physical, psychological, and moral integrity in light of AI profiling*
- *Adapting the right to data privacy to protect against indiscriminate, society-wide online tracking of individuals, using personal and non-personal data (which often serves as a proxy for personal identification)*
- *A right to transparency / explainability of AI outcomes including the right to an explanation of how the AI functions, what logic it follows, and how its use affects the interests of the individual concerned, even if the AI-system does not process personal data, in which case there is already a right to such information under GDPR."*

While banal at first glance, even seemingly simple use cases like an online search show that the use of AI can have an impact on the freedom of information: if Artificial Intelligence is tailored and trained to provide suitable suggestions, that may on the one hand help pursue with the online research, but on the other hand, certain results may be disregard, and this way, important information could be withhold.

Today's AI is so advanced that it has become impossible to distinguish human-generated from AI-generated content: "indistinguishability" has become the benchmark for positive AI performance since the Turing test, and that is why many authors stress the ethical need for more transparency, for example, by adding mandatory watermarks in machine-generated language,[501] which is believed to be a helpful step in the fight against manipulation – and already incorporated in some laws, for example, Canada,[502] or China.[503] In the event that Artificial Intelligence is used in a manipulative manner, that may have a political dimension, for example in the context of persuasion (e.g., creation of targeted propaganda) or deception (e.g., manipulation of videos) or analysis (e.g., evaluation of human behavior, moods and

[499] ECHR Art. 11.

[500] ECHR Art. 14, protocol 12.

[501] Connor Wright: The ethical need for watermarks in machine-generated language. Article published November 27 2022, available at https://montrealethics.ai/the-ethical-need-for-watermarks-in-machine-generated-language/?utm_source=substack&utm_medium=email. Retrieved January 10, 2023.

[502] For example, California's new bot law that prohibits the use of undeclared bots. The law became operative on July 1, 2022, and is available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001. Retrieved January 10, 2023.

[503] China's new law on Deep Fakes came into force in January 2023, see Arjun Kharpal: China is about to get tougher on deepfakes in an unprecedented way. Here's what the rules mean. Article published December 22 2022, available at https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html#:~:text=In%20January%2C%20China%20will%20introduce,the%20dissemination%20of%20fake%20news. Retrieved January 10, 2023.

beliefs) and may thus undermine the ability of democracies to sustain truthful public debates.[504] This is not only true for totalitarian regimes, any state and any political party nowadays can take advantage of using AI for elections to maximize the effectiveness of email or social media campaigns.[505] Voter influencing is core of every electoral campaign, but "well-functioning democracies require a well-informed citizenry, an open social and political discourse and absence of opaque voter influence."[506] Against this background, one of the pioneers of data privacy concluded that "we have come to realize that how well democracies balance the competing demands of privacy, disclosure, and surveillance will exert a major influence on the quality of civic life in the 21st century, and that shaping this balance will now have to be done in the context of continuing terrorist threats and actions. In short, privacy is a quality-of-life topic worth the best scholarship, thoughtful advocacy, and continuing attention of us all."[507]

4.6.14. Socio-economic impacts

The debate on the impact of Artificial Intelligence on the economy in general and employment in specific and how Big Data and AI applications will influence and change the job market[508] are already going on for a long time. Since AI helps with the transformation of businesses, AI will necessarily also have an impact on workforce: we have come to a point where not only monotonous tasks in production lines and factories or activities related to customer care can be automated, complex operations can be automated as well – even the legal profession may be severely impacted by this new kind of virtual workforce, because duties like document classification, summarization, comparison, knowledge extraction, discovery and retrieval are more and more based on technology and automation, and less on

[504] Miles Brundage et al: The malicious use of Artificial Intelligence: forecasting, prevention, and mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

[505] Manu Siddharth Jha: Want to win an election? Use AI and Machine Learning. Article published April 23 2020, available at https://www.mygreatlearning.com/blog/how-ai-and-machine-learning-can-win-elections/#:~:text=Artificial%20Intelligence%20for%20the%20Benefit%20of%20the%20Voter,help%20them%20make%20up%20their%20minds%20about%20candidates. Retrieved October 24, 2021.

[506] Catelijne Muller: The impact of Artificial Intelligence on human rights, democracy, and the rule of law. Report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Report published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 24, 2021.

[507] Alan Westin: Social and Political Dimensions of Privacy. Journal of Social Issues 2003, vol. 59, no. 2, 2003, pp. 431-453, available at https://www.sfu.ca/~palys/Westin-2003-Social&PoliticalDimensionsOfPrivacy.pdf. Retrieved October 24, 2021.

[508] Dennis Späth: Artificial Intelligence is transforming the workforce as we know it. Article published March 18 2019, available at https://workplaceinsight.net/artificial-intelligence-is-transforming-the-workforce-as-we-know-it/. Retrieved October 24, 2021.

human work.[509] That is why some raise concerns regarding AI in the employment context[510] or started discussing unconditional basic income.[511] Others claim that "robots will take your jobs, government will have to pay your wage."[512] Some argue that, in the future, workforce may face growing disparities with middle-wage earners losing ground, and that internationally, the lack of access to new technologies in least developed countries will increase inequalities between countries even further.[513] The impact on AI on the digital economy was also raised by a number of international institutions, for example UNI, the global union federation for national and regional trade unions which is concerned with protecting workers' rights[514] or the Committee on Artificial Intelligence of the Council of Europe: their 2020 report on the impact of AI on human rights, democracy and the rule of law[515] also addressed the issue of social and economic rights, and G20's human-centered AI principles[516] not only stress that AI shall be fair, transparent and accountable and that it shall respect privacy, equality, diversity – it also underlines that Artificial Intelligence shall respect internationally recognized labor rights. Fact is that nowadays, even getting a job starts with AI because resume screenings and background checks are very often being automated, and the draft AI Regulation addresses employment and recruitment issues and classifies AI applications used for such purpose / in this sector as high-risk[517] with all its consequences. In addition, existing directives on non-discrimination in the employment context based on religion or belief,

[509] George Krasadakisd: Artificial Intelligence: The impact on employment and the workforce. How is AI replacing jobs? Which roles and industries will be most impacted? How can societies get prepared? Article published January 2018, available at https://medium.com/innovation-machine/artificial-intelligence-3c6d80072416. Retrieved October 24, 2021.

[510] John Barnett: Will AI revolution lead to mass unemployment? What Artificial Intelligence might mean for your job and industry. Article published April 25 2017, available at https://www.business.com/articles/john-barnett-artificial-intelligence-job-market/#:~:text=Well%2C%20the%20real%20answer%20lies%20somewhere%20in%20between.,will%20result%20in%20huge%20losses%20and%20then%20layoffs. Retrieved October 24, 2021.

[511] Doug Bolton: The rise of artificial intelligence could put millions of human workers out of jobs - could a basic income be a solution? Article published February 19 2016, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/basic-income-artificial-intelligence-ai-robots-automation-moshe-vardi-a6884086.html. Retrieved October 24, 2021.

[512] Catherine Clifford quotes Elon Musk in her article for CNBC published November 4 2016 (updated January 29 2018), available at https://www.cnbc.com/2016/11/04/elon-musk-robots-will-take-your-jobs-government-will-have-to-pay-your-wage.html. Retrieved October 24, 2021.

[513] United Nations Department of Economic and Social Affairs commented on this issue in their blog post: Will robots and AI cause mass unemployment? Not necessarily, but they do bring other threats. Article published on September 13 2017, available at https://www.un.org/development/desa/en/news/policy/will-robots-and-ai-cause-mass-unemployment-not-necessarily-but-they-do-bring-other-threats.html. Retrieved October 24, 2021.

[514] Background information on UNI Global Union is available at https://uniglobalunion.org/. Retrieved October 24, 2021.

[515] Catelijne Muller: The impact of Artificial Intelligence on human rights, democracy, and the rule of law. Report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Paper published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 24, 2021.

[516] The G20 Ministerial Statement on Trade and Digital Economy was published in June 2019, and is available at https://www.mofa.go.jp/files/000486596.pdf. Retrieved October 24, 2021.

[517] The law firm Hunton Andrews Kurth provides details on the proposed AI Act in their 2021 blog post: European Commission publishes proposal for Artificial Intelligence Act. Article published April 22 2021, available at https://www.huntonprivacyblog.com/2021/04/22/european-commission-publishes-proposal-for-artificial-intelligence-act/. Retrieved October 24, 2021.

disability, age or sexual orientation[518] or equal treatment of men and women in matters of employment and occupation[519] must be taken into consideration as well.

4.6.15. Liability

A technology like AI that is characterized by systems operating in an autonomous manner leads to yet another issue with regards to AI: liability. While accountability as a value and privacy principle is stressed in most publications, fewer texts deal with the fact that AI has the potential to challenge the traditional notions of legal personality including agency and responsibility.[520] The European Parliament dealt with liability issues and published a study on robotics[521] which deals with liability law solutions in respect of autonomous robots. The European Parliament furthermore issued a resolution on a civil liability regime for AI,[522] and a resolution on civil law rules on robotics.[523] Moreover, the European Commission published a report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics[524] and its Expert Group on Liability and New Technologies issued a report[525] on liability for AI and other emerging technologies in which it explains key findings with regards to questions like new duties of care, strict and vicarious liability, the burden of proof for both, causation, and damage, as well as insurance issues. At European level, the AI Liability Directive[526] is

[518] Council Directive 2000/78/EC of 27 November 2000 against discrimination at work on grounds of religion or belief, disability, age or sexual orientation establishing a general framework for equal treatment in employment and occupation is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078. Retrieved October 24, 2021.

[519] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054. Retrieved October 24, 2021.

[520] Mihalis Kritikos: Artificial Intelligence ante portas: legal and ethical reflections. EPRS briefing published March 2019, available at https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf. Retrieved October 24, 2021.

[521] European Civil Law Rules on Robotics published in 2016, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf. Retrieved October 24, 2021.

[522] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL) is available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html. Retrieved October 15, 2021.

[523] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL) is available at https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. Retrieved October 15, 2021.

[524] European Commission: Report to the European Parliament, the Council and the European Economic and Social Committee on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. Report published February 19 2020, available at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX:52020DC0064. Retrieved October 24, 2021.

[525] The report has been published November 21, 2019, and is available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. Retrieved October 24, 2021.

[526] The text of the AI Liability Directive is available at https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en. Retrieved January 7, 2023.

probably the most important step towards adding legal clarity.[527] The idea of a legal personality for AI and the potential of damages caused by autonomous robots are not the only issues to consider since there are also product liability implications[528] and AI might furthermore call for changes to copyright laws.[529] If algorithmic decision-making is used in criminal proceedings without human involvement, AI may furthermore have to be examined and assessed in the light of due process requirements.[530] AI can thus be examined from various legal perspectives, ranging from data protection, tort liability, copyright authorship and criminal law[531] – a multitude of areas of liability arises from different use cases of AI. From an individual's perspective, the question would be whom to turn to: a court[532] or a regulator[533] or a company, and if so, which one: from a GDPR perspective, there are controllers, processors and joint controllers; from a DGA perspective there are data holders and data users, and there is not just data but "representations of acts, facts or information and any compilation of the same including sound as well as visual or audiovisual recording,"[534] and looking at the categorization of relevant players in the context of the draft AI regulation, the situation becomes even more complex as there are providers, manufacturers, distributors, importers, users – how should an average person without corresponding expertise be able to tell who is responsible for which part and under which conditions, particularly now that the European Court of Justice has clarified the competences of non-lead data protection authorities and has given them greater ability to pursue Big Tech companies which are not headquartered in their

[527] According to IAPP's and FTI Consulting joint 2023 report on privacy and AI governance, this is highly welcome from a business perspective: Privacy and AI Governance Report published January 2023, available at https://iapp.org/resources/article/ai-governance-report-summary/?mkt_tok=MTM4LUVaTS0wNDIAAAGJg-8GK3cP-hfHi0yz1s63YttbFgDBnovCnlsyOUnEB_zUcoykvCDEfx57nVN5ye6zeM2saf2pII4Kot0-eahTGgIkN5FfAJS1RdCct8yoY4zQ. Retrieved January 29, 2023.

[528] John Villasenor: Products liability law as a way to address AI harms. Article published October 31 2019, available at https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/. Retrieved October 24, 2021.

[529] On October 30, 2019, the U.S. Patent and Trademark Office requested comments on intellectual property protection for AI innovations, see Federal Register 2019, vol. 84, no. 210, available at https://www.govinfo.gov/content/pkg/FR-2019-10-30/pdf/2019-23638.pdf. Retrieved October 24, 2021.

[530] Mihalis Kritikos: Artificial Intelligence ante portas: legal and ethical reflections. EPRS briefing published March 2019, available at https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf. Retrieved October 24, 2021.

[531] These topics were covered in the conference "AI, Law, and Agency in the Age of Machine Learning" which took place in November 2019 in Tel Aviv. Background information is available at https://en-ethics.tau.ac.il/AI_Law_And_Agency_in_the_Age_of_Machine_Learning/. Retrieved October 24, 2021.

[532] Lars Lensdorf, Robert Henrici, Moritz Hüsch, Nicholas Shepherd: A new day for GDPR damages claims in Germany? Article published February 25 2021, available at https://www.insideprivacy.com/data-privacy/a-new-day-for-gdpr-damages-claims-in-germany/. Retrieved October 24, 2021.

[533] Vincent Manancourt: Have a GDPR complaint? Skip the regulator and take it to court. Article published August 30 2020, available at https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/. Retrieved October 24, 2021.

[534] Debbie Heywood: The EC draft Data Governance Act – an altruistic approach to data. Article published January 29 2021, available at https://www.taylorwessing.com/en/insights-and-events/insights/2021/01/the-ec-draft-data-governance-act---an-altruistic-approach-to-data#:~:text=The%20DGA%20applies%20to%20a%20very%20broad%20range,the%20form%20of%20sound%2C%20visual%20or%20audiovisual%20recording%22. Retrieved October 24, 2021.

territory,[535] which also questions the one-stop-shop mechanism that was once believed to be one of the major advancements the GDPR would bring to organizations.[536]

4.6.16. Security

Security is always an important component[537] whenever data processing is in question, and since Big Data and AI are about complex operations, security is a priority in an increasingly digital and data-driven economy and society.[538] If security issues are not taken seriously, this may lead to unauthorized (increased) accessibility, disclosure of (sensitive) information and unintended (undesired) inferences[539] as well as reputational damage for both, the company using AI techniques and the affected individuals. GDPR, to name just one example of legislation dealing with security,[540] correspondingly covers various such aspects[541] and Recitals 75 and 76 clearly show that the Regulation pursues a risk-based approach[542] as it distinguishes between processing activities with a high and a low likelihood and severity to the rights and freedoms of natural persons.[543] Consequently, mitigation measures have to be taken into consideration, and these have to be adjusted to the type of information processed, the devices in question as well as access to location of, and retention and preservation of data.[544] In addition, the operational environment as well as governance, resources and project management, potential conflicts of interest

[535] Scott Ikeda: Big Tech companies may face blizzard of new probes in EU as CJEU ruling clears path for data protection authorities. Article published June 28 2021, available at https://www.cpomagazine.com/data-protection/big-tech-companies-may-face-blizzard-of-new-probes-in-eu-as-cjeu-ruling-clears-path-for-data-protection-authorities/#:~:text=The%20new%20CJEU%20ruling%20gives%20the%20data%20protection,protection%20authorities%20will%20need%20to%20meet%20certain%20conditions. Retrieved October 24, 2021.

[536] Heidi Waem, Simon Verschaeve: What's left of the GDPR's one-stop-shop? CJEU clarifies the competences of non-lead data protection authorities. Article published July 5 2021, available at https://blogs.dlapiper.com/privacymatters/eu-whats-left-of-the-gdprs-one-stop-shop-cjeu-clarifies-the-competences-of-non-lead-data-protection-authorities/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter. Retrieved October 24, 2021.

[537] See, for example, GDPR Article 32.

[538] Background information on this issue is provided by the OECD: Digital Economy Paper on digital security risk management. Paper published October 2019, available at https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826. Retrieved October 24, 2021.

[539] Andrew Burt: Privacy and cyber-security are converging. Here's why that matters for people and for companies. Article published January 3 2019, available at https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies. Retrieved October 24, 2021.

[540] In 2019, the German Federal Industries Association developed a tool to illustrate the current state of play regarding country-specific regulations on cyber security, critical infrastructure protection, incident notification and the protection of Intellectual Property from cyber risks, published October 2 2019, available at https://english.bdi.eu/topics/global-issues/cyber-landscapes/. Retrieved October 24, 2021.

[541] Article 32, security of processing; Article 25: data protection by design and by default; Articles 35 and 36: data protection impact assessments; Articles 33 and 34: breach notifications.

[542] Nico Härting: Datenschutzgrundverordnung. Dr. Otto Schmidt Publishing 2016, p. 34.

[543] A summary of risk-relevant provisions can be found in: Thomas Kranig, Andreas Sachs, Markus Gierschmann: Datenschutz-Compliance nach der DSGVO – Handlungshilfe für Verantwortliche inclusive Prüffragen für Aufsichtsbehörden. Bundesanzeiger Publishing 2017, p. 87.

[544] Mike Dutch: A data protection taxonomy, paper for the Storage Networking Industry Association. Paper published June 2010, available at https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf. Retrieved October 24, 2021.

and issues of ownership, company values and ethics[545] play an important role to minimize risk – however, all this is based on the traditional view GDPR takes regarding companies as controllers: the true security danger we are facing with AI is that, even though AI can be used for security purposes like intrusion detection,[546] new systemic risks arise since more and more critical infrastructures[547] depend on centralized systems with operations that are based on algorithmic (automated) decisions. Another factor to consider is that from both, an individual's and societal perspective, this technology can "empower malicious actors ranging from cybercriminals to totalitarian states in their desire to control populations"[548] and this way, may pose a threat to security.

4.6.17. Malicious use of AI

The mere fact that a technology is new does not mean that it will automatically worsen the situation in terms of security. On the contrary, the majority of successful cyberattacks start with a person intentionally or unintentionally fooled into clicking somewhere they shouldn't; hackers target people because the real weakest link is often the least obvious.[549] However, fact is also that much more attention has been paid to beneficial applications of AI than the ways in which Artificial Intelligence could be used maliciously, and some predict that the growing use of AI systems will change the landscape of threats, because adequate defenses to potential security threats from malicious uses of AI are not yet developed.[550] A report surveyed potential security threats in the context of Artificial Intelligence and came to the following conclusions:[551] the use of Artificial Intelligence will expand existing threats and change the typical character of threats, because AI may simply lower the costs of attacks since AI is scalable and can complete tasks that would ordinarily require human labor, intelligence and expertise;

[545] Government of Canada: Guide to risk taxonomies, last modified March 29 2016, available at https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html#toc2. Retrieved October 24, 2021.

[546] Bruno Capone: Intrusion detection based on Deep Learning. Article published October 16 2020, available at https://www.aitech.vision/en/2020/10/16/intrusion-detection-based-on-deep-learning/. Retrieved October 24, 2021.

[547] Deven Desai, Christos Makridis: We should have known SolarWinds would be a target. Article published January 6 2021, available at https://www.cfr.org/blog/we-should-have-known-solarwinds-would-be-target. Retrieved October 24, 2021.

[548] Catelijne Muller: The impact of Artificial Intelligence on human rights, democracy, and the rule of law. Report for the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI). Report published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da. Retrieved October 24, 2021.

[549] Stu Sjouwerman: Seven reasons for cybercrime's meteoric growth. Article published December 23 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/#:~:text=Cybercrime%20has%20been%20on%20the%20rise%20for%20years.,more%20criminals%20are%20leveraging%20the%20internet%20to%20steal. Retrieved October 24, 2021.

[550] Valerie Thomas: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 24, 2021.

[551] Miles Brundage et al: The malicious use of Artificial Intelligence: forecasting, prevention, and mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

the use of AI for malicious purposes could be especially effective, because it could be finely targeted, difficult to attribute, and thus likely to exploit vulnerabilities (e.g., by using speech synthesis for impersonation), and complete tasks that would be otherwise be impractical for humans (e.g., labor intensive attacks). AI can moreover be used in novel ways, for example by "exploiting human vulnerabilities (e.g., through the use of speech synthesis for impersonation), by exploiting existing software vulnerabilities (e.g., through automated hacking) – or the vulnerabilities of AI systems (e.g. through data poisoning or by introducing training data that causes a learning system to make mistakes or by inputs designed to be misclassified by Machine Learning systems."[552] The latter is a particularly interesting aspect insofar as AI itself may be vulnerable as well: if AI systems can exceed human performance, but they may also fail in ways that a human never would. Finally, Artificial Intelligence could also be used in a political context, for example for creating targeted propaganda or to manipulate videos with the help of deepfakes,[553] or threaten physical security by subverting systems or through the use of drones.[554] In consequence, a new quality of malicious actors may emerge, and AI can thus be considered a dual-use technology.[555] It is therefore necessary to address these dual-use concerns correspondingly and collaborate closely with the relevant stakeholders, researchers and experts to investigate, prevent and mitigate potential malicious uses of AI:[556] AI's dual-use character, its efficiency and scalability, its anonymity and psychological distance together with the fact that Artificial Intelligence may exceed human capabilities and that it implies novel unresolved vulnerabilities may lead to serious threats that could affect our security, for example, by criminals training machines to hack or socially engineer victims at scales beyond what humans are doing now or by privacy-eliminating surveillance and profiling, or through automated and targeted disinformation campaigns or by non-state actors weaponizing drones or robots.[557] However, even seemingly harmless use cases in the online world show the potential for risk: so-called dark patterns,[558] i.e., methods to misinform or inappropriately influence users' behavior and manipulate consumer actions, ranging from annoying-but-innocent to unlawful (e.g. checkbox, scroll-down) design, leading to violations of existing laws such as Section 5

[552] Miles Brundage et al: The malicious use of Artificial Intelligence: forecasting, prevention, and mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

[553] Kanan Purkayastha: Challenges from malicious use of AI. Article published May 18 2020, available at https://www.observerbd.com/news.php?id=257035. Retrieved October 24, 2021.

[554] Saheli Choudhury: Malicious use of A.I. could turn self-driving cars and drones into weapons, top researchers warn. Article published February 21 2018, available at https://www.cnbc.com/2018/02/21/malicious-use-of-ai-by-hackers-could-pose-security-risks-threats.html.

[555] Jayshree Pandya: The dual-use dilemma of Artificial Intelligence. Article published January 7 2019, available at https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/. Retrieved October 24, 2021.

[556] Miles Brundage et al: The malicious use of Artificial Intelligence: forecasting, prevention, and mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 24, 2021.

[557] Valerie Thomas: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 24, 2021.

[558] The website https://www.darkpatterns.org/about-us has been established to raise public awareness of deceptive digital practices, and changed its name to https://www.deceptive.design/. Retrieved February 5, 2023.

of the FTC Act, or consumer[559] and data privacy laws.[560] Consequently, the EDPB dealt with the phenomenon and issued guidance on deceptive design patterns in social media platform interfaces.[561] Obfuscatory checkboxes are probably the most common examples of dark patterns,[562] and dark patterns are not just a side-effect of AI uses, they have become a massive problem as a report by the Princeton research group on popular shopping websites shows:[563] the report claims to have found dark patterns in 11% of those websites, and it also identified dozens of third-party entities that offer turnkey solutions enabling sellers to build dark patterns into websites.[564]

4.6.18. Concentration of power

Some say that data is the oil of the 21st century, but that is incorrect because the volume of (machine, sensor, personal, etc.) data keeps growing exponentially[565] whereas the occurrences of oil are finite. Like every other industrial revolution, "Industry 4.0" has its own challenges and risks – and concentrations of power: we live in a world where a small number of companies has the power to control much of what we do – "Alphabet controls our search and much of our mobile experience, Apple controls the remainder of our mobile and much of our content experience, Amazon controls a large portion of our content experience and much of the Internet of Things, and Microsoft essentially sweeps up everything else,"[566] and the issue is that, without corresponding future regulation, data may be processed rather in accordance with corporate terms and conditions, and perhaps less with applicable privacy laws. The

[559] Laura Kim, John Graubert: Dark Patterns: what they are and what you should know about them. Article published July 9, 2019, available at https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/. Retrieved October 24, 2021.

[560] For example, the California Privacy Rights Act (CPRA), the first legislation explicitly regulating dark patterns in the United States: background information on the CPRA is provided by Jennifer King and Adriana Stephan: Regulating privacy dark patterns in practice – drawing inspiration from California Privacy Rights Act. Georgetown Law Technology Review 2021, vol. 5 pp. 251-276, available at https://georgetownlawtechreview.org/regulating-privacy-dark-patterns-in-practice-drawing-inspiration-from-california-privacy-rights-act/GLTR-09-2021/

[561] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0 published February 14 2023, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en. Retrieved February 28, 2023.

[562] Ben Davis: 13 examples of dark patterns in ecommerce checkouts. Article published on April 6 2017, available at https://econsultancy.com/13-examples-of-dark-patterns-in-ecommerce-checkouts/. Retrieved October 24, 2021.

[563] Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites Draft. Article published June 25 2019, available at https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns.pdf. Retrieved October 24, 2021.

[564] By Laura Kim, John Graubert: Dark Patterns: what they are and what you should know about them. Article published July 9 2019, available at https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/. Retrieved October 24, 2021.

[565] The McKinsey Global Institute estimates that the global volume of data doubles every three years. Report published December 2016, available at https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world. Retrieved October 24, 2021.

[566] Julia Black, Andrew Murray: Regulating AI and Machine Learning: setting the regulatory agenda. European Journal of Law and Technology 2019, vol. 10, issue 3, available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 24, 2021.

concentration of data leads to a concentration of power for those who control the data to an extent that this circumstance is relevant under antitrust law.[567] So far, the focus of regulation was on personal data and privacy self-management; legislation dealt with specific industries and specific types of data and specific uses cases (processing activities) that may result in risk or may lead to negative consequences for the individual behind the data but not with regulating machine-generated data.[568] The problem with taking market power into consideration in the framework of regulating AI starts with the fact that the existing legal landscape was not mapped.[569] However, initiatives like the DGA, DSA and DMA to regulate huge platforms and information gatekeepers are important steps, and this may help to end the "era of light-touch self-regulation."[570] Given the multitude of implications arising from AI as a technology and market dominance as a phenomenon, there is more work ahead, but the situation for companies like Meta is getting more and more complicated: in one of the biggest challenges the U.S. government has ever brought against a tech company in decades, the Federal Trade Commission wants to force Meta to sell Instagram and WhatsApp.[571] Unlike the FTC's case, the £2.3 billion class action lawsuit Meta was facing for unfair trading conditions by forcing users to give up large swathes of their personal data to use the app, and then sell the data to advertisers, was rejected.[572]

This chapter illustrated in detail the various implications when algorithmic data processing and decision-making are used due to significant impacts on individuals in consequence of opaqueness, information mismatch, concentration of powers, secondary use of data or AI's potential for discrimination, surveillance, intrusion, or addiction. This is important since it seems that the undisputed benefits and advantages of Big Data, ADM and AI dominate the perception and discussion of such applications, whereas AI could also be used in a manipulative or malicious manner. The chapter also explained the

[567] The German Facebook case showed that antitrust issues may be a factor to consider, however, the antitrust authority's ruling that social-media giant abused its dominance was reversed: Article by Sara Germano, published August 26 2019, available at https://www.wsj.com/articles/facebook-wins-appeal-against-german-data-collection-ban-11566835967. Retrieved October 24, 2021.

[568] Jan Christian Sahl: Brauchen wir ein Datenschutzrecht für Maschinendaten? Article published in the framework of the "Berliner Datenschutzrunde", available at https://www.berliner-datenschutzrunde.de/node/162. Retrieved October 24, 2021.

[569] AccessNow: Europe's approach to artificial intelligence: How AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 24, 2021.

[570] Gabriela Ramos, Mariana Mazzucato: AI in the common interest. Article published December 22 2022, available at https://www.project-syndicate.org/commentary/ethical-ai-requires-state-regulatory-frameworks-capacity-building-by-gabriela-ramos-and-mariana-mazzucato-2022-12. Retrieved January 20, 2023.

[571] Isobel Hamilton: The FTC can move forward with its bid to make Meta sell Instagram and WhatsApp, judge rules. Article published January 12 2022, available at https://www.businessinsider.com/ruling-ftc-meta-facebook-lawsuit-instagram-whatsapp-can-proceed-2022-1#:~:text=Judge%20James%20Boasberg%20ruled%20on%20Tuesday%20that%20the,lawsuit%2C%20which%20was%20rejected%20by%20Boasberg%20in%20June. Retrieved February 28, 2023.

[572] Adebusola Bada: UK tribunal rejects application for £2.3 billion class action suit against Meta. Article published February 21 2023, available at https://www.jurist.org/news/2023/02/uk-tribunal-rejects-application-for-2-3-billion-class-action-suit-against-meta/#:~:text=The%20UK%E2%80%99s%20competition%20tribunal%20Monday%20rejected%20an%20application,required%20for%20the%20class%20action%20to%20move%20forward. Retrieved February 28, 2023

relevance of this new technology for major principles of data protection laws such as purpose limitation and elaborated on the political and human rights dimension as well as societal implications. These aspects are particularly important as they show the limitations of privacy self-management and the necessity to rethink traditional approaches since such technologies not only pose challenges at individual level, but conceptually question traditional approaches to data protection.[573]

5. Relevant sources of law

This chapter is a core element of the Thesis as it examines the existing legal landscape from a data protection perspective. The overview starts with rules at international level, with important sources like the Universal Declaration of Human Rights, Convention 108+, the Charter of Fundamental Rights of the European Union, which deal with fundamental rights, including data protection and privacy. At EU level, the chapter presents numerous regulations and directives covering topics like know-how protection, cyber security and product safety, database rights, or equal treatment and discrimination. None of them are essentially about data protection or privacy, but all of them are relevant to complete the picture about the existing legal and regulatory framework for Big Data and AI, and since these laws cover issues like liability, security, or conformity, they are relevant from a data protection, and consequently individual's perspective. Furthermore, this chapter puts focus on the General Data Protection Regulation, for good reason: the GDPR was a major step after decades in which the Directive governed data protection within the EU and strengthened transparency, individual rights, and enforcement powers. Moreover, the GDPR can be considered a role model law, which is shown by the fact that emerging data protection regulations around the globe are matched against the General Data Protection Regulation, for example, Brazil's data protection law LGPD,[574] China's PIPL[575] or Japan's act on the protection of personal information.[576] The examination of the GDPR is of particular interest as it allows for an analysis of the viability and challenges of traditional concepts in data protection law. The chapter also elaborates on further relevant sources of law, for example, national data protection and consumer protection laws, competition as well as labor, equal opportunity laws, and IT-security laws including Internet of Things. Moreover, various sector, industry, or product, purpose, and data specific laws exist which must be obeyed when AI applications and algorithmic systems are used, for example,

[573] Alexander Roßnagel, Christian Geminn: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. Report published November 26 2019, available at https://www.heise.de/downloads/18/2/8/0/2/5/0/7/vzbv.pdf. Retrieved October 20, 2021.

[574] Renato Monteiro: GDPR matchup – Brazil's general data protection law. Article published October 4 2018, available at https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Retrieved October 20, 2021.

[575] Xu Ke, Vicky Liu, Yan Luo, Zhijing Yu: Analyzing China's PIPL and how it compares to the EU's GDPR. Article published August 24 2021, available at https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/. Retrieved October 20, 2021.

[576] Kensaku Takase: GDPR matchup – Japan's act on the protection of personal information. Article published August 29 2017, available at https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/. Retrieved October 20, 2021.

for high frequency algorithmic trading, in the employment context, for facial recognition, autonomous driving, or autonomous weapons, medical devices, biometric data and genetic information. The fact that numerous laws that deal with algorithm-based decisions, ADM, and AI as well as purpose, data, and processing specific rules have been enacted show that this area of law is not as immature as one may think; this rather demonstrates the complexity of the legal landscape. In this regard, U.S. legislation is very interesting, not only because the legal framework in the U.S. has become very vibrant in recent years, but also because the impact of laws targeting big tech companies like Google, Microsoft or Meta is not national, but global. Finally, the chapter presents various private-sector initiatives, and concludes with technical standards that are relevant in the context of compliance and (presumption of) conformity.

5.1. International level

5.1.1. United Nations Universal Declaration of Human Rights

In response to World War II, the United Nations (UN) adopted and proclaimed the Universal Declaration of Human Rights in 1948.[577] The Universal Declaration of Human Rights (UDHR) sets out, for the first time, fundamental human rights to be universally protected, and this includes privacy since UDHR Article 12 sets forth that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

5.1.2. European Convention on Human Rights

In Europe, there are two systems which ensure the protection of fundamental human rights in Europe, the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (Charter): The European Convention on Human Rights[578] was adopted in 1950. ECHR Article 8 states that "everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[577] The text of Universal Declaration of Human Rights is available at http://www.un.org/en/universal-declaration-human-rights/index.html. Retrieved September 26, 2021.

[578] The text of the European Convention on Human Rights is available at https://www.echr.coe.int/Documents/Convention_ENG.pdf. Retrieved September 26, 2021.

5.1.3. Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union[579] was enacted in 2000 and is a legally binding[580] human rights instrument, and it also deals with the right to respect for his or her private and family life, home and communications (Article 7), but what is special is that it specifically addresses the protection of personal data: Article 8 of the Charter of Fundamental Rights of the European Union postulates that "everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".[581] Although the Convention and the Charter contain provisions on human rights, they operate within separate legal frameworks:[582] The Charter of Fundamental Rights of the European Union was drafted by the European Union and is interpreted by the Court of Justice of the European Union. The European Convention on Human Rights was drafted by the Council of Europe[583] and is interpreted by the European Court of Human Rights. The Charter constitutes the legal framework for human rights in the European Union, of which the European Convention on Human Rights forms an important part.[584] Unlike the Charter of the Fundamental Rights of the European Union, the Convention does not contain a specific provision on data protection, but this

[579] The text of the Charter of Fundamental Rights of the European Union is available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Retrieved September 26, 2021.

[580] The European Union competent to pass legislation on data protection matters based on Article 16 of the Treaty on the Functioning of the European Union and used this competence to include Article 8 on the right to data protection in the Charter.

[581] The question of the relationship between Article 7 and 8 of the Charter is controversially discussed. Some authors consider that Article 8 is lex specialis: Sebastian Bretthauer in: Louisa Specht/Reto Manz: Handbuch europäisches und deutsches Datenschutzrecht 2019, p. 29.

[582] Background information on the relationship between the Charter and the Convention is provided by UK's Equality and Human Rights Commission, a national human rights institution, and is available at https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union. Retrieved September 26, 2021.

[583] The following background information on various institutions is provided at the Council of Europe's website, available at https://www.coe.int/en/web/about-us/do-not-get-confused?desktop=true: the Council of Europe is an international organization in Strasbourg which comprises 47 countries of Europe. It was set up to promote democracy and protect human rights and the rule of law in Europe. The European Council is an institution of the European Union, consisting of the heads of state or government from the member states together with the President of the European Commission, for the purpose of planning Union policy". Retrieved October 2, 2021.

[584] Some authors distinguish these two models of human rights protection as follows: the European Convention on Human Rights is considered to be a "court-centred-model" of protection, whereas the Charter of Fundamental Rights may be considered a "legislative-centred-model", see Simon Bronitt: A Tale of Two European Charters of Rights – Comparing the European Convention on Human Rights and the EU Charter of Fundamental Rights, article available at http://www.academia.edu/6410839/A_Tale_of_Two_European_Charters_of_Rights_Comparing_the_European_Convention_on_Human_Rights_and_the_EU_Charter_of_Fundamental_Rights. Retrieved October 2, 2021.

does not mean that rights of data subjects are not guaranteed within this framework, as steadily growing case law confirms that corresponding control mechanisms are in place.[585]

5.1.4. Council of Europe Data Protection Convention 108+

The Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data[586] dates to 1980 and addresses challenges for privacy resulting from the use of new information and communication technologies. This convention was the first legally binding international instrument in data protection,[587] and that is why some believe that the Council of Europe has played a pioneering role the existing data protection legislation.[588] This view is underlined by the fact that the Council of Europe issued two Resolutions which formulated what later became fundamental principles of data protection law.[589] While keeping the convention's philosophy, the convention ("*108+*") has been modernized:[590] The Council of Europe updated the treaty in 2018 to reinforce the data protection principles of Convention 108, and include additional safeguards to better protect personal data in the digital age, including with regards to international data transfers, and to further strengthen data protection globally.[591] The convention lays down a number of principles which states must transpose into national law to ensure that personal data are processed only for specific purposes, that data are not retained longer than is necessary for the underlying purpose(s), and that the collection and processing of data is not excessive in relation to the purposes.[592] The modernized convention maintains the Convention's provisions at principle-level, contains technologically neutral provisions, and aims to ensure consistency and compatibility with other data protection legal frameworks, including the European Union's legislation.[593] The modernized convention consists of general, simple and concise principles, and allows states parties a certain measure of discretion when implementing them through

[585] Nomi Byström: The data subject and the European Convention on Human Rights: Article published December 31 2014, available at https://www.edilex.fi/viestintaoikeuden-vuosikirja/181000010. Retrieved October 2, 2021.

[586] The text of the Convention is available at https://rm.coe.int/16808ade9d. Retrieved October 2, 2021.

[587] David Wright, Paul De Hert, Serge Gutwirth: Are the OECD guidelines at 30 showing their age? Communications of the ACM 2011, vol. 54, issue 2, pp. 119-127, available at https://dl.acm.org/citation.cfm?id=1897848. Retrieved October 2, 2021.

[588] The German consultancy Datenschutz Nord reported on this issue in their online blog on March 19 2019, which is available at https://www.datenschutz-notizen.de/die-konvention-nr-108-die-kleine-schwester-der-dsgvo-0222164/. Retrieved October 2, 2021.

[589] For instance, the principle of purpose limitation, see Nikolaus Fargo, Stefanie Hänold, Benjamin Schütze: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Fargo (eds.): New Technology, Big Data and the Law: Springer Publishing 2017, p. 23.

[590] See "The modernized Convention 108: novelties in a nutshell", available at https://rm.coe.int/16808accf8.

[591] An overview of the novelties of the protocol is available at the COE's website https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8. Retrieved June 9, 2022.

[592] Further dtails are available at COE's website, available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet. Retrieved October 2, 2021.

[593] The Council of Europe provides details on the "Modernization of the Data Protection "Convention 108" on their website, available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet. Retrieved June 9, 2022.

their national legislation.[594] Considering the constantly increasing number of ratifications,[595] this convention[596] has the potential to become a global standard.[597] In addition, Data Protection Convention 108+ may also play a role for adequacy considerations.[598]

5.1.5. OECD Privacy Guidelines

The Organization for Economic Co-operation and Development (OECD) issued guidelines on the "Protection of Privacy and Transborder Data Flows of Personal Data" which were passed in September 1980[599] and updated in 2013.[600] These guidelines focus on the practical implementation of privacy protection through an approach which is based on risk management. Consequently, the revised 2013 version also deals with privacy management programs including operational (and data breach) mechanisms.[601] Just like Convention 108, these guidelines also incorporate the principle of purpose specification and the notion of incompatibility.[602] Apart from these guidelines, the OECD also issued recommendations on cross-border co-operation in the enforcement of laws protecting privacy in 2007.[603]

[594] A detailed comparison of the individual regulations within „Convention No. 108" and "Convention No. 108+" is provided by Carlo Piltz and Philipp Quiel: The role of „Convention No. 108" and "Convention No. 108+" as part of the examination of the level of protection in third countries under the GDPR. Article published September 1, 2020, available at https://www.delegedata.de/2020/09/the-role-of-convention-no-108-and-convention-no-108-as-part-of-the-examination-of-the-level-of-protection-in-third-countries-under-the-gdpr/. Retrieved June 8, 2022.

[595] The latest signatories are Mexico and Cabo Verde in 2018, Tunisia in 2017 and Mauritius and Senegal in 2016. The chart of signatures and ratifications is available at COE's website https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Retrieved October 2, 2021.

[596] The Council of Europe provides background information on the "Modernisation of the Data Protection Convention 108" at their website, available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet. Retrieved October 2, 2022.

[597] European Digital Rights (EDRi): Protecting personal data worldwide: Convention 108+. Paper published April 24 2019, available at https://edri.org/our-work/protecting-personal-data-world-wide-convention-108/#:~:text=Currently%2C%20the%20global%20standard%20for%20data%20protection%20could,a%20number%20of%20improvements%20to%20the%20previous%20text%3A. Retrieved October 2, 2022.

[598] Jennifer Baker: What does the newly signed 'Convention 108+' mean for UK adequacy? Article published October 30, 2018, available at https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/. Retrieved June 8, 2022.

[599] The text of the original 1980 version is available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines. Retrieved October 2, 2021.

[600] OECD's privacy framework has been published in 2013 and is available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Retrieved October 2, 2021. The expert group which dealt with the update also identified a number of topics which were raised but not fully addressed as part of the review process, and which could be considered for possible future study. Their report is available at https://www.oecd-ilibrary.org/docserver/5k3xz5zmj2mx-en.pdf?expires=1549789641&id=id&accname=guest&checksum=C6CB4D94745FBAC6759C9EA424F70745. Retrieved October 2, 2021.

[601] Further details are provided at OECD's website, available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Retrieved October 2, 2021.

[602] Nikolaus Fargo, Stefanie Hänold, Benjamin Schütze: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Fargo (eds.): New Technology, Big Data and the Law: Springer Publishing 2017, p. 25.

[603] OECD's recommendations on cross-border co-operation in the enforcement of laws protecting privacy have been published in 2007, and are available at https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd_guidelines_en.pdf. Retrieved October 2, 2021.

Even though OECD's guidelines are non-binding, they can nevertheless be considered a milestone initiative, also because their material content and underlying principles are congruent with the Council of Europe Data Protection convention.[604]

5.1.6. Further Conventions, Resolutions and Guidelines[605]

Privacy is furthermore mentioned in various other legal instruments at international level,[606] for example Article 14 of the United Nations Convention on Migrant Workers,[607] Article 16 of the United Nations Convention on rights of the Child,[608] as well as Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[609] The United Nations 2015 Guidelines on Consumer Protection[610] define the protection of consumer privacy as a general principle and specify that "businesses should protect consumers' privacy through a combination of appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data" as part of "principles for good business practices". In 2016, the United Nations moreover issued a resolution on the Right to Privacy in the Digital Age[611] in which the UN actively call upon states and upon business enterprises and in which they reaffirm the right to privacy, "according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights".

5.2. Global Trade Agreements

When it comes to privacy and data protection at an international level, many think of United Nations Universal Declaration of Human Rights, Convention 108+ or the European Convention on Human

[604] Unlike the Council of Europe Data Protection Convention, the OECD Guidelines do not mention the need to establish national data protection authorities, a typical (important) element in European data protection rules.

[605] The difference between these instruments is that some are legally binding, and some are not. Corresponding background information is available at http://www.unesco.org/new/en/social-and-human-sciences/themes/advancement/networks/larno/legal-instruments/nature-and-status/. Retrieved October 2, 2021.

[606] The Electronic Frontier Foundation provides background information on further international privacy standards on their website, available at https://www.eff.org/de/issues/international-privacy-standards. Retrieved October 2, 2021.

[607] The text of the 1990 International Convention on the Protection of the Rights of all Migrant Workers and Members of Their Families, UN Doc. A/RES/45/158 is available at http://www.un.org/documents/ga/res/45/a45r158.htm. Retrieved October 2, 2021.

[608] The text of the 1989 Convention on the Rights of the Child, UN Doc. A/RES/44/25 is available at http://www.un.org/documents/ga/res/44/a44r025.htm. Retrieved October 2, 2021.

[609] The text of the 1966 International Covenant on Civil and Political Rights, UN Doc. A/6316 is available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. Retrieved October 2, 2021.

[610] The text of the 2016 UNCTAD Guidelines on Consumer Protection are available at https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf. Retrieved October 2, 2021.

[611] The text of the 2016 resolution on Right to Privacy in the Digital Age is available at https://digitallibrary.un.org/record/848969/files/A_C-3_71_L-39_Rev-1-EN.pdf. Retrieved October 2, 2021.

Rights and the Charter of Fundamental Rights of the European Union. But the collection, processing and transfer of data including personal information are not only governed by data protection laws (and other areas of law, depending on the specific case in question): there seems to be little awareness that global trade and investment agreements in fact do address the issue of handling (i.e., transfer) of data: rules on trans-border data flows are incorporated in a variety of global agreements, for example the World Trade Organization's (WTO) General Agreement on Trade and Services (GATS)[612], the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[613] or the Comprehensive Economic and Trade Agreement (CETA) between Canada and the European Union.[614] These agreements are legally binding and have in common that they set forth (minimum) standards and core norms of non-discrimination, including protections against unjustified data localization requirements: the Trans-Pacific-Partnership (TPP) Agreement, for example, prohibits members from requiring companies located in a TPP country to build data centers in the market countries in which they serve.[615] Consequently, any future legislation which foresees data localization may be challenged owing to the existing overarching trade law framework.[616]

5.3. EU level

5.3.1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

The General Data Protection Regulation[617] replaces[618] the 1995 Data Protection Directive which was adopted when the Internet was in its infancy, at a time when Facebook and so many other things so many people nowadays consider indispensable did not exist. GDPR was introduced as the Data

[612] The text of the 1995 General Agreement on Trade in Services (GATS) is available at WTO's website https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm. Retrieved October 2, 2021.

[613] The text of the 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) as well as associated documents are available at https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents/Pages/official-documents. Retrieved October 2, 2021.

[614] The text of the 2017 Comprehensive Economic and Trade Agreement (CETA) between Canada and the EU is available at https://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf. Retrieved October 2, 2021.

[615] Mark Mao et al: Data privacy – the current legal landscape. Article published February 2016, available at https://iapp.org/media/pdf/resource_center/TS_CurrentLegalLandscape_February_2016.pdf. Retrieved October 2, 2021.

[616] An overview over global trade agreements is provided by Sean Stephenson and Paul Lalonde: The limits of data localization laws. The article was published August 9, 2019, and is available at http://www.dentonsdata.com/the-limits-of-data-localization-laws-trade-investment-and-data/. Retrieved October 2, 2021.

[617] The bill text of the General Data Protection Regulation is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Retrieved October 2, 2021.

[618] Further details including a GDPR timeline are available at https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Retrieved October 2, 2021.

Protection Directive failed to achieve the desired harmonization[619] throughout the European Union due to different implementation and application of its provisions within various Member States. GDPR's title demonstrates its twin goals, "the protection of natural persons with regard to the processing of personal data and (…) the free movement of personal data."[620] GDPR aims at reducing fragmentation and aligning legislation and legislative practice, however, these goals are somewhat questionable due to a rather high number of so-called opening clauses[621] in important areas like data protection in the employment context.[622] The regulation nevertheless marks the biggest shift in data protection laws ever due to its expanded scope and owing to the introduction of a new framework for data protection with increased obligations for organizations including serious penalties for non- compliance.[623]

5.3.2. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

The European Data Protection Supervisor (EDPS) stresses[624] the relevance of personal data to the concept of trade secrets, for good reasons: Due to the fact that personal data may form part of a trade secret and given that the holder of a trade secret holder in many cases will also be a data controller if information relating to identified or identifiable individuals is processed, this directive[625] is of importance to Big Data applications. The protection of know-how is not only a standard topic in non-disclosure agreements; this new directive will have a direct impact on organizational culture including the dealing with service providers (processors).[626] Another aspect is that is generally recognized that, if

[619] David Bender: GDPR harmonization: Reality or myth? Article published on June 7 2018, available at https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/. Retrieved October 2, 2021.

[620] See GDPR Art. 1 (1).

[621] The GDPR contains dozens of opening clauses allowing EU Member States to put national data protection laws in place to supplement the GDPR. A summary on this topic is provided by Julia Kaufmann, Michael Schmidl, Holger Lutz (editors) for Baker McKenzie in their GDPR national legislation survey. Survey published January 2018, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en. Retrieved October 2, 2021.

[622] However, it shall be noted that the original 2012 Commission proposal included a dedicated chapter on the processing of employment data. That text, however, did not survive the lawmaking process and make it to the final version of the Regulation. Background information on the Commission's proposal is provided by Gerrit Hornung: A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25 January 2012. Article published March 6 2018, available at https://script-ed.org/article/general-data-protection-regulation-europe-light-shade-commissions-draft-25-january-2012/. Retrieved July 22, 2022.

[623] Global Legal Group: The international comparative legal guide to data protection, 5th edition 2018, available at https://iapp.org/media/pdf/resource_center/Legal_Guide_To_Data_Protection_2018.pdf. Retrieved October 2, 2021.

[624] EDPS 0pinion published March 12, 2014, available at https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf. Retrieved October 2, 2021.

[625] The text of this directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943. Retrieved October 2, 2021.

[626] Thomas Hoeren and Reiner Münker: Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung unter besonderer Berücksichtigung der Produzentenhaftung. Wettbewerb in Recht und Praxis 2018, vol. 2, pp. 150-155, available at https://www.itm.nrw/wp-content/uploads/Die-EU-Richtlinie.pdf. Retrieved October 2, 2021.

an information is a secret, it has a commercial value, and the same is discussed for personal data.[627] Know-how protection therefore is another important factor in the introduction of Big Data.

5.3.3. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

The European Commission proposed the EU Network and Information Security Directive[628] as part of EU's cyber-security strategy which aims at strengthening resilience for providers of critical infrastructure services and applies to sectors such as health and energy, transport, banking, water, as well as digital service providers.[629] This directive (also known as the Cyber-security Directive, in brief: NISD) is the first piece of EU-wide cyber-security legislation,[630] and even though it does not apply to all companies, it may serve as an orientation in terms of security standards, because all businesses have to take care of the security of processing.[631] Moreover, it has significant intersections with GDPR in terms of accountability, one of GDPR key elements,[632] and it also includes a wide range of organizational requirements (e.g. risk management, incident reporting).[633] NISD and GDPR, however, are not exactly the same as, for example, NISD breach notification requirements extend beyond those of GDPR.[634] The European Commission announced to review the NIS Directive by the end of 2020,[635] and a political agreement between the European Parliament and EU Member States on the NIS 2 Directive has been reached in May 2022.[636]

[627] Marc van Lieshout: The value of personal data. In: Jan Camenisch, Simone Fischer-Hubner, Marit Hansen (eds). Privacy and Identity Management for the Future Internet in the Age of Globalisation, pp. 26-38. Springer Publishing 2015.

[628] The text of EU's Network and Information Security Directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG. Retrieved October 2, 2021.

[629] Digital service providers (online marketplaces, online search engines and cloud computing services) are subject to slightly different rules: Lawrence Kalman: The GDPR and NIS Directive – a new age of accountability, security and trust? Presentation held during the 2017 OWASP summit, available at https://www.owasp.org/images/b/b9/Olswang_slides_-_GDPR_and_NIS_Directive_-_accountability_security_and_trust_-_25_Jan_2017.pdf. Retrieved October 2, 2021.

[630] Background information on the NIS Directive is provided by the European Agency for Network and Information Security, available at https://www.enisa.europa.eu/topics/nis-directive. Retrieved October 2, 2021.

[631] See GDPR Article 32.

[632] See GDPR Article 5 (2): "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

[633] Further details are available at https://www.twobirds.com/en/news/articles/2016/global/new-security-and-reporting-requirements-for-infrastructure-providers-and-certain-digital-businesses. Retrieved October 2, 2021.

[634] Gabe Maldoff: NIS + GDPR = A New Breach Regime in the EU. Article published December 22 2015, available at https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/. Retrieved October 2, 2021.

[635] After a period of public consultation, the European Commission started their work in June 2020, see https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive. Retrieved October 2, 2021.

[636] European Commission press release: Commission welcomes political agreement on new rules on cybersecurity of network and information systems, published 13 May 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985 Retrieved July 20, 2022.

5.3.4. Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber-security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cyber-Security Certification

This regulation,[637] also called Cyber-security Act, aims to achieve a high level of cyber-security and cyber resilience, and to reinforce the role of the European Union Agency for Cyber-security as the European Union's center of cyber-security expertise in the framework of a permanent mandate. Among other things, ENISA will be responsible for a cyber-security certification framework. This is remarkable insofar as this initiative is the first internal market law that creates that takes up the challenge of enhancing the security of IoT devices and connected products. This way, a one-stop shop for cyber-security certification will be created that could lead to the removal of potential market-entry barriers and significant cost saving for enterprises, since they would otherwise need to apply for several certificates in several EU countries.[638] Businesses could use such certifications to have their security features independently verified and strengthen users' trust in their products and services. In this context, it should also be mentioned that the EU published Digital Operational Resilience Act (DORA), which will be applicable to most financial institutions: DORA aims to consolidate and up-grade ICT risk requirements and establish a streamlined digital operational resilience framework across the EU financial sector; it will include a new oversight framework for critical ICT third-party service providers.[639]

5.3.5. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

Unlike the ePrivacy Regulation, the above regulation[640] is already in force[641] and is part of the EU's digital single market strategy.[642] Its main goal is to boost and promote the data economy[643] by facilitating the cross-border exchange of data and the development of new technologies by removing existing data

[637] The text of the regulation is available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0151+0+DOC+PDF+V0//EN. Retrieved October 2, 2021.

[638] The European Commission offers detailed information on the Cyber-security Act and ENISA's role and tasks including advantages for businesses on their website, available at https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en. Retrieved October 2, 2021.

[639] Anthony Day, Nichola Donovan, David Ossack: Operational Resilience: Update EU – publication of DORA. Article published January 16 2023, available at https://www.technologyslegaledge.com/2023/01/operational-resilience-update/?utm_source=DLA+Piper+-+Technology%27s+Legal+Edge&utm_campaign=29e7915ae6-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_451d831b6d-29e7915ae6-92373648. Retrieved January 17, 2023.

[640] The text of EU's regulation on non-personal information is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.303.01.0059.01.ENG. Retrieved October 2, 2021.

[641] It will be applicable in all European Union Member States as of May 2019.

[642] Background information on EU's digital single market strategy is available at https://eufordigital.eu/discover-eu/eu-digital-single-market/. Retrieved January 30, 2023.

[643] Stephanie de Smedt: Free flow of non-personal data and GDPR. Article published June 19 2019, available at https://www.lexology.com/library/detail.aspx?g=240c3d71-f818-4233-a7f3-01b32f17b3b3. Retrieved October 2, 2021.

localization requirements and at enabling storage of data[644] in multiple locations across the European Union. New technologies include Artificial Intelligence,[645] and that makes this regulation particularly interesting to Big Data applications. As for practical implications, it is foreseeable that problems will arise from the demarcation between personal (identifiable) and non-personal data such as aggregate and anonymized data. The fundamental underlying problem is that anonymization is hard to achieve:[646] an investigation of as little as four spatiotemporal points (credit card metadata) was enough to uniquely re-identify 90 % of individuals behind the data.[647] This example of reverse engineering shows that it is necessary to rethink and question currently implemented (technical) privacy standards.[648] Given the growing relevance of machine-generated, non-personal data in the Industry 4.0, some authors stress the necessity of regulations for this type of data as so far, the focus of regulation is with personal data.[649]

5.3.6. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regards to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

This regulation[650] concerns the processing of personal data by European Union institutions, bodies, offices, and agencies. It abolished Regulation (EC) No 45/2001[651] which also dealt with the protection of individuals with regard to the processing of personal data by community institutions, and which established the European Data Protection Supervisor to be the independent data protection authority

[644] With exceptions where data localization restrictions are justified on grounds of public security, see Jörg Hladjk, Undine von Diemar, Olivier Haas and Jonathon Little: European Union: New regulation favors free flow of non-personal data in the EU. Article published17 December 2018, available at http://www.mondaq.com/x/762982/data+protection/New+Regulation+Favors+Free+Flow+Of+NonPersonal+Data+In+The+EU. Retrieved October 2, 2021.

[645] See the Council's corresponding press release 603/18: Free flow of data: EU adopts new rules. Press release published November 9, 2018, available at https://www.consilium.europa.eu/en/press/press-releases/2018/11/09/free-flow-of-data-eu-adopts-new-rules/. Retrieved October 2, 2021.

[646] In their 2014 opinion (05/2014) on anonymization techniques, the Article 29 Working Party explains how difficult it is to anonymize personal data. Opinion 05/2014 is available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Retrieved October 2, 2021.

[647] Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh and Alex Pentland: Unique in the shopping mall: On the reidentifiability of credit card metadata. Science 2015, vol. 347, issue 6221, pp. 536-539, available at http://science.sciencemag.org/content/347/6221/536/tab-pdf. Retrieved October 2, 2021.

[648] Sector-specific reactions occurred, e.g., the Payment Services Directive (PSD2) for the banking industry which introduces "regulatory technical standards enabling consumers to benefit from safer and more innovative electronic payments", see the European Commission 2017 fact sheet on PSD2: Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments. Factsheet published November 27 2017, available at http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm. Retrieved October 2, 2021.

[649] Jan Christian Sahl: Brauchen wir ein Datenschutzrecht für Maschinendaten? Newspaper interview on May 7 2018, available at https://www.marktundmittelstand.de/recht-steuern/die-dsgvo-gilt-auch-fuer-personenbezogene-maschinendaten-1271211/. Retrieved October 2, 2021.

[650] The bill text is available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725. Retrieved October 2, 2021.

[651] The bill text is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001R0045. Retrieved October 2, 2021.

which is tasked to ensure that the right to privacy is respected by European institutions and bodies.[652] It is noteworthy that both, the predecessor and the current version of the regulation contain provisions on compatible processing of personal data, which is important for the interpretation of purpose limitation and thus of relevance to Big Data and AI uses.

5.3.7. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Like the GDPR, the Law Enforcement Directive[653] also entered into force in May 2018. The directive is a little-known, much overlooked part of the EU data protection reform package.[654] This directive applies when a competent authority processes personal data for law enforcement purposes, i.e. for preventing, investigating, detecting and prosecuting crimes. In practice, so-called predictive policing relies on AI, for example for the calculation of geographic threat scores.[655] However, the Law Enforcement Directive also applies to processing that is conducted by private bodies, as long as the processing purpose is law enforcement, meaning that, for example, public transportation may rely on this directive in relation to ticket offences. The applicability of this directive is therefore not limited to the public sector and needs to be evaluated on a case-by-case basis, which can be challenging in the context of public–private partnerships.[656]

[652] The bill text is available at https://edps.europa.eu/data-protection/our-work/subjects/regulation-452001_en. Retrieved October 2, 2021.

[653] The bill text is available at is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG. Retrieved October 2, 2021.

[654] Paul De Hert, Vagelis Papakonstantinou: The new police and criminal justice data protection directive: A first analysis. New journal of European criminal law 2016, vol. 7, issue 1, pp. 7-19, available at https://research.tilburguniversity.edu/en/publications/the-new-police-and-criminal-justice-data-protection-directive-a-f#:~:text=Allegedly%20the%20Police%20and%20Criminal%20Justice%20Data%20Protection,EU%20legislative%20agenda%20towards%20the%20end%20of%202015. Retrieved October 2, 2021.

[655] Detailed examples and use cases are summarized by Privacy International on their website, available at https://www.privacyinternational.org/examples/predictive-policing. Retrieved October 2, 2021.

[656] Nadezhda Purtova: Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships. International Data Privacy Law 2018, vol. 8, issue 1, pp. 52–68, available version at https://doi.org/10.1093/idpl/ipx021. Retrieved October 2, 2021.

5.3.8. Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases

The Database Directive[657] was enacted as the need for database protection has increased in the digital age, because copying of data at large scale is easy. Although most of the content of social networks was created by the users and not by operators, harvesting of information and personal data on such platforms may infringe the rights of the platform operator.[658] The directive aims at preventing competitors from skimming off investments by providing a specific (sui generis) property right for analogue and digital databases that is unrelated to other forms of protection such as copyright. The directive protects databases by copyright if they are original; non-original databases such as compilations of legal cases and laws, listings of advertisements or databases of scientific publications can also be protected, if the investment in obtaining, verifying and presenting the data was substantial.[659]

5.3.9. Directive 2000/43/EC on equal treatment and against discrimination and Directive 2004/113/EC on equality in the access to and supply of goods and services

When implementing and applying Big Data analytics and AI applications for eligibility decisions, for example in the context of housing, lending or healthcare, companies should also consider further directives which are primarily concerned with preventing (gender-based) bias and promoting fairness, for example, the directive against discrimination on grounds of race and ethnic origin (Directive 2000/43/EC)[660] and Directive 2004/113/EC[661] on equality in the access to and supply of goods and services. It can thus be said that discrimination and equal treatment are addressed at EU level, however, these directives have not been discussed in the context of Big Data or Artificial Intelligence.

[657] The text of the directive is available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31996L0009. Retrieved October 2, 2021.

[658] Thomas Hoeren: Big Data und Recht, p. 129. C.H. Beck Publishing 2014.

[659] Background information on the protection of databases is provided by the Commission at their website, available at https://ec.europa.eu/digital-single-market/en/protection-databases. Retrieved October 2, 2021.

[660] The text of the Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML. Retrieved October 2, 2021.

[661] Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004L0113. Retrieved October 2, 2021.

5.3.10. Directive 2000/78/EC against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; see also Directive 2006/54/EC equal treatment for men and women in matters of employment and occupation

Ditto for other directives at EU-level that are concerned with equal treatment at work, for example Directive 2000/78/EC[662] against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; see also Directive 2006/54/EC[663] equal treatment for men and women in matters of employment and occupation. Because the hiring process nowadays often starts with (mandatory) background checks and resume screenings, workplace decisions are very often being (partially) automated, and therefore, Artificial Intelligence plays a role in the employment context.

5.3.11. Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

Difficulties may also arise from the fact that the existing Product Liability Directive[664] has not been amended to reflect specific implications Big Data and AI applications may involve: The European Commission has determined that the Directive for Defective Products, which has been in place for over 30 years, requires further work, but is still fit for purpose.[665] But AI-driven products should be examined in the light of product liability to properly address the risk of accidents[666] and damage resulting from interaction with humans. The same applies to the General Product Safety Directive[667] which imposes general safety requirements on any product put on the market for consumers: it should be reviewed against modern safety and security threats as well as present cyber-security standards[668]

[662] The text of the Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078. Retrieved October 2, 2021.

[663] The text of the Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054. Retrieved October 2, 2021.

[664] The text of the Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374. Retrieved October 2, 2021.

[665] Report on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) issued May 7, 2018, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525769201372&uri=COM:2018:246:FIN. Retrieved October 2, 2021.

[666] For example, self-driving car fatalities: ‘Wired’ reported about the latest Tesla car crash. Article published May 16, 2019, available at https://www.wired.com/story/teslas-latest-autopilot-death-looks-like-prior-crash/. Retrieved October 2, 2021.

[667] The text of Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety is available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095. Retrieved October 2, 2021.

[668] See also rules on Internet-connected devices. Background information on the IoT regulatory framework for Europe is provided by Vodafone in their 2019 Whitepaper on connected devices, available at https://www.vodafone.com/content/dam/vodcom/files/public-policy/iot-whitepaper/IoT_whitepaper_.pdf. Retrieved October 2, 2021.

5.3.12. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services

The Directive on Digital Content[669] addresses business models in which consumers provide data in exchange for a digital content or service – a phenomenon that has been under discussion for many years within the privacy community. The Digital Content Directive aims to harmonize the legal relationship between consumers and traders for the supply of digital contents and it "gives consumers the right to a remedy when digital content or a digital service is faulty, regardless of whether they paid for it or only provided personal data."[670] But the proposal has sparked some controversy for possibly introducing an instrument that acknowledges contracts in which personal data is being treated as contractual "counter-performance"[671] – in times where NGOs like "None Of Your Business" (NYOB) file hundreds of complaints against cookie banners[672] and paywalls which requires users to "buy back their own data".[673]

5.3.13. Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests; Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

From a company (controller) perspective, the Injunctions Directive[674] and the Representative Actions Directive[675] increase the risk of being sued due to unlawful practices under these directives.[676] From an individual's point of view, these directives are valuable even though the directives do not primarily deal

[669] The text of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0770. Retrieved October 2, 2021.

[670] Further details on the Digital Content Directive are provided by the European Commission on their website, available at https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en. Retrieved October 2, 2021.

[671] Weizenbaum Institut: Statement on the proposed Digital Content Directive. Statement published July 4 2018, available at https://www.weizenbaum-institut.de/index.php?id=107&tx_news_pi1%5Baction%5D=&tx_news_pi1%5Bcontroller%5D=&tx_news_pi1%5Bnews%5D=36&L=5&cHash=416e3183f5ac501a1777c33e947ff6ae. Retrieved October 2, 2021.

[672] NYOB news published August 10 2021, available at https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners. Retrieved October 2, 2021.

[673] NYOB news published August 13 2021, available at https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price. Retrieved October 2, 2021.

[674] The text of the Injunctions Directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0022. Retrieved January 7, 2023.

[675] The text of the Representative Actions Directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.409.01.0001.01.ENG. Retrieved January 7, 2023.

[676] Thomas Lennarz, Peter Wende: Neue Verbandsklage tritt Mitte 2023 EU-weit in Kraft. Article published December 10 2020, available at https://www.cmshs-bloggt.de/rechtsthemen/verbrauchervertraege-im-digitalzeitalter/verbandsklage-richtlinie-qualifizierte-einrichtung-2023/. Retrieved July 10, 2021.

with data protection[677] because they address consumer rights, commercial practices, digital services, or unfair contract terms, which are also governed by another directive:

5.3.14. Directive 93/13/EEC on Unfair Terms in Consumer Contracts

Given the information asymmetries and imbalanced powers between parties, the Unfair Contract Terms Directive (UCTD)[678] is of relevance for individuals and a good example of the intersection of data protection and consumer protection: the directive aims to protect consumers against unfair standard contract terms and applies[679] to all kinds of contracts on the purchase of goods and services.[680] Since the UCTD was developed for the offline world, the EP commissioned a study[681] to examine if it is necessary to amend[682] the directive to improve consumer protection and to provide more legal certainty.

5.3.15. Further relevant directives

Depending on the intended use and design of Artificial Intelligence, further directives may be relevant, and their importance may not at all be apparent at first sight: owing to the fact that Artificial Intelligence nowadays is part of autonomous weapons systems, the Directive on Intra-EU Transfers of Defence-Related Products[683] comes into play. Even the BioTech Directive[684] will be relevant since Big Data and AI become more and more instrumental in Life Sciences,[685] and few people may be aware of the fact

[677] The European Commission provides background information on both, the Injunctions Directive and the Representative Actions Directive on their website, available at https://commission.europa.eu/law/law-topic/consumer-protection-law/injunctions-directive-and-representative-actions-directive_en#evaluation. Retrieved January 7, 2023.

[678] The bill text is available at https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:31993L0013. Retrieved October 28, 2022.

[679] In addition, the Commission adopted a Guidance Notice on the interpretation and application of Directive 93/13/EEC to present the rich case law on this Directive and to facilitate effective application of the directive. Guidance Notice published July 2019, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.323.01.0004.01.ENG&toc=OJ:C:2019:323:TOC. Retrieved Retrieved October 28, 2022.

[680] Background information on the directive is provided by the Commission at their website, available at https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/unfair-contract-terms-directive_en. Retrieved October 28, 2022.

[681] The study has been published in April 2021, and is available at https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)676006. Retrieved October 28, 2022.

[682] The Directive has been amended by Directive (EU) 2019/2161 of 27 November 2019 on better enforcement and modernization of EU’s consumer protection rules, available at https://eur-lex.europa.eu/eli/dir/2019/2161/oj. Retrieved October 28, 2022.

[683] The text of Directive 2009/43/EC on intra-EU transfers of defence-related products is available at https://ec.europa.eu/growth/sectors/defence/transfers-products_en#:~:text=The%20transfer%20directive%20Directive%202009%2F43%2FEC%20on%20intra-EU%20transfers,for%20transfers%20of%20defence-related%20products%20within%20the%20EU. Retrieved October 2, 2021.

[684] The text of Directive 98/44/EC on the legal protection of biotechnological inventions is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31998L0044. Retrieved October 2, 2021.

[685] Arlindo Oliveira: Biotechnology, Big Data and Artificial Intelligence. Biotechnology Journal 2019, vol. 14, issue 8. The article is available at https://doi.org/10.1002/biot.201800613. Retrieved October 2, 2021.

that research has pushed so far as to store information and data in DNA: "DNA molecules can store up to 215 petabytes, or 215 million gigabytes, of data in a single doubled stranded molecule, making it one of the highest storage density mediums in the world (… which is much more) than we can currently create, so there has been a lot of focus in trying to harness the power and data storage capabilities of DNA for our (…) data storage systems."[686] The progress is such that at present, scientists are working on "Organoid Intelligence" (OI) by creating AI that uses real human cell brains.[687] In the context of further relevant directives, the long-awaited[688] ePrivacy regulation[689] may be of importance[690] as well because it would affect companies with new rules on electronic communications, direct marketing, nuisance calls, the use of cookies or metadata, and consent.[691] Latest developments point to important changes such as processing of data without consent to detect fraud, or to "protect users' vital interests" in the context of monitoring for the spread of epidemics[692] - an example of tangible consequence for individuals' privacy protections and choices. The proposed admissible further processing of pseudonymized metadata and device information may lead to uncertainty as criteria seem to be loosely defined,[693] and that is why some privacy rights organizations question whether this draft may erode privacy protections that have been included in previous versions.[694] In their press release[695], the Council stresses their awareness regarding cookie consent fatigue, but cookies may not be the issue in the long

[686] Liam Critchey: Storing information and data with DNA. Article published August 11 2020, available at https://www.electropages.com/blog/2020/08/storing-information-and-data-dna. Retrieved October 2, 2021.

[687] Hannah Docter-Loeb: Scientists now want to create AI using real human brain cells. Article published February 28 2023, available at https://www.vice.com/en/article/qjkgap/scientists-now-want-to-create-ai-using-real-human-brain-cells. Retrieved February 28, 2023.

[688] History and discussion points are summarized by the European Digital Rights (EDRi), an association of civil and human rights associations from across Europe at their website, available at https://edri.org/tag/eprivacy-regulation/. Retrieved October 17, 2021.

[689] The text of the proposal is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010. Retrieved October 17, 2021.

[690] Background information on the relationship between PECD and GDPR is provided by the law firm of Brinkhof Advokaten who prepared a paper in 2018 for CIPL, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf. Retrieved October 17, 2021.

[691] Ceyhun Pehlivan, Peter Church: EU: The ePrivacy regulation - let the trilogue begin! Article published February 12 2021, available at https://www.linklaters.com/en/insights/blogs/digilinks/2021/february/eu---the-eprivacy-regulation---let-the-trilogue-begin. Retrieved October 17, 2021.

[692] The lawfirm Hunton Andrews Kurth provided details on the final terms of the draft regulation in their 2021 blog: EU Member States Agree on Council's Text for the ePrivacy Regulation. Article published February 2021, available at https://www.huntonprivacyblog.com/2021/02/10/eu-member-states-agree-on-councils-text-for-the-eprivacy-regulation/. Retrieved October 17, 2021.

[693] Lara White, Fiona Bundy-Clarke: Tentative further steps towards an agreed ePrivacy Regulation. Article published February 15 2021, available at https://www.dataprotectionreport.com/2021/02/tentative-further-steps-towards-an-agreed-eprivacy-regulation/. Retrieved October 17, 2021.

[694] Marianno Delli Santi: ePrivacy Regulation – an open letter from 30 civil society organizations: our letter to the European Parliament asking them to stand up against online tracking. Article published April 14 2021, available at https://www.openrightsgroup.org/publications/eprivacy-regulation-an-open-letter-from-30-civil-society-organisations/. Retrieved October 17, 2021.

[695] Council press release: Confidentiality of electronic communications: Council agrees its position on ePrivacy rules. Press release published February 10 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/. Retrieved October 17, 2021.

run: Google started testing Federated Learning of Cohorts (FLoC)[696] to replace third-party cookies. Some commented that this technology is more harmful than cookies since it will "make your browser do the profiling (…) by boiling down your recent browsing activity into a behavioral label, and then sharing it with websites and advertisers."[697] On the occasion of the World Wide Web Consortium in early 2021, Google announced that it will not be introducing FLoC in the European Union for the time being.[698] The fact that Google is omitting an area to which GDPR applies suggests that there is awareness of the potential implications, and that FloC may indeed raise privacy concerns.[699]

5.3.16. Directives which are no longer in force but relevant

The following Directives are no longer in force, but they are useful to understand the developments, discussions, and the overall context:

5.3.16.1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

In 1995, the European Data Protection Directive[700] was created. It regulated the processing (including the collection, use, storage, disclosure, and destruction) of personal data within[701] the European Union. This directive was the first framework for data protection regulation at European Union level and an important component of the European Union's data protection rights for more than two decades. The directive intended to harmonize data protection law across Europe.[702] Due to the fact that Member States must transpose directives into national law, this directive served as basis for numerous national data protection laws throughout the European Union. Differences in terms of content and timing of implementation of the requirements lead to somewhat differing levels of privacy protection even within

[696] Background information is provided by Marshall Vale: Privacy, sustainability, and the importance of "and". Article published March 30 2021, available at https://blog.google/products/chrome/privacy-sustainability-and-the-importance-of-and/. Retrieved October 17, 2021.

[697] Bennett Cyphers for the Electronic Frontier Foundation: Google's FLoC is a terrible idea. Article published March 3 2021, available at https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea. Retrieved October 17, 2021.

[698] Allison Schiff: Google will not run FLoC origin tests due to GDPR concerns. Article published March 23 2021, available at https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/. Retrieved October 17, 2021.

[699] Dieter Petereit: Google wird seine Tracking-Alternative FLoC zunächst nicht in Europa einführen. Der Suchmaschinenriese will erst die rechtliche Basis klären. DSGVO-Verstöße können schließlich sehr teuer werden. Article published March 24 2021, available at https://t3n.de/news/huch-dsgvo-googles-floc-scheitert-1369031/. Retrieved October 17, 2021.

[700] The text of the Data Protection Directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046. Retrieved October 2, 2021.

[701] Details on the scope (applicability) can be found in Article 4 of the directive, see https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Retrieved October 2, 2021.

[702] Jürgen Kühling: Die Europäisierung des Datenschutzrechts – Gefährdung deutscher Grundrechtsstandards? C.H. Beck Publishing 2014, p. 12.

the European. This also resulted in cases of conflict between European and national law, especially when there were overlaps with other areas of law, for example competition laws, since data protection laws are not the only issue to address for marketing activities. As regards the processing of personal data, Article 6 (1) b of the Data Protection Directive stipulated that Member States shall provide that personal data must be "(…) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards". Rules on compatible processing of personal data including exceptions for statistical or scientific purposes are important for Big Data applications.

5.3.16.2. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

The Data Retention Directive[703] obliged electronic communication service providers to retain traffic and location data for a certain period. The directive was invalidated in 2014 in a cutting-edge decision: Even though it was recognized that the purpose of the directive genuinely satisfies an objective of general interest, the CJEU[704] concluded that the directive was incompatible with Article 7 and 8 of the Charter. The reason for this was that, if traffic and location data are taken as a whole, this provides for a detailed picture of individuals' private lives, and therefore constitutes a serious interference with fundamental rights to respect for private life and to the protection of personal data. In another case,[705] the CJEU found that the generalized retention of traffic and location data may affect the use of electronic communication and how users' exercise their freedom of expression guaranteed in Article 11 of the Charter. Even though this directive is no longer in force, it cannot be disregarded as the CJEU's decision may well serve as an indicator when it comes to judging storage periods.[706] Moreover, the battle for the retention (use) of traffic and location data of telecommunications is not over: several Member States are putting pressure on the European Council to adopt rules that allow for the retention of metadata of communications; their ideas are far-reaching and could change existing data protection rules.[707] Some Member States made it

[703] The text of the Data Retention Directive is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[704] CJEU press release: CJEU rules that the Data Retention Directive is invalid. Press release published April 8, 2014, available at https://edps.europa.eu/press-publications/press-news/press-releases/2014/press-statement-cjeu-rules-data-retention_en. Retrieved October 2, 2021.

[705] The text of CJEU's decision dated December 21 2016 on the Tele2 Sverige (cases C-203/15 and C-698/15) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62015CJ0203&from=EN. Retrieved October 3, 2021.

[706] Those that are not governed by explicit requirements, e.g., tax matters.

[707] Alexander Fanta: France, Spain push for new EU data retention law. Article published March 5, 2021, available at

to advocate for the introduction of provision allowing for data retention measures in the Council version of the ePrivacy Regulation.[708] In this regard, it is important to note that various national constitutional courts[709] as well as the European Court of Justice continue with decisions that limit data retention measures.[710]

5.4. General Data Protection Regulation

It is impossible to examine the existing legal framework for Big Data and Artificial Intelligence from a data protection perspective without having a look at the core of EU's data protection regulation, the GDPR: the General Data Protection Regulation is a milestone in privacy regulation[711] and has served as a role model for many other data protection laws.[712] GDPR sets forth important principles like accountability, lawfulness, fairness and transparency, purpose and storage limitation, data minimization, accuracy as well as integrity and confidentiality[713] and introduced novelties like the right to data portability or obligatory report of data breaches.[714] However, GDPR also poses challenges, be it because of its extra-territorial scope and new sanctions, or because of new requirements, and indeterminate legal terms.

https://netzpolitik.org/2021/urgently-needed-france-spain-push-for-new-eu-data-retention-law/. Retrieved October 3, 2021.

[708] The text of the Council version of the ePrivacy Regulation is available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf. Retrieved October 3, 2021.

[709] Marek Zubik, Jan Podkowik, Robert Rybski: European constitutional courts towards data retention laws. Springer Nature Switzerland AG 2021.

[710] For example, in K. v. Prokuratuu (Case C-746/18H): The European Court of Justice found that crime must be serious to allow for access to traffic and location data, this way limiting data retention measures. Background information is provided by the European Agency for Human Rights, available at https://fra.europa.eu/en/caselaw-reference/cjeu-case-c-74618-judgment. Retrieved October 3, 2021.

[711] Anne Toth: New EU data protection law is a milestone in privacy regulation. Article published May 23 2018, available at https://www.thenationalnews.com/business/technology/new-eu-data-protection-law-a-milestone-in-privacy-regulation-1.733347#:~:text=New%20EU%20data%20protection%20law%20a%20milestone%20in,half%20a%20billion%20European%20A%20European%20Union%20flag. Retrieved May 20, 2022.

[712] For example, Brazil: See Robert Pocklington: The General Data Protection Act (LGPD) in Brazil: "the Brazilian GDPR". Article published September 30 2021, available at https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/general-data-protection-act-lgpd-brazil-brazilian-gdpr-2021-09-30_en. Retrieved July 22, 2022.

[713] See GDPR Art. 5.

[714] Background information on GDPR breach requirements is provided by the EDPB in their Guidelines 9/2022 on personal data breach notification under GDPR. Guidelines published October 2022, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en. Retrieved October 25, 2022.

5.4.1. Scope

The Data Protection Directive's territorial scope comprised Member States and non-EU members which are a part of the European Economic Area.[715] In comparison to the Data Protection Directive, the scope of the GDPR was expanded: the extra-territoriality principle is one of the biggest changes,[716] for good reason: personal data is collected and shared globally, and therefore, inconsistent (national) data protection laws are neither appropriate nor timely.[717] GDPR captures much more overseas organizations, because it does not only apply to organizations which are established within the European Union: according to GDPR Article 3 (1), the "Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". Recital 22 says that an "establishment implies the effective and real exercise of activity through stable arrangements" and clarifies that "the legal form of such arrangements (…) is not the determining factor". This leads to the result that there is a wide spectrum of what might be captured by the GDPR; depending on the circumstances, perhaps even single individual sales representatives may fall under the Regulation. In 2014, the CJEU ruled that that Google Inc. with EU based sales and advertising operations in Spain was established within the EU.[718] The court delivered another landmark ruling in 2015 in the so-called Weltimmo-case. The court considered the meaning of establishment and concluded that, because Weltimmo pursued real and effective activity in Hungary, it had an establishment in Hungary and is therefore subject to Hungarian data protection laws, even if Weltimmo is a Slovakian property website.[719] Weltimmo was thus subject to both, Hungarian and Slovakian data protection laws, i.e., the data protection of its home country. This decision dates to 2015 when GDPR was not valid yet, and it is interesting insofar as the Regulation envisages that companies will only have to deal with one single DPA,[720] typically the supervisory authority in the member state in which the company has its EU headquarters. What is more important, GDPR may also be applicable[721] when the company has no establishment within the European Union. An organization

[715] Iceland, Liechtenstein and Norway; Switzerland is a member of EFTA but does not take part in the EEA, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aem0024. The adequate protection of personal data in Switzerland was acknowledged by the Commission, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518. Retrieved October 24, 2021.

[716] Ivan Klekovic: EU GDPR vs. European data protection directive. Article published October 30 2017, available at https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/. Retrieved July 22, 2022.

[717] Christopher Kuner, Fred Cate, Christopher Millard, Dan Svantesson: The challenge of Big Data for data protection. International Data Privacy Law 2012, vol. 2, no. 2, p. 48.

[718] The court's decision in case C-131/12 dated February 27, 2012 is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=DE.

[719] The judgment of the court in case C-230/14 dated October 1 2015 is available at http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN. Retrieved October 24, 2021.

[720] See article 60 GDPR, the "cooperation between the lead supervisory authority and the other supervisory authorities concerned", also called "one-stop-shop"-mechanism.

[721] Or may not be applicable, see CNIL's decision on a US company providing a browser extension: Dan Cooper, Alix Bertrand, Diane Valat: French CNIL finds GDPR not applicable to a US company providing a browser extension. Article published January 5, 2023, available at https://www.insideprivacy.com/eu-data-

is still caught by the Regulation if it processes personal data of data subjects who are in the Union and where the processing activities are related to "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union".[722] Internet use profiling (Recital 24) is expressly referred to as an example of monitoring. Recital 24 underlines that the latter example refers to processors not established in the Union "if data subjects within the Union are profiled". The Regulation thus shifts its focus to the country of destination, and especially Recital 24 shows that, even though there is no single specific article on marketing, GDPR indeed targets the advertising industry if profiling and online tracking techniques are used. This approach is consequent as it means that companies who want to benefit from the European market will have to stick to EU rules. Finally, in order to allow for supervisory authorities to communicate with companies established outside the EU, the Regulation stipulates that a representative must be appointed.[723] Companies may not be able to escape or avoid GDPR's extra-territorial approach, but It remains to be seen whether companies will be able to forum shop by assigning their representative in a country where the supervisory authority is known to be rather tolerant as GDPR Article 27 (3) allows that the "representative is established in one of the Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are." The Directive focused on those who determined purposes and means of the processing, and this way, it primarily addressed controllers. Under the Directive, processors were subject to obligations which were imposed on them through contractual relationships with data controllers. This became particularly evident in the case of "processing chains" when the general contractor had to ensure that all other suppliers who act as data processors observe the contractual regulations laid down by the controller. In contrast, GDPR imposes direct obligations on data processors, i.e., entities and suppliers which are engaged by a controller to process personal data on their behalf. Under the GDPR, processors are required to obey numerous specific obligations, for example the maintenance of records of processing activities,[724] performance of impact assessments,[725] the implementation of appropriate security standards,[726] the appointment of a Data Protection Officer, if need be,[727] and the obligation to cooperate with supervisory authorities.[728] Just like controllers, processors may be liable to sanctions if they fail to meet these requirements and they may also face claims for compensation. Moreover, GDPR changed the definition of personal data to reflect technological changes and the way that personal information is used: comparatively, under the Data Protection Directive, personal data was defined as data such as names, photos, email addresses,

protection/french-cnil-finds-gdpr-not-applicable-to-a-us-company-providing-a-browser-extension/. Retrieved January 7, 2023.

[722] See GDPR Article 3 (2a, b).

[723] See GDPR Article 2.

[724] See GDPR Article 30 (2).

[725] See GDPR Article 35.

[726] See GDPR Article 32.

[727] See GDPR Article 37.

[728] See GDPR Article 31.

phone numbers, addresses, and personal identifiers like social security numbers; under the GDPR, personal data is defined as any information that could be used, on its own or in conjunction with other data, to identify an individual.[729] Despite these differences, it is important to underline the continuity between the Data Protection Directive and the General Data Protection Regulation as many general data protection principles like the accountability, use limitation and purpose specification or the security safeguards principle which are also common to other privacy frameworks[730] are maintained and / or enhanced.

5.4.2. Sanctions

5.4.2.1. Administrative fines

An important change under the Regulation is that businesses, in the event that they fail to comply with GDPR requirements, may be liable to pay fines of up to four percent of the annual worldwide turnover or 20 million Euros, whichever is higher.[731] In comparison to the previous legal setting under the Directive and national legislations,[732] this is a substantial increase in the maximum possible fine, especially given the fact that such fines are not calculated on the basis of a local entities' turnover:[733] The term undertaking is defined in GDPR Article 4 (19), and Recital 150 says that undertaking shall be understood "to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes". Even though the TFEU does not define the term undertaking and despite of the fact that, like in every legal field, extensive case law must be considered, it may be assumed that a group of companies shall be regarded as part of the same undertaking; the concept of an undertaking encompasses every entity that engages in economic activities regardless of its legal status or how the entity is financed. Fines will therefore not be imposed by reference to the individual controller or processor, but by revenue of an undertaking, and GDPR this way follows the broad definition of undertaking in anti-trust and anti-bribery laws. This conceptual change represents a high impact for businesses and may thus lead to data protection being taken seriously in terms of compliance risk. This is especially true for multinational businesses as group revenues will be taken into consideration when calculating fines. This is underlined

[729] Samantha Beaumont: The data protection directive versus the GDPR: understanding key changes. Article published March 6 2018, available at https://www.grcworldforums.com/gdpr/the-data-protection-directive-versus-the-gdpr/26.article#:~:text=%20The%20data%20protection%20directive%20versus%20the%20GDPR%3A,vs.%20Data%20Processors.%20A%20key%20difference...%20More%20. Retrieved July 22, 2022.

[730] For example, the 1980 OECD Privacy Principles, available at http://www.oecdprivacy.org/ or the 2004 APEC Privacy Principles, available at http://www.cyberlawcentre.org/ipp/apec_privacy_framework/apec_draft_v9.htm#3. Retrieved May 22, 2022.

[731] See GDPR Article 83.

[732] For example, the maximum fine in Germany prior to GDPR was 300000 EUR (§ 43 of the former German federal data protection law, BDSG).

[733] Carlo Piltz: How German data protection authorities interpret the GDPR. Article published July 5 2017, available at https://www.delegedata.de/2017/07/how-german-data-protection-authorities-interpret-the-gdpr/. Retrieved October 24, 2021.

by the fact that national data protection supervisory bodies will be coordinating their work across EU Member States, which will likely lead to a more pronounced enforcement, especially in an international context as the so-called “one-stop-shop” principle[734] shows: Even though this principle only applies to cross-border cases where the supervisory authority (SA) of the main establishment of the controller or processor will be competent to act as the lead SA and serve as a “one-stop-shop” to supervise all processing activities of that business, this mechanism is a perfect example of a cooperation procedure between several supervisory authorities and will thus ensure the desired consistency in law enforcement in the area of data protection. Various national SAs will have to ensure [735] the demand that administrative sanctions are effective, proportionate, and dissuasive,[736] which of course depends on the case in question. There has been a trend towards more drastic fines, and European data protection supervisory authorities announced the following penalties for GDPR violations:[737] TikTok: € 5 million,[738] Apple: € 8 million,[739] Vodafone: € 12 million,[740] Marriott: £ 18 million,[741] Google: € 50 million,[742] WhatsApp: € 225 million,[743] or Microsoft with € 60 million[744] and Meta with € 390[745] million and € 725 million;[746]

[734] See GDPR Article 60.
[735] Based on EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR. Guidelines published May 16 2022, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en. Retrieved January 7, 2023.
[736] See GDPR Article 83 (1).
[737] These examples are neither representative nor conclusive.
[738] CNIL fined TikTok for lack of transparency and lack of users’ choices. Decision published December 29 2022, available at https://www.cnil.fr/en/cookies-cnil-fines-tiktok-5-million-euros. Retrieved January 7, 2023.
[739] The French data protection authority fined Apple for its targeted advertising practices. Decision published December 22 2022, available at https://www.cnil.fr/en/advertising-id-apple-distribution-international-fined-8-million-euros. Retrieved January 7, 2023.
[740] The EDPB reports about the case: Aggressive telemarketing practices – Vodafone fined over 12 million Euro by Italian DPA. Statement published November 19 2020, available at https://edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en. Retrieved October 24, 2021.
[741] ICO fined Marriott International Inc for failing to keep customers’ personal data secure. Decision published October 30 2020, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/. Retrieved October 24, 2021.
[742] CNIL fined Google on January 21 2019. The regulator provides background on their decision on their website, available at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Retrieved October 24, 2021.
[743] The Irish Data Protection Commission fined WhatsApp on September 2 2021. The regulator provides background on their decision on their website, available at https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry. Retrieved October 24, 2021.
[744] CNIL fined Micorosoft on December 22 2022. The regulator provides background on their decision on their website, available at https://www.cnil.fr/en/cookies-microsoft-ireland-operations-limited-fined-60-million-euros?mkt_tok=MTM4LUVaTS0wNDIAAAGJF8ZRz37NoOE53B2LFnmWoShMFIuVifVL5e3BlhE0qNyD7Ku-Du5ycsZx2XGgFv0ENwYfHQbAKq5qwRUYulP_K62PCCuDGzuxwIO1bKjt2O4y. Retrieved December 30, 2022.
[745] Jennifer Bryant: Irish DPC fines Meta 390M euros over legal basis for personalized ads. Article published January 4 2023, available at https://iapp.org/news/a/irish-dpc-fines-meta-390m-euros-over-legal-basis-for-personalized-ads/. Retrieved January 7, 2023.
[746] The Irish data protection commission fined Meta on November 28 2022. The regulator provides background on their decision on their website, available at https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry. Retrieved December 30, 2022.

Amazon holds the record for one of the highest penalties ever imposed to date with € 746 million.[747] However, sanctions and fines under GDPR, member-state data privacy and administrative as well as business criminal law are not the same: certain Member States do not foresee for fines[748], other laws foresee that there must be a link to linked to a concrete, reproachable act of a natural person, which is not the same as the (group of) undertaking.[749] In addition, several cases have shown that regulator fines under GDPR may be contested[750], for a variety of reasons,[751] meaning that it is perhaps not as easy as envisaged to successfully issue penalties for GDPR violations. National data protection supervisory authorities came up with their own fine calculation models[752] to help standardize how fines are calculated. Most importantly, the European Data Protection Board published guidelines on the calculation of administrative fines under the GDPR[753] to ensure data protection authorities use the same methodology for the calculation of fines. It is believed that this shall help with the harmonization and transparency of the fining practice of DPAs.[754]

5.4.2.2. Enforcement powers

Apart from administrative fines, supervisory authorities are provided with wide-ranging powers[755] to enforce compliance with the Regulation, for example the right to issue warnings, to perform audits, the power to compel a controller or processor to provide any information which is relevant to the

[747] The Grand-Duchy of Luxemburg's National Commission for Data Protection fined Amazon Europe Core S.à r.l. on August 6 2021. The regulator provides background on their decision on their website, available at https://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html. Retrieved October 24, 2021.

[748] See Recital 151 that refers to Denmark and Estonia.

[749] Max Adamek, Julian Räder: DSGVO-Verstöße und das OWiG. Article published August 20 2021, available at https://haerting.de/wissen/dsgvo-verstoesse-und-das-owig/#:~:text=Gem.%20%C2%A7%2030%20Abs.%201%20Nr.%205%20OWiG,handelt%20und%20eine%20Straftat%20oder%20Ordnungswidrigkeit%20begangen%20hat. Retrieved January 22, 2022.

[750] The consultancy Datenschutz Lübbecke reports on a case in Berlin where a 14 million Euro fine was not successful because the fine imposed by the state data protection authority contained significant deficiencies: Peinlicher Vorfall: Deutsche Wohnen entkommt DSGVO-Bußgeld in Millionenhöhe. Article published February 24 2021, available at https://datenschutz-luebbecke.de/blog/peinlicher-vorfall-deutsche-wohnen-entkommt-dsgvo-bussgeld-in-millionenhoehe/#:~:text=Blamage%20f%C3%BCr%20die%20Datenschutzbeh%C3%B6rde%20in%20Berlin%3A%20Allem%20Anschein,Beschluss%20vom%2018.%20Februar%202021%20eingestellt%20worden%20ist. Retrieved January 22, 2022.

[751] Alexander Fanta: Millionenstrafe gegen Österreichische Post AG aufgehoben. Article published December 2 2020, available at https://netzpolitik.org/2020/dsgvo-millionenstrafe-gegen-oesterreichische-post-ag-aufgehoben/. Retrieved December 18, 2020.

[752] Susanne Werry: New German model for the calculation of GDPR fines - a blueprint for Europe? Article published October 21 2019, available at https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2019/10/new-german-model-for-the-calculation-of-gdpr-fines.html. Retrieved January 22, 2022.

[753] EDPB's Guidelines 04/2022 on the calculation of administrative fines under the GDPR have been published May 16 2022, and are available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en. Retrieved July 22, 2022.

[754] EDPB Chair Andrea Jelinek comments on the adoption of Guidelines 04/2022. Statement published May 16 2022, available at https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-calculation-fines-guidelines-use-facial-recognition_en. Retrieved July 22, 2022.

[755] See GDPR Article 58 (1 a).

performance of supervisory authority's duties as well as the possibility to impose a ban on processing.[756] Given the large number of conceivable infringements, which must always be assessed individually, it is difficult to tell how different supervisory authorities will implement their enforcement powers. Even though the GDPR has not been in force for long, the multitude of regulators that govern the use of personal information, the processing with the help of AI, including further bodies like the FTC or supervisory authorities in charge of competition law or consumer protection – set aside legal proceedings for claims for damages – shows that overlapping responsibilities could be problematic.

5.4.2.3. Representation of data subjects

On top of GDPR's administrative sanctions, the Regulation also allows for non-for-profit bodies, organizations or associations which are active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data and which disposes of statutory objectives that are in the public interest to lodge a complaint on behalf of the data subject and to exercise data subjects' rights including the right to receive compensation.[757] It is moreover necessary that such an association has been properly constituted in accordance with the law of a member state, meaning that not each and every NGO has the right to represent data subjects. Although this is not the same as a U.S. style class action, this novelty increases the risk of group privacy claims, and this type of actions leads to further pressure to observe the new rules as business typically fear potential negative consequences for public opinion. Another fact to consider is emerging legal tech: the number of providers who are offering assistance for individuals to exercise their data subject rights is growing,[758] and this poses further challenges, for example, in identification and valid representation of the individuals behind those claims.

5.4.2.4. Claims by individuals

Claims under competition law by competitors and contractual claims by business partners are not at all a new phenomenon; these risks are part of business life, but what is new is that GDPR makes it considerably easier for individuals to bring private claims against data controllers or processors: GDPR Article 81 (1) states that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered". The inclusion of non-material damage means that claims of

[756] See GDPR Article 58 (1 f). This shall be considered during the introduction of new tools, especially when there is a need to exchange with the works council for corresponding agreements.

[757] See GDPR Article 80.

[758] For both, data subjects and controllers, the market for DSAR automation is growing. It is estimated that already now, the industry has a three digit number of specialist vendors, see Datagrail background information provided at their website, available at https://www.datagrail.io/blog/product/gartner-subject-rights-requests-2021/. Retrieved October 24, 2021.

individuals are not limited to financial loss; even distress may justify a claim under GDPR Article 81. Recent developments show that there seems to be a trend to use data subject rights under GDPR to enforce other claims, namely in the context of severance claims in termination actions under labor law, which some consequently name as the “golden handshake”.[759]

5.4.3. GDPR’s goals

5.4.3.1. Broad applicability

GDPR’s broad applicability is not only due to the broader material and territorial scope, it is also based on the fact that the Regulation has a broader definition of personal data. Personally identifiable information such as online identifiers is explicitly included, and it is important to note that Recital 26 not only sets a low bar for the prerequisite "identifiable", but it also makes clear that personal data can be given despite the fact that the organization which holds the data cannot itself identify a natural person: the only requirement is that, if anyone can identify a natural person using all means reasonably likely to be used, the relevant data may be considered personal data.[760] Businesses are often not aware that, even though they might not be able to read a set of data, the same set of data is subject to data protection law. The effect of broader applicability also applies to special categories of data whose definition was also broadened in GDPR Article 9 as genetic and biometric data were expressly included. While a few decades ago, for example iris-scans were only used in movies, today, every modern smartphone can be unlocked by using a fingerprint. The increase in technical applications with security features which process biometric data has led to a proportional increase in the applicability of data protection law – with all data protection, security law and sector-specific consequences. Another point to consider is that the volume of data that is being produced rises at an incredible rate, because people dispose of more devices that generate more data, which again leads to a broader applicability of data protection laws.[761]

[759] Niko Härting: Mit der DSGVO zum “Golden Handshake” – von der Sprengkraft des “Rechts auf Kopie”. Article published March 29 2019, available at https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/. Retrieved October 24, 2021.

[760] GDPR Recital 26, sentence 3 and 4: “To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments”.

[761] GDPR itself explains the development in Recital 6: “Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life.“

5.4.3.2. Uniform applicability

GDPR's broad applicability must be distinguished from the intended uniform applicability of the Regulation: GDPR clearly aims at ensuring a consistent and high level of protection of the rights and freedoms of natural persons with regards to the processing of their data,[762] and that can only be achieved if that level is equivalent in all Member States. Even though a consistent and homogenous application of data protection laws is desired throughout the European Union, GDPR Article 23 clearly says that member state law may restrict "by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard national security, defense, (…)". This is just one example out of dozens of exceptions[763] for the regulatory scope of national legislators. It can therefore be said that the intended harmonization is relative insofar as many important issues and areas of law continue to be governed by national laws. Moreover, chapter IX of GDPR sets out various processing operations which include additional derogations and exemptions[764] such as processing and freedom of expression and information, processing and public access to official documents, processing of national identification numbers and processing in the context of employment.

5.4.3.3. Focus on accountability

Many of the principles laid down in GDPR Article 5 were also incorporated in the Data Protection Directive, for example the principle of purpose limitation or the principle of data minimization: Article 6 of the Directive stipulated that "personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. (…) (c) adequate, relevant, and not excessive in relation to the purposes for which they are collected and / or further processed (…)" and concluded with the statement in paragraph 2 that "it shall be for the controller to ensure that paragraph 1 is complied with". In contrast, Article 5 (2) of the Regulation requires that the controller is responsible for and must be able to demonstrate compliance with all data protection principles. The difference is that, even though most of the standards existed before, the focus on accountability requires that the lawfulness of processing activities is established, meaning that there is a burden of proof obligation that business operations are compliant with the

[762] GDPR Recital 10.

[763] Lukas Feiler provides an overview over the topic in his presentation: Die 69 Öffnungsklauseln der DSGVO. Presentation held on behalf of the law firm of Baker & McKenzie/Diwok Hermann Petsche Rechtsanwälte LLP & Co KG in Vienna during the meeting of JusIT on June 1, 2017, available at http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf. Retrieved October 24, 2021.

[764] See GDPR Articles 85, 86, 87 and 88.

Regulation. And the relief some expected due to, for example, the law not insisting on written format for consent, is not given as consent must be verifiable, meaning that the controller must obey documentation requirements. And there are numerous further documentation requirements, for example, for legitimate interest assessments,[765] the collection and processing of special category data,[766] or age verification,[767] to name a few. The accountability principle has become a core element of data protection in many other jurisdictions, for example Australia, Canada, or Singapore.[768] Accountability leads to greater efforts with regards to the documentation of processes, the performance of controls, the conclusion of (outsourcing) contracts, and the overall legality of decisions including providing proof of legal grounds for processing which allow controllers to be able to demonstrate compliance. The accountability principle primarily manifests itself in documentation obligations, namely records of processing activities[769] and the performance of data protection impact assessments.[770] While the latter only applies to high risk processing, records of processing activities have to be present for every single data processing activity the controller carries out.[771] Provided that Big Data and AI applications may pose high risks to the rights and freedoms of individuals, it is likely that many such processing activities will result in the creation of impact assessments, particularly when profiling is in question, when sensitive personal data are processed or when publicly accessible areas are systematically monitored on a large scale.[772] Other mandatory requirements include the implementation of Privacy by Design and Privacy by Default,[773] the establishment of mechanisms for data breaches[774] and responses to data subject requests.[775] The designation of a Data Protection Officer is necessary, either when certain conditions are met or when Union or Member State requires that a DPO is appointed.[776] This is yet another example of how the situation will continue to vary from one Member State to another, even with mandatory requirements. Data controllers may, on a voluntary basis, also opt for certification

[765] See GDPR Article 6 (1) lit. f.

[766] See GDPR Article 9.

[767] GDPR Article 8 (1).

[768] The law firm Hunton Andrews Kurth refers to the results of the 2018 intelligence gathering operation on organizations' data privacy accountability practices which was carried out by GPEN, a global network of more than 60 DPAs around the world. Article published March 5 2019, available at https://www.huntonprivacyblog.com/2019/03/11/gpen-and-national-dpas-publish-sweep-results-on-privacy-accountability/. Retrieved October 24, 2021.

[769] See GDPR Article 30.

[770] See GDPR Article 35.

[771] The issue was solved inconsistently in previous data protection laws within the EU; in some jurisdictions (for example in Austria), there was a requirement to notify the national data protection authority of data processing operations. In others, e.g., in Germany, this requirement was not applied as a general rule as the controller was obliged to maintain the relevant documentation and to provide it to the DPO for checking purposes (see § 4 e, g of the pre-GDPR-BDSG). Under GDPR, there is a general necessity to keep extensive internal records of data protection activities.

[772] See Recital 91 which provides background information and examples for data protection impact assessments.

[773] See GDPR Article 25.

[774] See GDPR Articles 33 and 34.

[775] See GDPR Articles 15 or 20.

[776] See GDPR Article 37 (4).

mechanisms to demonstrate compliance.[777] Some criticize voluntary or self-regulation because might be an escape from regulation,[778] and that is why it makes sense to explore the existing legal framework that already provides for joint controllership, accuracy, or accountability. But the question is whether accountability as set forth in existing data privacy laws goes far enough to guarantee responsibility, liability, contestability, safety, and fairness together with an approach to data processing that includes sound risk assessment and human oversight and human intervention if need be. Another problem with the application of existing legal principles of data protection is that there is a risk of trade-offs between different data protection principles: more data may lead to more accuracy, but at the expense of individual's privacy; if AI is tailored to avoid discrimination, i.e., if certain indicators are removed to that AI is fair, this may have an impact on accuracy.

5.4.3.4. Enhanced transparency

Transparency is a central principle in the GDPR because it promotes the objective of strengthening individuals' rights and underlines the importance of the lawfulness of processing personal information. Processing is only lawful if it is fair and transparent, and that is why any communication towards data subjects must be concise, transparent, intelligible and easily accessible, and use clear and plain language.[779] In connection with transparency requirements, one is immediately tempted to think about one specific use case: privacy notices on website that must be provided at the time data is collected.[780] But much of the content that is displayed as mandatory information on websites in fact is not solely based on data protection law. For example, neither the imprint nor terms and conditions or payment information is a genuine data protection issue; this is rather about consumer protection and provider identification, in some cases extended with information on the competent regulatory authority.[781] A positive development could be that GDPR's requirements might have already changed users' perceptions since information obligations apply in many scenarios: on websites, in apps, during the application process, etc. But at the same time, a negative consequence is that this may lead to users being overwhelmed with information which in turn leads to information fatigue.[782] Transparency requirements

[777] ICO: GDPR guidance – contracts and liabilities between controllers and processors. Guidance published September 2017, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Retrieved October 24, 2021.

[778] Ben Wagner: Ethics as an escape from regulation. From ethics-washing to ethics-shopping? In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds,): Being profiled – cogitas ergo sum. 10 years of profiling the European citizen. Amsterdam University Press 2018, pp. 84-88.

[779] See GDPR Article 12 (1).

[780] See GDPR Articles 13 and 14.

[781] This is mandatory for certain professions and subject to national legislation.

[782] Müge Fazlioglu: Transparency and the GDPR: Practical guidance and interpretive assistance from the Article 29 Working Party. Article published December 14 2017, available at https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/. Retrieved September 25, 2021.

are sometimes difficult to implement,[783] and more importantly, they are limited even when automated decision-making including profiling is in question because controllers are not required to provide all kinds of information,[784] not to mention protected business information. Trade secrets are only one reason for limitations, general information asymmetries[785] are another aspect to consider, and the information mismatch goes hand in hand with the imbalance of powers between the parties and adds to dilemma data subjects face. The GDPR made a genuine effort to better inform individuals, but the Regulation also removed the need to register with supervisory authorities and notify them for certain endeavors,[786] which shows that GDPR is predominantly concerned with transparency towards affected individuals. While it must be recognized that transparency truly is an elusive goal because it is difficult to explain processing operations and / or decisions made by a multitude of algorithms that work together, transparency is decisive from the individual's perspective, but in many instances, information obligations are fulfilled in a legalistic manner. But they could be further developed in the direction of comprehensive and meaningful, repetitive[787] and public[788] information to allow for explainability that addresses not only affected individuals, but a wider audience, for example, by establishing public databases for high-risk processing operations allowing any interested party to access relevant information such as details on risk evaluations, mitigation measures and information on sub-processors since various service providers may be involved in data processing. AI's potential for opaqueness and its ability to act in unforeseeable ways adds to the fear that certain types of AI systems may leave data subjects with insufficient information about how their data is treated. That is why some think about the introduction of labeling obligations or mandatory watermarks for AI generated content,[789] and others stress the necessity to concretize transparency obligations to the effect that information must be provided

[783] For example, in the case of CCTV or when buying a personalized train ticket when the journey has already begun. There are numerous scenarios in which full transparency about the data processing is only feasible with the help of a multi-step approach. Background information on the so-called layered approach in the context of transparency obligations is provided by the ICO, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/#how2. Retrieved September 25, 2021.

[784] Sandra Wachter, Brent Mittelstadt, Luciano Floridi: Why a right to explanation of automated decision-making does not exist in the GDPR. International Data Privacy Law 2017, vol. 7, issue 2, pp. 76-99. Retrieved September 25, 2021.

[785] Masooda Bashir, Carol Hayes, April Lambert, Jay Kesan: Online privacy and informed consent – the dilemma of information asymmetry, Proceedings of the Association for Information Science and Technology 2015, vol. 52, issue 1, pp. 1-10, available at https://doi.org/10.1002/pra2.2015.145052010043. Retrieved October 23, 2021.

[786] For instance, in Austria, where § 16 of the Federal Austrian Data Protection Law (DSG 2000) required companies to do so. Background information is available at the official (archived) website https://web.archive.org/web/20161220005959/https://www.dsb.gv.at/rechtsgrundlagen-und-beschreibung. Retrieved October 24, 2021.

[787] See GDPR Article13 III.

[788] Website information may already be considered as public information, but compared to public registries or databases, details and reach are different.

[789] For example, watermarks for AI generated content and texts, see Christoph Cemper: 13 AI content detection tools tested and AI watermarks. Article published December 29 2022, available at https://www.linkresearchtools.com/blog/ai-content-detector-tools/. Retrieved January 10, 2023.

on the scope and actual effects, not only basics on the underlying logic, and not only when there are significant legal implications, but in any profiling scenario.[790]

5.4.3.5. Strengthening of data subject rights

Data subject rights have been rights have been extended: the right to information and the right to access existed before, but the right to data portability and the explicit right to be forgotten are genuine novelties. Subject access rights must be answered during a certain period of time,[791] and given that the maximum period to answer such requests is three months, that sounds feasible, but the scope of this data subject right poses challenges,[792] especially when raised in combination with claims for damages in the context of termination actions under labor law. Practical problems also arise out of the right to request information or a copy of personal data by electronic means:[793] first, the controller has to make sure that he is answering to the correct person, i.e., the data subject whose data are in question; second, answering by electronic means must not mean that a simple e-mail can be used for communicating with the date subject unless encryption is used. This would necessarily lead to a violation of GDPR Article 32, security of processing. That means that something as simple as a demand by email necessarily leads to additional processes, primarily the identification of the individual.[794] This is the mandatory first step businesses need to think about, and depending on their business model (B2B or B2C) and the number of incoming requests, it is conceivable that data subject rights are resolved e.g. by the implementation (further customization) of a customer portal[795] including relevant log-in data in order to verify and ensure that the right person requests the right information. Such a self-service would also be valuable for other data subject rights, for example the right to copy of their data. At present, the relationship between the right to information about personal data and the right to a copy of personal data is unclear; guidance at national or local authority level[796] is not always helpful as not all SAs explain the scope and relationship between

[790] Alexander Roßnagel, Christian Geminn: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. Report published November 26 2019, available at https://www.heise.de/downloads/18/2/8/0/2/5/0/7/vzbv.pdf. Retrieved October 20, 2021.

[791] As a basic rule, such requests shall be answered within one month; this period may be extended by two further months where necessary, e.g., in the event that the request is of complex nature: see GDPR Article 12 (3).

[792] For example, because it was questionable whether data subject must be informed about recipients. The European Court of Justice ruled that the controller must provide the actual identity of recipients, unless it is impossible to identify them or the data subject's requests are manifestly unfounded or excessive: Curia Case C-154/21, available at https://curia.europa.eu/juris/liste.jsf?language=en&num=C-154/21. Retrieved January 10, 2023.

[793] See GDPR Article 12 (3).

[794] The State Commissioner for Data Protection and Data Security in the German state of Baden-Württemberg dealt with this neglected topic. Their findings are available in the corresponding press release published February 6, 2019, available at https://www.baden-wuerttemberg.datenschutz.de/identitaetspruefung-bei-elektronischen-auskunftsersuchen-nach-art-15-ds-gvo/. Retrieved October 24, 2021.

[795] Recital 63 deals with the issue of providing data subjects with remote access to their data.

[796] Some countries have more than just one regulator in charge of data protection, for example, Germany. A list of local German SAs is provided by the federal German Information Commissioner, available at https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html. A list of European national data

those rights,[797] however, the situation became clearer since the EDPB dealt with the matter.[798] Some local data protection authorities seem to suggest that a copy could be considered the format of the right for information or equal to the right to access,[799] others quote Recital 63 and argue that the scope of the right to a copy is limited by trade secrets or intellectual property rights and / or rights and freedoms of others.[800] Others think about the possibility that data subjects shall be provided with an "overview" over their data as a simplified first step of information rather than enabling them to access all data the controller holds about them.[801] The right to access should be interpreted broadly as the opposite would lead to a limitation of data subject rights, especially as information is the basis for many other initiatives data subjects might want to take. But Recital 63 says that, if the "controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specifies the information or processing activities to which the request relates". Moreover, the European Court of Justice ruled[802] that the right to access shall not be interpreted in a manner that allows data subjects to request full duplicates of datasets, but that it is sufficient to provide the information in the form of an overview of the stored data. Even though the decision dates back to 2014 and thus refers to the Directive, it may still be considered applicable as the rationale the ECJ quoted remained the same in the Regulation, i.e. to enable the data subject to obtain knowledge of their data and to verify that it is accurate and processed in accordance with applicable laws with the goal to put the data subject in a position to examine further rights if need be. The aforementioned challenges with identification and secure transmission of information may lead to manual process which may result in data being provided on a mobile storage device and sent to a postal address at which a person is officially registered as this is the address a controller can legally rely upon. This is ironic insofar as the legislator intended to enhance data subject rights and to facilitate a smooth and easy way of communication and exchange. Not only does this problem not fit in the digital age; the solutions

protection agencies is provided by the EDPB and available at https://edpb.europa.eu/about-edpb/about-edpb/members_en. Retrieved October 24, 2021.

[797] For instance, the German DSK paper: Auskunftsrecht der betroffenen Person nach Art. 15 DSGVO. Paper published 2017, available at https://www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf. Retrieved October 24, 2021.

[798] EDPB Guidelines 01/2022 on data subject rights -right of access. Guidelines published January 28 2022, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en. Retrieved March 24, 2022.

[799] For example, the short-paper of the Bavarian supervisory authority which oversees the private sector: EU-Datenschutz-Grundverordnung - Das BayLDA auf dem Weg zur Umsetzung der Verordnung. Paper published 2017, available at https://www.lda.bayern.de/media/baylda_ds-gvo_16_right_of_access.pdf. Retrieved October 24, 2021.

[800] See GDPR Article 15 (4).

[801] Intersoft Consulting Services: Die Kopie von personenbezogenen Daten im Auskunftsanspruch. Article published on their company website on March 8 2019, available at https://www.datenschutzbeauftragter-info.de/die-kopie-von-personenbezogenen-daten-im-auskunftsanspruch/. Retrieved October 24, 2021.

[802] The court's decision in joined cases C-141/12 and C-372/12 dated July 17 2014 is available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=DD36E0EFF4D8F25CEA8CC48A373DDE4C?text=&docid=155114&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3639809. Retrieved October 24, 2021.

that have so far been presented for identification purposes[803] (and for avoidance of mistakes, i.e., data breaches) all have in common that they are in potential conflict with the principle of data minimization, because they all require even more information. Most potential solutions suggest that applicants provide further information and / or a copy of their ID card or that they undergo a postal or video identification process.[804] Apart from the fact that it is not possible to connect ID card information to an e-mail address, which may vary, which may be replaced in the course of time, any such proposals lead to additional problems, for example duration and safety of storage of ID documents. This way, average companies might face further challenges like the avoidance of identity theft as one simple access request might lead to a full set of personal including ID data being stored in systems which are not tailored to meet the needs of handling such sensitive data (technical security measures, authorization concept, retention periods, etc.). If the data subject by mistake contacted the wrong controller, then his request is the initial ignition for a full set of data including sensitive information like national identification numbers (which might be subject to national legislation according to GDPR Article 87) being collected and stored. If one is seriously thinking of postal or video-identification-processes for identification purposes, this means that data subjects would have to put up with a great deal of effort, only because they want to exercise their rights. In addition, video-identification-processes involve biometric data (voice, iris), and that leads to further problems as special categories of data enjoy special protection in accordance with GDPR Article 9 (1), and as a basic rule, must not be processed – unless, for example, the data subject explicitly and voluntarily consented. As a result, even more data is collected (time, date, signature) and documentation (evidence) is produced. As a matter of fact, this procedure can only represent one solution, because if the data subject does not consent, then an alternative must be provided as the proper execution of data subject rights is mandatory. In summary, the overall effort and implications of data subject requests shall not be underestimated, particularly because data subjects enjoy additional rights on top of the right to access information, for example the right to restrict processing of their personal data in defined circumstances[805] where the accuracy of the data is contested or where the processing is believed to be unlawful. Individuals may also require that their data is rectified[806] if it is inaccurate or incomplete, or that their data is deleted, the so-called right to be forgotten,[807] which now has its own article in the Regulation. The forerunner of this right was CJEU’s decision in which the court ruled that Google had to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.[808] However, the right to be forgotten as any other right has limitations, typically the

[803] This text only uses the term identification, although to identification and authentication are meant.

[804] The State Commissioner for Data Protection and Data Security in Baden-Württemberg summarized possible solutions and evaluated them their February 6, 2019 press release which is available at https://www.baden-wuerttemberg.datenschutz.de/identitaetspruefung-bei-elektronischen-auskunftsersuchen-nach-art-15-ds-gvo/. Retrieved October 24, 2021.

[805] See GDPR Article 18 which provides further details.

[806] See GDPR Article 16.

[807] In accordance with GDPR Article 17.

[808] The judgment of the court in case C-131/12 dated May 13 2014 is available at

rights of others, and that applies especially to the field of media as the right to be forgotten must not lead to censorship as freedom of expression must be respected.[809] In in everyday business life, requests for deletion may quite often fail as controllers have to obey statutory retention periods, meaning that they have legitimate grounds to continue to process/store the data. As a result, the right to be forgotten only applies in rather a narrow set of circumstances, notably where the controller has no legal ground for processing the information. The right to data portability is new and has no equivalent in the Data Protection Directive. It is based on the idea that data subjects should be able to obtain their data in a structured, commonly used and machine-readable format,[810] including the right to transmit those data to another controller without hindrance.[811] Recital 68 clarifies that the data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. This clarification is important as there was a fear that this new right would result in businesses tailoring their (CRM, HR, etc.) systems to fulfill such requests in an automated (ad hoc) manner. In fact, the Regulation clearly says that such investments are not needed. Depending on the underlying business model it is however likely that certain providers will agree upon certain standards between each other, for example email and cloud service providers and social networks. A request for data portability does not mean that data the (first) controller holds shall (also) be deleted, nor does it mean that the right only exists when a customer or client finishes the (business) relationship; data subjects are free to request data portability at any time – but only if certain conditions are met: this right can only be exercised when the (automated) processing of personal data is justified on the basis of consent, or where processing is necessary for the performance of a contract. Recital 68 makes it clear that the right to data portability is not given when the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or when the processing was carried out in public interest. Since there is hardly one dataset in real life to which the same legal grounds apply for each and every entry, in most of the cases where a data subject requests their data to be transmitted to either themselves or another recipient, the data set will have mixed legal grounds. For example, an application for a credit loan requires certain basic data such as full name and date of birth for identification purposes and (retrospective) salary information for credit rating purposes. This is the data the subject provides directly and voluntarily. Because the bank is obliged to perform a background check with regards to liquidity and the matching against sanction lists, further data are collected from other sources such as credit agencies. Then there is yet other data the bank must collect from all applicants like the tax and / or identification number. Depending on whether the credit applied for is received through a website, further data will be collected, and this is usually the moment when Big Data comes into play as user and device information are collected and evaluated. This data together

http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=667631. Retrieved October 24, 2021.

[809] See GDPR Article 17 (3).

[810] This does not mean that data subjects can insist on a specific format as the Regulation only requires that data are provided in a structured and commonly used format that is machine-readable.

[811] See GDPR Article 20 (1).

represents the dataset for the credit application, and includes various legal bases, for example data needed for the performance of a contract, data needed to fulfill a legal (compliance) obligation and data which can be used for legitimate purposes. Apart from the fact that one could already argue which pieces of information fall under the category of data needed for the performance of a contract, it is even more questionable whether consent is the right legal basis for certain (extended) background checks or if legitimate interests of the controller may apply, especially in the field of predictive analytics. As data portability only applies to those data which the data subjects provide themselves and which are based either on consent or if the processing was necessary for the performance of a contract to which the data subject is party, it seems problematic to customize the right set of information. One solution could be to downsize accordingly, another solution could be over-fulfillment in the sense of providing more information than needed. Companies may like to tend to provide more than necessary by law to avoid conflicts, however, the dataset must always be checked against collateral data and / or information which may be considered business secrets. In any event, data portability is a perfect example of how important it is to carefully select suitable legal grounds for processing as the right to portability is the “price for consent”; the right does not apply when data are processed on the basis of legitimate interests.[812] As a result, consent is not always the best and easiest solution to place data processing on a legal basis,[813] especially because any processing based on consent alone needs to be stopped immediately once consent is withdrawn,[814] and that can happen any time without providing any reasons.[815]

5.4.3.6. Setting the bar for lawful processing

From a data protection standpoint, one of the core questions is lawfulness. GDPR Article 6 provides for six lawful bases for processing, and the challenge already starts with the question whether these lawful bases may be deemed to be equivalent.[816] From a business perspective, a well-known problem is that companies as controllers fail to recognize that consent is neither the only nor the best legal grounds for the processing of personal data. Choosing the right legal grounds depends on the overall context, the underlying purposes of the processing and the existing relationship with the data subject.[817] This

[812] But the “price” is balancing of interests.

[813] Nico Härting described this phenomenon as the “consent fetishism” as many businesses fail to recognize that consent is neither the only nor always the best legal grounds for data processing. He provided thoughts on this problem during his 2012 presentation in the framework of the annual DSRI academy summit (DSRI Herbstakademie) that was held September 12-15 2012. The presentation is available at https://rsw.beck.de/cms/?toc=ZD.60&docid=338853. Retrieved October 24, 2021.

[814] See GDPR Article 7 (3): The withdrawal does not affect the lawfulness of processing before its withdrawal.

[815] The difference between GDPR Article 7 (3) and GDPR Article 21 (1) is that freely given consent can be withdrawn at any time, for any reason - unlike the need to specify or explain “grounds relating to his or her particular situation” when processing is based on legitimate interests or is performed for a task carried out in the public interest. See GDPR Article 21 (1) in conjunction with GDPR Articles 6 (1) lit. e, f.

[816] ICO Guide to the General Data Protection Regulation, p. 49. Guide published 2018, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Retrieved October 24, 2021.

[817] This can lead to advantages, e.g., in the area of direct marketing.

structure and approach was already present in the Directive, but the Regulation places more emphasis on being accountable for and transparent about the relevant lawful basis for processing. For example, if a procedure is based on the controller's legitimate interests, the prerequisite for that is that any such legitimate interests are documented internally[818] and communicated externally.[819] Given the complex matter, transparency needs in the framework of Big Data and AI applications and automated individual decision-making could be considered a higher barrier for data processing as the controller has to ensure that data subjects are furnished with all relevant information in conjunction with GDPR Articles 6, 7 and 12 to 22 in order to put them in the position to realize how such a processing may (and will) affect him.[820] If GDPR requirements in the context of lawfulness are taken seriously, it could be argued that the bar for processing of personal information changed with GDPR: despite the fact that the catalogue of data processing principles in GDPR Article 5 (1) is clear and comprehensible, what is often overlooked is that every legal basis for processing of personal data involves the evaluation of whether or not such processing is necessary.[821] Necessity must not be confused with the method chosen to operate a business in a particular way;[822] necessity is "a fundamental principle when assessing the restriction of fundamental rights, such as the right to the protection of personal data".[823] Therefore, even if the principle of data minimization is only mentioned once in the text of the Regulation explicitly,[824] Recital 39 further clarifies the principles of data processing and specifies that the processing of personal data should be limited to what is necessary for the purposes for which they are processed. The same idea is expressed in the principle of purpose limitation,[825] and both principles are crucial topics in the framework of Big Data and AI applications as these applications mostly depend on large (growing) datasets and quite often also on changing (dynamic) purposes.[826] The bar for lawful processing has several further manifestations. A simple example is that consent cannot be based on mere inactivity or

[818] See GDPR Article 6 lit f. which says that processing is only lawful if legitimate interests of a controller are not "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (…)". This means that a balancing of interests has to take place and given that controllers are accountable to demonstrate compliance with the principles relating to the processing of personal data in accordance with GDPR Article 5 (2), they have to document that they obeyed the principle of lawfulness, fairness and transparency in accordance with GDPR Article 5 (1 a).

[819] Transparency needs in accordance with GDPR Articles 13 and 14.

[820] Laurens Nauds: The right not to be subject to automated decision-making: the role of explicit consent. Article published August 2 2016, available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/. Retrieved October 24, 2021.

[821] GDPR Article 6 (1) lit. b, c, d, e and f explicitly mention that processing has to be necessary; GDPR Article 6 (1 a) – processing on the basis of the individual's consent – does not mention this term. However, GDPR Article 7 (4) stipulates that, when "assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

[822] ICO: Guide to the General Data Protection Regulation, p. 53, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Retrieved October 24, 2021.

[823] Background information on the principles of necessity and proportionality are provided by the EDPS, available at https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. Retrieved October 24, 2021.

[824] See GDPR Article 5 (1 c).

[825] See GDPR Article 5 (1 b).

[826] See GDPR Article 6 (4) sets forth the conditions of such processing.

acquiescence of the data subject because consent can only be provided by a statement or by a clear affirmative act.[827] Even though there is no requirement to provide consent in a written format, Recital 42 says that the controller must be able to demonstrate that the data subject has given consent, and that leads to a burden of proof for the controller. However, if consent is to be given in the context of a written declaration which involves other matters, the request for consent must be presented in such a way that it makes it "clearly distinguishable from all other matters, in an intelligible and easily accessible form, using clear and plain language".[828] The latter shall not be underestimated for simple reasons like the length of terms.[829] Consent must be informed and specific[830] and the GDPR forces organizations to demonstrate that the data subject's consent has been freely given,[831] and this circumstance may serve as an argument that the GDPR concretized the bar for legal processing from a documentation and burden of proof perspective. In the context of valid consent, European supervisory authorities commented on the issue of cookies:[832] the problem with the practice of using cookies is that users are often not asked for consent in an appropriate manner as some providers tend to rely on the idea that pop-up windows are sufficient in order to create transparency about the manner in which cookies are used, or that consent is mandatory in order to proceed with accessing the content and using the services of the website.[833] In March 2019, the Dutch SA published their opinion[834] on so-called cookie-walls on websites. A cookie-wall has the effect that access to the website is only granted when consent to the placing of tracking cookies[835] and similar technologies is given. The Dutch authority said that the (required) consent obtained in this way is not freely given, because individuals have no genuine and free choice as withholding consent has adverse consequences. The use of a cookie-walls results in a take-it-or-leave-it-approach, and this practice is not compliant with the GDPR. Consequently, the regulator recommend that websites shall offer a real choice for users to either accept or reject cookies, meaning that the website must remain accessible if tracking cookies are refused.[836] The guidance of the Dutch supervisory

[827] See GDPR Recital 32 explicitly mentions that inactivity cannot constitute consent.

[828] See GDPR Article 7 (2).

[829] Nate Lanxon, Jess Shankleman: The terms and conditions reckoning is coming. The authors report that PayPal's terms and conditions are almost 50,000 words spread across 21 separate web pages. Article published April 20 2018, available at https://www.bloomberg.com/news/articles/2018-04-20/uber-paypal-face-reckoning-over-opaque-terms-and-conditions. Retrieved October 24, 2021.

[830] See GDPR Article 6 (1 a).

[831] Detlev Gabel, Tim Hickman: Chapter 8: Consent – unlocking the EU General Data Protection Regulation. Article published April 5 2019, available at https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation. Retrieved July 22, 2022.

[832] The EDPB adopted Guidelines 05/2020 on consent under Regulation 2016/679. Guidelines published May 2020, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

[833] For the purposes of this example, it is assumed that consent is necessary, regardless of whether GDPR or PECR are the appropriate legal framework.

[834] The statement of the Dutch supervisory authority from March 7 2019 is available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies. Retrieved October 24, 2021.

[835] Consent is not required for placing functional cookies and non-privacy sensitive analytical cookies.

[836] Sibylle Gierschmann: Was bringt deutschen Unternehmen die DSGVO – mehr Pflichten, aber die Rechtsunsicherheit bleibt. Zeitschrift für Datenschutz 2016, p. 54.

authority is a remarkable decision after a much-disputed decision[837] Austrian case[838] in late 2018 in which a complaint about consent that was obtained through a cookie-wall was not freely given was rejected. Instead, it validated (paid) subscription models as a viable alternative to (ad) tracking. It is true that the freedom to contract principle applies to private parties, and therefore, it could be assumed that providers are not obliged to make their content available free of charge and they have the right to set certain conditions for allowing access to their website or other services. But it seems difficult to recognize free choice when the choice is reduced to personal data or money in return. Such an interpretation is open to challenge, because as a result, it reinforces business models on the basis service against data. In this context, regulators issued further guidance which is not only relevant for cookies, but also meaningful for international data transfers since they underline the inadmissibility of such transfers to the U.S.:[839] in late 2021, the Austrian regulator held that that the use of Google Analytics by a local website provider led to transfers of personal data such as identifiers, IP address and browser parameters to Google LLC in the U.S., and that this is in violation of Chapter V of the GDPR, because "the SCCs concluded between the respondents do not offer an adequate level of protection, because Google LLC qualifies as "electronic communication service provider" under 50 U.S. Code § 1881(b)(4) and is subject to surveillance by U.S. intelligence services and because any additional safeguards which have been put into place in addition to where insufficient as they could not prevent U.S. intelligence services from accessing the data subject's personal data".[840] But there are not only remarkable decisions, but there are also remarkable penalties: the French regulator CNIL issued high fines for Google and Meta, because following investigations, the CNIL found that the websites facebook.com, google.fr and youtube.com do not make refusing cookies as easy as to accept them and thus fined Meta € 60 million and Google € 150 million and ordered them to comply within three months.[841] In Germany, the former BDSG[842] took a clear position by saying that the conclusion of a contract must not be made dependent

[837] Background information on the case is provided by Christopher Jeffery: Dutch data protection guidance on the use of cookie walls. Article published May 1 2019, available at https://www.taylorwessing.com/en/global-data-hub/2019/may---adtech/dutch-data-protection-authority-guidance-on-the-use-of-cookie-walls. Retrieved October 24, 2021.

[838] Unlike in Germany, there was no explicit provision in Austria under their pre-GDPR Data Protection Act. Before GDPR came into force, § 28 (3b) BDSG stipulated that "the conclusion of a contract may not be made dependent on consent (...) if another access to equivalent contractual services is not possible or not reasonably possible without such consent." (Free translation from German).

[839] For example, the EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Recommendations published June 18 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. Retrieved October 24, 2021.

[840] Max Schrems' organizsation None Of Your Business (NOYB) represented the data subject. Background information on the case is available on NOYB's website, available at https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257_(D155.027)&fbclid=IwAR2j5-utq3BCBMr-CFl4afREQjdY5kcnqI4dEE6J-wGSHO9jGT_gWOR7qIU. Retrieved January 22, 2022.

[841] CNIL's decision to fine Google and Facebook for non-compliance with French legislation dated January 6 2022 is available at https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance#:~:text=Cookies%3A%20the%20CNIL%20fines%20GOOGLE%20a%20total%20of,refusing%20cookies%20as%20easy%20as%20to%20accept%20them. Retrieved January 22, 2022.

[842] BDSG § 28 3b.

on the data subject's consent if access to equivalent contractual services is not (reasonably) possible without such consent.[843] The law intended to stress that services must not be made dependent on consent for data which are not required for the execution of the specific service. But it is important to note that the prohibition of tying only applies if the person concerned cannot reasonably be expected / is unable to switch to another supplier – such a thought is foreign to the General Data Protection Regulation as there is no such criterion in GDPR Article 7 (4); the norm merely states that "when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". This means that any such circumstance must be taken into consideration, but it does not mean that any such circumstance would automatically lead to invalid consent. Several courts in Germany held that consent must be obtained for certain cookies,[844] and Germany introduced a new Telecommunications Telemedia Data Protection Act (TTDSG) applicable as of late 2021 which combines data protection provisions from the Telemedia Act (TMG) and the Telecommunications Act (TKG):[845] according to the new law which came with a twelve year delay, consent would not be required in certain instances, and the law also allows for consent management services so that users to indicate whether, where and under which conditions they consent or refuse to the setting of cookies. As regards freely given consent, the problem is that even within the Regulation, the relevant Article and the corresponding Recital are not congruent: Recital 43 says that "consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance." GDPR Article 7 (4) and Recital 43 may thus lead to different results.[846] Given that GDPR-Articles have priority over Recitals, some authors claim that the effectiveness of coupling has to be assessed on case-by-case.[847] Others claim that consent is always freely given when the data subject is free to choose between providers.[848] The much discussed ePrivacy Regulation may help answer the question whether making access to website content without direct monetary payment conditional to the consent of the end-user will (not?) be considered disproportionate: it seems that cookie-walls will not be prohibited as long as users are given an "equivalent offer" and that consent will be feasible through browser settings – and that users who consented to the use of cookies

[843] A very similar provision is included in § 95 (5) of the German Telecommunications Act.

[844] For example, the Frankfurt am Main County Court in a decision that was issued October 19 2021 (Az.: 3-06 O 24/21), and available at https://openjur.de/u/2378854.html.

[845] Andy Splittgerber: German cookie law enters into force on Dec. 1, 2021. Article available at https://viewpoints.reedsmith.com/post/102gyp8/german-cookie-law-enters-into-force-on-dec-1-2021. Retrieved January 22, 2022.

[846] Niko Härting: Kopplungsverbot nach der DSGVO – erste Sichtung der Literatur. itrb-Rechtsberater 2019, Sonderheft zur DSGVO, p. 5.

[847] Eike Michael Frenzel in Paal/Pauly: Kommentar zur Datenschutzgrundverordnung. C.H. Beck Publishing 2018, note 18 on GDPR Article 7.

[848] Kai-Uwe Plath: Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Publishing 2016, note 14 on GDPR Article 7.

will have to be periodically reminded of their choices.[849] The trouble with obtaining valid consent might to lead to a shift of legal basis: provided that the desired processing of personal data can be justified with legitimate interest, consent could become a phase-out model.[850] Some authors therefore believe that the economy will have to start to base processing of personal data on legitimate interests, because consent as a legal instrument appears to be weakened.[851] This argument is reinforced by the fact that Recital 43 mentions another criterion as it stresses that consent is not valid if there is a clear imbalance between the data subject and the controller. This is very important in practice; a typical example of imbalances is the relationship between employer and employee.[852] The imbalance between processor and data subject was also criticized by the German Federal Cartel Office: the Cartel Office prohibited Meta from merging user data from various sources. The Cartel Office said that the data processing conditions for the use of Meta violate data protection law as set forth by the GDPR and that they constitute an abuse of Meta's dominant position in the market for social networks for private users.[853] The result is that, as far as Germany is concerned, WhatsApp and Instagram may continue to collect data. However, in the future, data may only be assigned to a Meta user account with the user's consent. If such consent is not given, the data must remain with the other services and may not be processed in combination with Meta data. The same applies to the collection and assignment of data from third-party websites to the Meta user account, which will also only be possible in the future if the user voluntarily consents to the assignment to his or her Meta user account. While data protection practitioners may welcome this opinion as it is in favor of data subjects, the decision caused astonishment, because the German Federal Cartel Office felt competent[854] to comment on a data protection matter. The Cartel Office moreover does not seem to see a conflict between the application of antitrust law and data protection law,[855] since it attempted to establish its competence by examining data protection law within the framework of antitrust law. But this view seems contestable given that GDPR aims at a uniform

[849] Jetty Tielemanns, Müzge Fazlioglu: ePrivacy Regulation – Q&A on select topics. Article published May 25 2021, available at https://iapp.org/news/a/eprivacy-regulation-qa-on-select-topics/. Retrieved October 24, 2021.

[850] Winfried Veil: Die Datenschutzgrundverordnung: Des Kaisers neue Kleider. Neue Zeitschrift für Verwaltungsrecht 2018, p. 695.

[851] Niko Härting: Kopplungsverbot nach der DSGVO – erste Sichtung der Literatur. itrb-Rechtsberater 2019, Sonderheft zur DSGVO, p. 6.

[852] However, the individual case has to be examined as it is conceivable that employees consent to data processing, for example in the framework of an internal corporate videos, see also the Article 29 Working Party Guidelines on consent under Regulation 2016/679 (2018 version), available at https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf. Retrieved October 24, 2021.

[853] Decision of the German Federal Cartel Office published February 2 2019: Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen, and is available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html. Retrieved October 24, 2021.

[854] See GDPR Article 51 (1) and Article 55: a cartel office is not a data protection supervisory authority.

[855] Carlo Piltz: Bundeskartellamt erlasst Untersagungsverfügung gegen Facebook – Warum das Vorgehen der Behörde datenschutzrechtlich kritisch betrachtet werden muss. Article published February 7 2019, available at https://www.delegedata.de/2019/02/bundeskartellamt-erlasst-untersagungsverfuegung-gegen-facebook-warum-das-vorgehen-der-behoerde-datenschutzrechtlich-kritisch-betrachtet-werden-muss/. Retrieved October 24, 2021.

application of the Regulation, and that is why cooperation between supervisory authorities is foreseen.[856] The opinions on the relationship between (freely given) consent and other legal bases also do not show a uniform picture: despite the fact that GDPR Article 6 (1) says that processing is lawful "if and to the extent that at least one of the following applies (…)", therefore clearly saying that more than just one legal basis may be applicable for the case in question, it is disputed whether or not data processing may be based on several legal bases mentioned in GDPR Article 6. Some believe that consent may be used as a precautionary measure in the event that there is doubt which other legal bases may be applicable.[857] This interpretation seems comprehensible, since a literal interpretation of GDPR Article 6 (1) does not suggest that a particular legal basis is favored or preferred, but that all the possibilities mentioned are equivalent.[858] Consequently, some authors suggest that several legal grounds may be used as a legal basis for processing, while other authors believe that recourse on other legal grounds such as legitimate interests is not possible whenever consent was provided, especially if consent was revoked.[859] The reason for this is that, if consent is obtained, this serves as an indicator that the data subject is in full control of the data processing, and that the use of any other legal basis shall be considered contradictory and therefore inadmissible.[860] In this context, some also speak of the blocking effect which unfolds when consent is given.[861] This argument is rejected by others, because this way, consent would have a more important position than other legal provisions.[862] The situation is worsened by the fact that many businesses continue to "misuse" consent as an easy means of obtaining legal grounds, either not knowing or ignoring that, depending on the case, consent may not be needed and may therefore not be the appropriate legal basis: a typical example is that companies ask for consent even though the data processing for the service in question is covered by GDPR Article 6 (1) lit. b, the performance of a contract, which is regularly the case for many services which are rendered for customers.[863] However, if companies base (part of) their data processing operations on the performance of a contract, such legal grounds must not be overused either: the EDPB adopted guidelines on the scope and application of

[856] See GDPR Article 60.

[857] The Hessian supervisory authority issued FAQs on GDPR issues, and the SA says that (free translation from German: "It can often be difficult to determine the right legal basis for data processing or to clearly identify its limits. In such cases, it is not harmful for both responsible bodies and data subjects to obtain consent as a precautionary measure, particularly for reasons of security and transparency." The FAQs were published on the SA's website and are available at https://datenschutz.hessen.de/infothek/h%C3%A4ufig-gestellte-fragen-hgf#Einwilligung. Retrieved October 24, 2021.

[858] Benedikt Buchner, Jürgen Kühling: Kommentar zur DSGVO, C.H. Beck Publishing 2016, note 16 on GDPR Article 7.

[859] Sebastian Schulz in Gola: Kommentar zur DSGVO, C.H. Beck Publishing 2018, note 11 on GDPR Article 6.

[860] Benedikt Buchner, Thomas Petri in Kühling/Buchner: Kommentar zur DSGVO. C.H. Beck Publishing 2016, note 23 on GDPR Article 6.

[861] Maria Cristina Caldarola, Joachim Schrey: Big Data und Recht. C.H. Beck Publishing 2019, pp. 54 and 55.

[862] Niko Härting: Berechtigte Interessen nach der DSGVO. itrb-Rechtsberater, Sonderheft zur DSGVO 2019, p. 3.

[863] In this regard, it is interesting to read the examples provided by the Commission on their website: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en. Retrieved October 24, 2021.

GDPR Article 6 (1b) in the context of information society services.[864] The EDPB restricts the possibility for companies to base the processing of users' data on the legal basis fulfillment of contract. This view was welcomed, because it is argued that, if GDPR sets strict conditions for the permissibility of consent, it shall not be acceptable to bypass this requirement simply by including certain data processing operations in contracts (terms and conditions) that actually do not have much to do with the provision of their (online) services.[865] Apart from these general rules for consent, special conditions apply to vulnerable groups[866] like the consent of children,[867] and special requirements also apply if consent is given in relation to sensitive personal data.[868] On the one hand, it could be argued that GDPR's emphasis on accountability and documentation as well as principles like purpose specification indicate a strict bar for processing, but the other side of the medal is that GDPR acknowledges various privileges for certain purposes, and it also recognizes legitimate interests as a legal basis and allows for secondary use of personal information. Admissible use of personal data for secondary purposes is only feasible when certain conditions are met, but it still means that continuous data processing in principle is legally acknowledged. Since many AI applications include ADM, it is worthwhile to examine rules that apply to automated decision-making as this may indicate where to draw the line as regards legal basis in the sense of: what are scenarios in which either the law provides for limitations, or where the individual is afforded the power to prevent data processing, and based on which grounds? As regards legal conditions for ADM, it shall first be noted that under GDPR, only legal obligations, contract, and consent can justify qualifying ADM; the rest of the GDPR provisions applies to automated individual decision-making regardless of Article 22 conditions. What is more difficult to answer is the question whether automated processing may or may not include human involvement, and what qualifies as a decision with legal or similarly significant effects. To that end, a recent report[869] examined publicly available judicial and administrative decisions and regulatory guidelines across EU / EEA jurisdictions and the UK to evaluate this issue based on more than 70 cases, i.e., court rulings, enforcement decisions, individual opinions or general guidance issued by national supervisory authorities and the European Data

[864] Background information is provided in EDPB's Guidelines 2/2019 on the processing of personal data under Article 6 (1) lit. b GDPR in the context of the provision of online services to data subjects (version for public consultation) Guidelines adopted April 9 2019, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf. It is important to note that "all documents adopted during the EDPB Plenary are subject to the necessary legal, linguistic and formatting checks and will be made available on the EDPB website once these have been completed", see https://edpb.europa.eu/news/news/2019/ninth-plenary-session-guidelines-processing-personal-data-context-information-society_de. Retrieved October 24, 2021.

[865] Ulrich Kelber, German Federal Commissioner for Data Protection and Freedom of Information (BfDI), comments on the guidelines in a news entry published April 10 2019 at the BfDI's website, available at https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/15_EDSA_Art.6_1_b.html. Retrieved October 24, 2021.

[866] This is a newly introduced concept which did not exist in the Directive.

[867] See GDPR Article 8 GDPR and Recital 38.

[868] See GDPR Article 9 (2 a).

[869] The Future of Privacy Forum evaluated dozens of cases (limited to documents released until April 2022): Automated decision-making under the GDPR – practical cases from courts and data protection authorities. Report published May 2022. Retrieved July 7, 2023.

Protection Supervisor. The publication showed that ADM uses must be judged on a case by case basis, for example, "live facial recognition in schools was declared unlawful in several cases primarily because it did not have a valid lawful ground for processing in place; consent was considered to be the only ground that could justify the use of this technology to process personal data of students, and consent was not considered to be freely given in any of the cases analyzed that related to students and schools. On the contrary, relying on live facial recognition to ensure safety on a football stadium was considered lawful by a DPA even if it was not based on consent, but on substantial public interest, and provided that a set of safeguards was also ensured."[870] Owing to the fact that the body of case law grows, the criteria for assessing "solely automated decisions" and "legal or similarly significant effect" of automated decision-making on individuals are becoming increasingly sophisticated; the report showed that, in several cases, it was acknowledged that solely automated processing may include human involvement, and that courts and supervisory authorities consider the entire organizational environment, i.e., organizational structure, reporting lines or staff trainings, in order to decide whether a decision was solely automated or had meaningful human involvement.[871] While there is consensus that the processing of personal data which takes place in public interest is privileged,[872] it remains unclear whether processing may be based on commercial interests. In this context, the highest administrative court in the Netherlands published a highly anticipated judgment in July 2022 regarding assessment of legitimate interest under GDPR Article 6 (1 lit. f) to clarify whether purely commercial interests may qualify as legitimate interests within the meaning of GDPR Article 6 (1 lit. f)[873] However, the court held that, in this specific case, the controller had other legitimate interests that could be relied on which were not exclusively commercial, and therefore, there was no need to consider the question of whether purely commercial interests could be considered a valid legal basis in the sense of GDPR Art. 6 lit f. legitimate interest.

[870] Future of Privacy Forum: Automated decision-making under the GDPR – practical cases from courts and data protection authorities, p. 48. Report published May 2022. Retrieved July 7, 2023.

[871] Future of Privacy Forum: Automated decision-making under the GDPR – practical cases from courts and data protection authorities, p. 28. Report published May 2022. Retrieved July 7, 2023.

[872] See GDPR Article 6 (1) lit. e which allows for the processing of personal data when public interest is in question, even for sensitive data (GDPR Article 9 (2) lit. g, even for data transfers to third countries (GDPR Article 49 (1) lit. d.

[873] Richard van Schalk, Francesca Pole: Netherlands – highest court side-steps determining whether legitimate interests may be purely commercial. Article published 28 July 2022, available at https://blogs.dlapiper.com/privacymatters/netherlands-highest-court-side-steps-determining-whether-legitimate-interests-may-be-purely-commercial/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter. Retrieved July 30, 2022.

5.4.3.7. Contract and vendor management

Much of the literature on GDPR is concerned with new requirements including controller and processor duties, which of course makes sense as companies have to comply with (partially) new rules – especially because, under the Regulation, practically everything is sanctioned as GDPR uses the general term "infringements of the provisions" and then specifies which type of infringement leads to which (maximum) fine.[874] This was not the case under the previous regime with the Directive and national laws across the EU as penalties and sanctions were not harmonized and varied significantly in different Member States. The result was that, for example in Germany, for years, there were only sporadic sanctions according to § 44 of the pre-GDPR Federal Data Protection Act.[875] Another difference is that enforcement is likely to change as national data protection supervisory authorities will be coordinating their enforcement powers across Member States: following an EDPB statement on enforcement cooperation,[876] the Commission plans to change rules for cooperation and consistency, for example GDPR Art. 60 (3), and discussed a possible standardized rights of participation as suggested by EDPB. It is important to note that the maximum fine of up to 20 million Euros[877] may be imposed for infringements in the framework of transfers of personal data to recipients in a third country or an international organization pursuant to GDPR Articles 44 to 49.[878] Considering that data transfers outside the own organization and inside an undertaking is very common and that interconnectedness and globalization are growing, there is a definite necessity to review the existing (contractual) framework with suppliers, subsidiaries and parent companies.[879] This is particularly true when an international context is given, because different rules may apply as simple data processing agreements might not be sufficient. It is likely that nowadays, most companies are aware of the need for a (contractual) data protection framework when data transfers are in question, but it is also questionable whether they are prepared for a proper contract and vendor management including background screenings, since there are differences between the Directive and the Regulation: GDPR establishes a cumulative liability regime for controllers and processors[880] and thus foresees a joint and several liability. Controllers still carry primary responsibility for compliance, but processors have become subject to several obligations

[874] See GDPR Article 83.

[875] Christiane Schulzki-Haddouti: Datenschutz-Verstöße werden sehr selten sanktioniert. Article published April 4 2016, available at https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/. Retrieved October 24, 2021.

[876] EDPB statement on enforcement cooperation. Letter published April 28 2022, available at https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdfhttps:/edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf. Retrieved February 20, 2022.

[877] Or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: GDPR Article 83 (5).

[878] See GDPR Article 83 (5 c).

[879] For the sake of simplicity, this paragraph does not cover issues of joint controllership.

[880] Brendan van Alsenoy: Liability under EU Data Protection Law - from Directive 95/46 to the General Data Protection Regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2016, p. 282.

and are directly liable towards data subjects in case of non-compliance.[881] Second, eventual fines will also depend on factors which are influenced by the processor's behavior and prehistory: mainly the degree of responsibility of the processor;[882] any relevant previous infringements the processor committed;[883] any previous measures referred to in GDPR Article 58 (2) which have previously been ordered;[884] the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement.[885] The framework for outsourcing of services which implies the processing of personal data did not change substantially, however, businesses must take note of the fact that outsourcing standards were altered as regards format and content. The latter depends on the jurisdiction,[886] industry sector[887] or profession in question.[888] The GDPR provides that processing by a processor shall be governed by a contract or other legal act under Union or member state law, binding the processor to the controller.[889] In the framework of a parliamentary question session in August 2018,[890] the European Commission clarified that a legal act may be "an ordinance or other type of administrative decision whereby controllers vested in public authority may stipulate the conditions for processing personal data on their behalf". The Commission also addressed the question of the appropriate format of such an agreement as GDPR Article 28 (9) states that the contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including the electronic format. It said that "the rules for entering into contracts or other legal acts, including in electronic form, are not set forth in the GDPR but in other EU and / or national legislation. The e-commerce Directive[891] provides for the removal of legal obstacles to the use of electronic contracts. It does not harmonize the form electronic contracts can take. In principle, automated contract processes are lawful. It is not necessary to append an electronic signature to contracts for them to have legal effects. E-signatures are one of several means to prove their conclusion and terms". One the one hand, GDPR

[881] See GDPR Article 82 (2).
[882] See GDPR Article 83 (2 d).
[883] See GDPR Article 83 (2 e).
[884] See GDPR Article 83 (2 i).
[885] See GDPR Article 83 (2 h).
[886] The Bavarian State Commissioner for Data Protection issued guidance in which the following opinion was expressed (free translation) "Provided that the treaties complied with the previous legal requirements, the need for adaptation to the GDPR should be manageable". Der Bayerische Landesbeauftragte für den Datenschutz: Orientierungshilfe Auftragsdatenverarbeitung, p. 10. Paper published 2018, available at https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf. Retrieved October 24, 2021.
[887] For example, specific rules apply in the banking sector as risk management must apply to the outsourcing and other external procurement of IT services. Details on this issue are summarized by Ulf Morgenstern: 5. MaRisk-Novelle in Kraft getreten – deutliche Herausforderungen für Kreditinstitute. Article published December 20 2017, available at https://bankinghub.de/banking/steuerung/5-marisk-novelle-kraft-getreten. Retrieved October 24, 2021.
[888] For instance, because of professional secrecy that applies to solicitors, notaries or physicians: these professional groups have always had to take special care to ensure that data about their clients and patients are securely processed and stored.
[889] See GDPR Article 28 (3).
[890] Question reference: E-003163/2018 available at http://www.europarl.europa.eu/doceo/document/E-8-2018-003163-ASW_EN.html.
[891] The text of the Directive on electronic commerce is available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031. Retrieved October 24, 2021.

allows for more flexibility when data processing agreements are in question. On the other hand, real life will show whether businesses will make use of the above possibilities. If important contracts may be concluded in such an easy manner, this carries the risk that unauthorized staff may engage in contractual agreements. The same idea applies to amendments: if a simple email will suffice to change or amend a contractual arrangement, this may lead to undesired results. It is therefore probable that many companies will stick to the written format in favor of legal certainty. Exceptions seem likely for business models in which the controller offers an online platform for their suppliers in which they can easily access business relevant documents such as terms and conditions and conclude relevant contracts including data processing agreements. This type of process automation depends on the underlying cooperation in question and especially on whether the parties intend or desire to conclude standard contracts rather than negotiating agreements individually. Speaking of negotiating agreements individually – this is an extremely important topic when it comes to damages and liability as the Regulation provides that controllers and processors will be jointly and severally liable where they are both responsible for damage caused by their processing.[892] According to GDPR Article 82 (2) and (3), a processor "shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller". If a company acts as a processor, it shall be exempt from liability if it is able to provide proof that it is not in any way responsible for the event giving rise to the damage. In the event that one party pays all of the compensation for the damage, it is entitled to claim back relevant amounts from the other party.[893] Since GDPR significantly increases possible fines, vendors may well try to shift present liability limits to their own favor. As a result, not only is there a need to review existing data processing agreements to check whether they match all new requirements; vendor management will become a key issue in the framework of business compliance. The invalidation of the Privacy Shield and subsequent regulator recommendations on supplementary measures such as transfer impact assessments is a good example of how important the profound selection and evaluation of appropriate service providers including underlying contractual agreements is.[894] Controllers shall moreover examine their insurance policies to make sure that they have the needed coverage. The problem being that even data protection authorities will need some time to determine a reasonable and market standard approach to the appropriate allocation of risk and financial responsibility for such fines as between customers and third-party processors.[895] Another point of criticism is that the GDPR is concerned with controllers and

[892] ICO GDPR guidance – contracts and liabilities between controllers and processors. Guidance published 2018, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Retrieved October 24, 2021.

[893] See GDPR Article 82 (5).

[894] EDPB recommendations on supplementary measures adopted June 21 2021, available at https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en. Retrieved October 24, 2021.

[895] ICO GDPR guidance – contracts and liabilities between controllers and processors. Guidance published 2018, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Retrieved October 24, 2021.

processors, but does not address manufacturers. Given the potential high impact of AI on individuals, many stress that it is important to come up with very clear liability rules and to take a holistic approach that covers all relevant players, including manufacturers, meaning that certain requirements as well as remedies and damages shall apply to them as well.[896]

5.4.3.8. Emphasis on governance and response mechanisms

Information and notification requirements which occur in the framework of data breaches[897] are a perfect example of response mechanisms that are foreseen in the Regulation. The same applies to data subject requests as processes must be in place to check and fulfill individual requests for information, deletion, or data portability. Depending on the business model, this will either be resolved case-by-case or lead to the implementation of corresponding (self-service) tools.[898] The difference being that the timeline for answering data subject request is different[899] from the deadline for reporting data breaches: in the event of a personal data breach, the controller has to notify the competent supervisory authority without undue delay, where feasible, no later than 72 hours after having become aware of the data breach.[900] But it is questionable whether it will be feasible to provide all necessary information[901] on such short notice. It seems likely that, in many cases, it will not be feasible to find all necessary details on the nature and consequences of the data breach, especially when service suppliers are involved, meaning that the controller is dependent on their approach to the incident. In addition, reporting on such short notice can only focus on ad-hoc-measures, but not on long-term security (preventive) technical and organizational measures, and that is why some believe that data breach notifications under GDPR are an unrealistic default and shall be corrected.[902] Given the breach and response mechanisms, (expert) manpower will be needed, and this is underlined by a wide of range of tasks needs to be fulfilled: from the implementation of relevant (information, data subject, design, reporting) processes, various

[896] Alexander Roßnagel, Christian Geminn: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. Report published November 26 2019, available at https://www.heise.de/downloads/18/2/8/0/2/5/0/7/vzbv.pdf. Retrieved October 20, 2021.

[897] See GDPR Articles 33, 34.

[898] Michele Nati, Cert Ahlin: Data Portability 2.0 is yet to come. Article published September 17 2018, available at https://medium.com/mydata/data-portability-2-0-is-yet-to-come-1c438c2a96c1. The authors summarize the current stage of the right to data portability and report that major social platforms are offering data portability functions. Retrieved October 24, 2021.

[899] Depending on case and circumstances, the controller may take up to three months: GDPR Article 12 (3), first and second sentence: "The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests".

[900] See GDPR Article 33 (1).

[901] See GDPR Article 33 (3) specifies which details must be provided in the framework of a breach notification.

[902] On April 3 2019, the German state of Lower Saxony proposed amendments to data protection provisions to the Germany Federal Council, and one of the motions was to review the current deadline for data breach notifications as set forth in GDPR Article 33 (1) for adequacy, see: https://www.datenschutzticker.de/2019/04/niedersachesen-schlaegt-aenderung-datenschutzrechtlicher-bestimmungen-im-bundesrat-vor/. Retrieved October 24, 2021.

documentation and (risk) assessment needs over data minimization, quality, security and retention issues up to the management of breaches and third parties – all this together with the need to make sure that the lawfulness of the processing of all personal data the organization holds is given (including proof of legal grounds/origin of data/ rules for special data) can only be achieved if a corresponding governance structure is present. GDPR Article 5 (2) stipulates that the controller is responsible and "must be able to demonstrate compliance with paragraph 1", i.e., the basic principles relating to processing of personal data such as accuracy, integrity and confidentiality, lawfulness, fairness and transparency as well as purpose and storage limitation. That means that, regardless of the question of whether a Data Protection Officer must be appointed,[903] organizations must make sure that there are individuals accountable for data protection. The above requirements show that, rather to sticking to certain conditions which must be met for certain data, the Regulation requires the overall modeling of various processes and procedures based on relevant documentation for evidentiary purposes, i.e., company's privacy programs that are not based on paper compliance but live on existing processes. If, for example, a certain data processing is based on legitimate interests or if the underlying purposes for a certain data processing operation is to be changed or amended, the corresponding assessment and reasoning must be demonstrated even years later. At the same time, governance needs lead to an ongoing assessment, which is also of relevance for Big Data and AI applications, since businesses will have to review their level of compliance with GDPR requirements for every newly introduced set of data and for every newly introduced (purpose for) data processing.

5.4.4. GDPR's challenges

5.4.4.1. Heterogeneous and indeterminate terms

In the framework of data subject rights, the Regulation uses the terms fundamental rights and freedoms, but deviations in the interpretation of the Regulation could result from the fact that GDPR Articles 22 (2) b and 35 (7) c which relate to profiling and impact assessments use the term "rights and freedoms", whereas GDPR Articles 4 (24) or 6 (1) lit. f and 23 (1) which relate to legitimate interests and restrictions of obligations and rights provided for in GDPR Articles 12 to 22 and Article 34, use the term fundamental rights and freedoms. Fundamental rights and freedoms are governed by the Charter of Fundamental Rights and the European Convention on Human Rights, and the starting point for the interpretation of this term is the fundamental right to the protection of personal data pursuant to Article

[903] The requirement to appoint a DPO varies between Member States, see GDPR Article 37 (4). Depending on certain circumstances like industry and business model, organizations may have to appoint more than data protection officers, for instance, compliance officers (e.g., banking sector) or authorized recipients (e.g., in the framework of the German Network Enforcement Act). Another example is the mandatory contact person as foreseen in the e-evidence proposal.

8 of the Charter,[904] since these terms must be interpreted within the context of European law and not according to a purely national understanding[905]. The problem is that, prior to GDPR, national interpretation of data protection regulations dominated the application and transposition of data protection law into national law within the EU for decades.[906] Another challenge is that other sources of law which are part of the (global) data protection framework use a different terminology. While the Charter of Fundamental Rights and the draft of the ePrivacy-Regulation are concerned with "data protection", the European Convention on Human Rights deals with the "respect for private life", the Council of Europe Convention 108 as well as the corresponding OECD Guidelines talk about "privacy", the Data Protection Directive and the General Data Protection Regulation speak about "(fundamental) rights and freedoms" of natural persons, while the Charter of Fundamental Rights or the draft ePrivacy Regulation also deal with the protection of "communications".[907] The notion of privacy is not exactly the same like data protection, and the core issue in this context is that the applicability of data protection rules depends on these terms. As regards data subject rights, the Regulation uses the term interests[908] without providing further background information like is the case with other terms (articles). This term comprises economic, financial, and other, intangible interests,[909] but the question is how such broad concepts shall be balanced against each other as both, data subjects and controllers have economic, financial as well as tangible and intangible interests. Data subject rights such as the right to information / right of access show how important the correct interpretation of legal terms indeed is: a German case demonstrated the explosive power of right to copy[910] in the framework of the termination of an employee. The problem is that the wording of GDPR Article 15 (3) can be understood in a manner that allows for an interpretation which leads to the result that the person concerned must be provided with a copy of each e-mail, document and note he has ever written or received. The seemingly simple right to copy is a good example of how important it is to further concretize data subject rights. Another example of the challenges around terminology, definitions and / or indeterminate terms is that, while many terms

[904] This basically covers all fundamental rights which are at least indirectly protected by data protection law: Datenschutzkonferenz: Risiko für die Rechte und Freiheiten natürlicher. Working Paper no. 18, p. 1, published April 26 2018, available at https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Retrieved October 24, 2021.

[905] Datenschutzkonferenz: Risiko für die Rechte und Freiheiten natürlicher. Working Paper no. 18, p. 1, published April 26 2018, available at https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Retrieved October 24, 2021.

[906] Coherence mechanisms were usually only important for BCRs or the like; businesses typically faced the problem of multiple interpretation of the law in multiple jurisdictions, especially as there are typical overlaps with other areas of law such as labor or competition or IT-security laws.

[907] Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil II). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved October 24, 2021.

[908] For example, GDPR Articles 6 (1) lit. f and Article 9 (2) lit. b or Article 49 (1) lit. c.

[909] Datenschutzkonferenz: Risiko für die Rechte und Freiheiten natürlicher. Working Paper no. 18, p. 3 published April 26 2018, available at https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf. Retrieved October 24, 2021.

[910] Niko Härting: Mit der DSGVO zum "Golden Handshake" – von der Sprengkraft des "Rechts auf Kopie". Article published March 29 2019, available at https://www.cr-online.de/blog/author/haerting/. Retrieved October 24, 2021.

have been defined in the Regulation, there are no definitions or specific articles on highly relevant business activities such as marketing, despite the fact that advertising, (online) tracking and profiling are an important element of business operations. One exception is Recital 47 which deals with the admissibility of direct marketing in the framework of legitimate interests, but further clarification would have been helpful since Big Data and AI applications are frequently used for marketing purposes, and the situation gets more complicated if one takes a look beyond the GDPR. This is necessary because, depending on the processing scenario in question, the admissibility of the operation is not only governed by data protection law, but competition, e-commerce, and / or consumer protection laws, and the question is what is lex specialis, which rules are stricter, etc. For example, one interpretation of this specific Recital would affirm the admissibility of direct e-mail-marketing, but the perspective of national laws against unfair competition could be that consent is required: the German competition law (Gesetz gegen den unlauteren Wettbewerb, UWG) is based on Directive 2002/58, the so-called ePrivacy Directive (PECD), and some believe that it would have been more suitable to enshrine this regulation in data protection law.[911] The relationship between the PECD and the GDPR does not seem to be clear: even though Recital 173 says that "this Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons", the second sentence of the Recital shows that there is a necessity for further clarification: "In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation."

5.4.4.2. Unclear protective goals

The above discussion on relevant, consistent and future-proof legal terms is closely connected to the question of the purposes of data protection in the sense of: what exactly is to be protected? What is so valuable that no deviations are accepted? As for the latter, GDPR Article 9 (2) a makes a clear statement on the relationship of sensitive data and individuals' consent: the processing of sensitive data such as health, biometric or genetic data or personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership is not permitted unless certain exceptions which are listed in GDPR Article 9 (2) lit. a to lit. j apply. One exception is that the data subject has given explicit consent to the processing of those personal data for one or more specified purposes – but Union or member state law may provide that the prohibition may not be lifted by the data subject. This is an important aspect as it shows that individual's rights and freedoms have limitations, which can also

[911] Helmut Köhler: Die Umsetzung der Richtlinie über unlautere Geschäftspraktiken in Deutschland – eine kritische Analyse. Gewerblicher Rechtsschutz und Urheberrecht 2012, pp. 1073 and 1079.

be demonstrated in different settings: while one may claim to have certain entries deleted, this may not always work in the anticipated manner, for example, when the desired deletion could lead to censorship, or when freedom of press is concerned.[912] With regards to data subject rights, the following examples may explain what shall be protected: the right to be forgotten is about the right to make a fresh start,[913] and the right not to be subject to automated decision-making is perhaps rather about enabling due process and preventing discrimination[914] than about objecting to sophisticated data processing, and the principles of fairness and storage limitation reflect these ideas. Whenever the sense behind data protection regulation is questioned, there is a tendency to summarize data protection legislation by saying that data protection is not about the protection of data, but about the protection of the individuals behind the data. However, it is important to realize that, while GDPR wants to strengthen data subject rights by protecting "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data",[915] it also aims at ensuring the free flow of personal data: "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[916] Another important aim GDPR wanted to achieve as a reaction to the previous Directive that did not make it to harmonize data protection within the EU is questionable due to a variety of so-called opening clauses.[917] Moreover, processing is regularly possible when public interests are in question, which underlines that data processing that takes place in public interest is privileged.[918] And that is not the only relevant aspect: many courts confirmed that data protection requirements may, depending on the case,[919] also be relevant to competition law as competitors may issue warnings,[920] meaning that data protection laws may not

[912] Ivor Shapiro, Brian MacLeod: How the "Right to be Forgotten" challenges journalistic principles. Article published 18 November 18 2016, available at https://www.tandfonline.com/doi/abs/10.1080/21670811.2016.1239545?journalCode=rdij20. Retrieved October 2, 2021.

[913] Raphael Gellert: Understanding data protection as risk regulation. Journal of Internet Law 2015, pp. 3-15.

[914] In his article, the author stresses that the biggest issues stemming from automated data processing are not violations of privacy, but social sorting practices which are discriminating and infringe upon the right to due process, see Raphael Gellert: Understanding data protection as risk regulation. Journal of Internet Law 2015, pp. 3-15.

[915] See GDPR Article 1 (2).

[916] See GDPR Article 1 (3).

[917] The GDPR contains dozens of opening clauses allowing EU Member States to put national data protection laws in place to supplement the GDPR. A summary on this topic is provided by Julia Kaufmann, Michael Schmidl, Holger Lutz (editors) for Baker McKenzie in their GDPR national legislation survey. Survey published January 2018, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en. Retrieved October 2, 2021.

[918] See GDPR Article 6 (1) lit. e which allows for the processing of personal data when public interest is in question, even for sensitive data (GDPR Article 9 (2) lit. g, even for data transfers to third countries (GDPR Article 49 (1) lit. d.

[919] Some authors believe that it is likely that infringements of transparency needs may lead to the issuance of warnings, whereas other violations shall not automatically serve as a justification for competitors to initiate actions, see Marlene Schreiber: Drohen wettbewerbsrechtliche Abmahnungen wegen Verstößen gegen die DSGVO? Article published July 4 2018, available at https://www.haerting.de/neuigkeit/drohen-wettbewerbsrechtliche-abmahnungen-wegen-verstoessen-gegen-die. Retrieved October 24, 2021.

[920] Niko Härting provides an overview over the relevant case law in Germany: Sind Datenschutzverstöße abmahnfähig? Ein Rechtsprechungsüberblick. Article published July 24 2013, available at https://www.cr-

only result in claims by individuals, but claims by competitors. It is furthermore interesting to note that certain jurisdictions acknowledged that data protection laws not only protect natural persons, but also protect legal persons, which questions the notion and connection between data protection laws and fundamental rights.[921] As regards the Regulation, GDPR says that individuals' (fundamental) "rights and freedoms" shall be protected. But the scope and concrete content of this statement is unclear. The challenge is that this is an important prerequisite as none of the many interpretation issues of the GDPR can be answered in a satisfying manner as long as the protected good(s) remain unclear: the problem is that, without an identification of the protective goals and the protected goods, it is hard to find a benchmark for numerous considerations controllers have to undertake in the framework of various necessity, proportionality, compatibility and risk tests, and that is why some conclude that the GDPR is an example of the misery of data protection laws.[922] In the US, the FTC states that data protection is about consumer protection,[923] and this view is comprehensible as the example of preset (default) checkboxes demonstrates. It is a good example of inadmissible practices which are not tolerated, neither from a data or consumer protection nor from a competition law perspective, meaning that various laws go hand in hand, which is why data protection shall not be judged in isolation. A literal interpretation of the Regulation allows for the assumption that individuals' controls as part of their privacy self-management are anchored: several Recitals operate with the term "control" when talking about rights and freedoms of natural persons: Recital 7 says that natural persons shall have control over their own data, and Recital 75 deals with risks to rights and freedoms of data subjects and explains that risks may occur when data subjects are prevented from exercising control over their personal data. Recital 85 specifies that a "personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data". Altogether, these text passages reinforce the importance of exercising control in the framework of data subject rights, but the comprehensive protective purpose of the Regulation which is expressed in the detailed catalogue of examples for potential risks and harms Recital 75 presents, is viewed

online.de/blog/2013/07/24/sind-datenschutzverstose-abmahnfahig-ein-rechtsprechungsuberblick/. Retrieved October 24, 2021.

[921] Martin Schirmbacher: Österreich: Grundrecht auf Datenschutz für juristische Personen. Article published September 1 2020, available at https://haerting.de/wissen/oesterreich-grundrecht-auf-datenschutz-fuer-juristische-personen/#:~:text=F%C3%BCr%20die%20Praxis%20ist%20bedeutend%2C%20dass%20sich%20juristische,Auf%20die%20grundlegenden%20Rechte%20f%C3%BCr%20Betroffene%20k%C3%B6nnen%20. Retrieved October 24, 2021.

[922] Winfried Veil: Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved October 24, 2021.

[923] However, there are discussions about whether an additional federal authority shall be introduced in the U.S. to cover Internet privacy and data security as this could enhance consumer protection, see U.S. Government Accountability Office: Internet Privacy and Data Security – additional federal authority could enhance Consumer protection and provide flexibility. Statement published March 7 2019, available at https://www.gao.gov/products/GAO-19-427T. Retrieved October 24, 2021.

critically by some authors who say that "no life risk of this world remains unmentioned in Recital 75",[924] and they thus question where data protection ends. In this regard, other authors underline that data protection law, unlike other areas of law, does not dispose of limiting, restrictive criteria and is thus about to change the nature of the data protection regime to a fully prehensive cover.[925] Other authors raise similar concerns by saying that, owing to the fact that more and more data may be considered as personal data, literally any handling of data will be subject to data protection laws,[926] which could lead to undesired incentives for companies to abandon de-identification and therefore increase rather than alleviate privacy risks. It is undisputed that the question of whether information may be viewed as personally identifiable is a fundamental normative question, but the way in which data protection laws (and corresponding sanctions) shall be interpreted and applied very much depends on the question on what exactly is to be protected. Some authors suggest that data protection shall be interpreted as a legal framework for the regulation and risks to fundamental rights.[927] They claim that mechanisms and tools of data and risk regulation are similar as both rely on methods which involve proportionality (balancing) testing, and they also stress that data protection was a technology-specific legislation at the time of its emergence.[928] The simple reason for this is that data protection laws were a reaction to technical developments. Record keeping existed for centuries, the difference is that new technologies pose new risks.[929] This argument is underlined by the fact that, for example. the 1980 OECD Guidelines apply to "personal data, which, because of the manner in which they are processed, (…) pose a danger to privacy and individual liberties".[930]

[924] Niko Härting: Wann ist eine Datenverarbeitung eigentlich erforderlich? Article published February 1 2019, available at https://www.cr-online.de/blog/2019/02/01/wann-ist-eine-datenverarbeitung-eigentlich-erforderlich/. Retrieved October 24, 2021.

[925] In this regard, the author quotes the equivalence theory and adequacy theory which is used in other areas of law: Winfried Veil, Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/. Retrieved October 24, 2021.

[926] Omer Tene, Jules Polonetsky: Privacy in the age of Big Data – a time for big decisions. Stanford Law Review 2012, vol. 64:63, p. 66.

[927] Raphael Gellert: Understanding data protection as risk regulation. Journal of Internet Law 2015, pp. 3-15.

[928] Viktor Mayer-Schönberger: Generational development of data protection in Europe in: Philip Agre, Marc Rotenberg (eds.): technology and privacy – the new landscape. Massachusetts Institute of Technology Press 1998, pp. 224.

[929] Raphael Gellert: Understanding data protection as risk regulation. Journal of Internet Law 2015, pp. 3-15.

[930] The 1980 OECD guidelines are available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines. Retrieved October 2, 2021.

5.4.4.3. Significance of accountability

The issue of indeterminate legal terms has not only been raised in the framework of basic definitions, the interpretation of terms is also relevant for the meaning and scope of the accountability principle:[931] The term accountability itself only appears in GDPR Article 5 (2) and GDPR Article 24 (1). According to GDPR Article 5 (2), the "controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." GDPR Article 24 (1) says that the "controller shall implement appropriate (…) measures to (…) be able to demonstrate that processing is performed in accordance with this regulation". It is clear that the accountability principle leads to a catalogue of tasks businesses have to perform in order to demonstrate that they are compliant with the Regulation, for example by preparing corresponding documentation to serve as evidence.[932] The Regulation pursues a risk-based approach[933] as Recitals 75 and 76 clearly show that GDPR distinguishes between processing activities with a high and those with a low likelihood and severity of risks to the rights and freedoms of data subjects. Various articles of the General Data Protection Regulation stress this approach, for example GDPR Articles 35 and 36: data protection impact assessment, GDPR Articles 33 and 34: data breach notification, GDPR Article 25: data protection by design and by default and GDPR Article 32: security of processing.[934] As a result, low-risk processing activities face a reduced compliance burden, but it is questionable what shall be considered (minimum) standard and therefore subject to fines if there is a proven lack of compliance. In this regard, there is controversy within literature as to whether businesses may claim for themselves the principle of proportionality in the sense of a limitation of the level of requirements to what is commensurate and reasonable.[935] The scope of documentation obligations is only one question; the other issue is that relationship between the controller's obligation to provide evidence has to be balanced against the supervisory authority's duty to investigate an incident: even if a regulator has good reason to approach a controller or processor, businesses may well have the duty of cooperation, but there is no duty of self-accusation,[936] because it is up to the competent supervisory authority to examine the case meaning that it is up to the authority to ensure enlightenment.[937] The

[931] For instance, Winfried Veil: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz 2018, vol. 1, pp. 9-16.

[932] For example, records of processing activities, templates for contract or consent, impact assessments, etc.

[933] Nico Härting: Datenschutzgrundverordnung. Dr. Otto Schmidt Publishing 2016, p. 34.

[934] A summary of risk-relevant provisions can be found in: Thomas Kranig, Andreas Sachs, Markus Gierschmann: Datenschutz-Compliance nach der DSGVO – Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden. Bundesanzeiger Publishing 2017, p. 87.

[935] Winfried Veil summarizes the discussion in his 2018 article: Accountability – Wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, Zeitschrift für Datenschutz 2018, vol. 1, pp. 9-16.

[936] Thomas Petri in: Spiros Simitis: note 46 on GDPR Article 5 in: Bundesdatenschutzgesetz. Nomos Publishing Baden Baden 2014.

[937] Nico Härting: Post von der Datenschutzbehörde – Risiken des Wohlverhaltens: Was ist zu beachten, wenn eine Datenschutzbehörde Auskünfte verlangt? Article published November 8 2018, available at https://www.cr-online.de/blog/2018/11/08/post-von-der-datenschutzbehoerde-risiken-des-wohlverhaltens/. Retrieved October 24, 2021.

investigation principle is a basic principle of administrative procedural law,[938] which is accompanied by the right not to incriminate themselves. An (absurd) comparative example would be that any driver would have to demonstrate that he or she always obeyed all traffic rules.[939] Another problem is that further regulations such as the draft AI Act introduced further roles and responsibilities. This shall be welcomed as this may help establish a liability regime and capture all parties involved in the AI value chain, but this further complicates the situation, especially for complex processing operations within joint controllership scenarios, meaning that one and the same party may hold several roles.

5.4.4.4. Persistence of fragmentation

GDPR aimed at providing a single framework for data protection to provide an adequate response to the fact that Member States had a different level of implementation in times of the Directive. The result was that European data protection laws in many cases were substantially different. GDPR's goal to harmonize data protection law is actually questionable given the large number of opening clauses,[940] which leads to a number of areas in which businesses may have to cope with different national requirements in each member state, for example, employment law.[941] The same applies in the context of freedom of expression, processing of data for academic and artistic purposes,[942] or when personal information is processed for reasons of national security.[943] Other out-of-scope areas include the processing of national ID numbers[944] and personal data contained in official documents.[945] Member States may moreover create their own rules in relation to controllers or processors which are subject to obligations of professional secrecy.[946] The result is that some requirements are no longer governed by national law or have been abandoned,[947] while many other data processing scenarios continue to be governed by national law.[948] The problem is reinforced by the growing complexity of the legal

[938] Background information can be found on the German Federal Administrative Court's Website: https://www.bverwg.de/en/rechtsprechung/verwaltungsgerichtsbarkeit/grundsaetze-des-verwaltungsprozesses. Retrieved October 24, 2021.

[939] Gabriele Buchholtz, Rainer Stentzel in: Gierschmann, Schlender, Stentzel, Veil: Kommentar zur Datenschutzgrundverordnung. Bundesanzeiger Publishing 2017, note 46 on GDPR Article 5.

[940] An overview of opening clauses is provided by Julia Kaufmann, Michael Schmidl, Holger Lutz (editors) for the lawfirm Baker McKenzie. Paper published January 2018, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en.
Retrieved October 24, 2021.

[941] See GDPR Article 88.

[942] See GDPR Article 85.

[943] See GDPR Article 2 (2 d).

[944] See GDPR Article 87.

[945] See GDPR Article 86.

[946] See GDPR Articles 9 (2 I and 3), 14 (5 d), 54 (2) and 90 as well as Recitals 50, 53, 75, 85, 164.

[947] For example, the registration requirement with the local supervisory authority.

[948] This includes the processing personal data in the context of churches and religious establishments (GDPR Article 91, Recital 165). However, this provision is unlikely to be of practical significance for majority of organizations.

landscape, more and more data protection laws are applicable throughout the world,[949] and the emerging legal framework in the U.S. is also a crucial factor to consider as any data privacy statutes that apply to US-headquarters companies like Amazon, Google, Microsoft, or Meta may de facto have a global impact since these companies process a huge portion of business and personal data globally.

5.4.4.5. Shifting of the protection of fundamental rights

If the processing of personal data becomes more difficult, because valid consent is – for a variety of reasons – difficult to obtain, and the processing cannot be justified with the fulfillment of a contract as set forth in GDPR Article 6 (1) lit. b, then the only way to defend the data processing is to use legitimate interests as a legal justification. Consequently, some authors claim that GDPR Article 6 (1) lit. f, that is: legitimate interests, will play a central role in the future of data processing including Big Data and AI applications. The challenge with this development is that, if companies decide about data subject rights in the framework of balancing their fundamental rights and freedoms against their own economic interests, this leads to a shift of the data protection regime because the private sector becomes the responsible body for the individuals' data protection. Some authors are very critical about such "outsourcing of fundamental rights protection" to controllers.[950] If legitimate interests become the central aspect of processing in the framework of Big Data and AI applications, this may lead to a self-regulatory regime which many criticize as AI ethics washing[951] they compare to green washing used in marketing. If companies' project managers decide upon the design and implementation of algorithmic applications, the problem is that these staff members are not trained or qualified in data protection, and another issue to keep in mind is that they are potentially prejudiced: it may well be assumed that diverging interests between data subjects and organizations are given, and it may also be assumed that the latter could prevail. The complexity of the data protection regime as such is argument enough to envisage that employees could simply be overwhelmed by data protection issues, and employees' economic dependencies on their employer as the data controller will likely make them follow their employer's instructions.

[949] The broad territorial scope of many new data protection laws is similar to the GDPR, for example, Brazil's LGPD, see Caitlin Fennessy: Top five operational impacts of Brazil's LGPD. Part 3: international transfers. Article published November 5 2020, available at https://iapp.org/news/a/top-5-operational-impacts-of-brazils-lgpd-part-3-international-transfers/. Retrieved October 17, 2021.

[950] Martin Schallbruch: E-Evidence – Outsourcing von Grundrechtsschutz. Article published May 10 2018, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/. Retrieved October 17, 2021.

[951] Jean-Etienne Goubet: AI Ethics – beware of AI ethics washing. Article published September 24 2019, available at https://www.genesys.com/blog/post/ai-ethics-beware-of-ai-ethics-washing. Retrieved October 24, 2021.

5.4.4.6. Viability of traditional concepts

Many authors reflected on the issue of future-proof definitions[952] and the Regulation's future-viability[953] as much of its concept is based on principles which date back to an era in which technology was not as sophisticated as it is now. Even though the General Data Protection Regulation is a piece of legislation that was created in times when Big Tech and social media companies already existed, the whole setting in which personal data is being processed changed. A significant difference is that previously, data used to be a by-product of the purpose for which the data was collected while today, the exact opposite is the case as data is no longer a simple by-product. A "positive day in the life" of a modern citizen is characterized by constant data processing: ambient intelligence at home, connected cars and smart cities on their way to work, mobile devices at the workplace, customer loyalty systems in supermarkets, and Internet searches or the use of health and dating apps in the evening. A "bad day" in the life of a modern citizen may be due to CCTV surveillance and facial recognition in public spaces, mandatory use of biometric data to access systems, unpleasant online experiences such as behavioral tracking, undesired search results, or may be based algorithms deciding to raise the price for shopping cart items owing to profiling and device fingerprinting, or the fact that AI turned down an application for an interesting job or rejected a loan for a new house based on scoring. We are now dealing with players whose dominance is so strong that even antitrust authorities felt called to intervene. "Alphabet controls our search and much of our mobile experience, Apple controls the remainder of our mobile and much of our content experience, Amazon controls a large portion of our content experience and much of the Internet of Things, and Microsoft essentially sweeps up everything else."[954] There is hardly any escape: using the right browser settings may not help as many websites do not respond to such settings;[955] using alternative browsers may not help as associates illegal activities within the dark web,[956] and refraining from the use of apps may not help as collateral data is collected,[957] exercising individuals rights may not help as this is only addressed to one controller as opposed to a network of operators processing data. But processing of personal data is nowadays characterized by the interaction and networking of many actors: very often,

[952] Lokke Moerel: Big Data protection: How to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, p. 43, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164. Retrieved October 23, 2021.

[953] Winfried Veil: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018 in, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4. Retrieved October 24, 2021.

[954] Julia Black, Andrew Murray: Regulating AI and Machine Learning: setting the regulatory agenda. European Journal of Law and Technology 2019, vol. 10, issue 3, available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 24, 2021.

[955] Background information is provided in the blog post: "Do Not Track" setting on your browser means nothing. Blog post published January 15 2021, available at https://avoidthehack.com/do-not-track-setting-on-your-browser-means-nothing. Retrieved March 25, 2023.

[956] Rebecca James: When using the Tor browser becomes illegal? Article published March 24 2023, available at https://beencrypted.com/privacy/anonymous-browsing/is-tor-illegal/. Retrieved March 25, 2023.

[957] Jay Choi, Doh-Shin Jeon, Byung-Cheol Kim: Privacy and personal data collection with information externalities. Journal of Public Economics 2019, vol. 173, pp. 113-124, available at https://www.sciencedirect.com/science/article/abs/pii/S0047272719300131. Retrieved March 25, 2023.

data passes through many service providers, very often crossing many national borders. It can no longer be assumed that individual parties face each other, and that is why longstanding legal approaches may not be suitable anymore. Protections that were traditionally and primarily directed against the state and its institutions, and not against private companies, may simply not work. Data subject rights such as the right to information, the right to object, or the right to withdraw consent may not afford the needed protections. Data protection principles like purpose limitation[958] or data minimization[959] may not lead to lead to the required limitations, and best practices like fair information[960] or notice and choice[961] may not result in the necessary transparency. That is all the more true given that many processing operations can be justified by legitimate interests and compatible processing in accordance with GDPR Article 6 (1) lit. f and 6 (4). Far too often, information duties are fulfilled in a legalistic manner, consent degenerated to a mere click mechanism, and many average users have no idea what can be done with their data. These examples show that the challenges we are facing in data protection today have substantially changed, and that concepts like privacy self-management do not seem to be viable anymore. GDPR's focus on individuals' rights and risks as opposed to societal implications as well as GDPR's catalogue of duties for controllers and processors as opposed to all players involved in the AI value chain may be considered a bad thing. However, GDPR's emphasis on processes and not only data[962] together with its risk-based approach are a good thing – and something that is not embedded in other legal initiatives that operate with exhaustive high-risk AI lists.[963]

5.5. Rules at national level

5.5.1. National data protection laws

One of GDPR's main goals was to harmonize data protection rules throughout Europe. However, owing to various mandatory and optional opening clauses,[964] Member States shall and may carve out exceptions

[958] Lokke Moerel, Corien Prins: On the death of purpose limitation. Article published June 2 2015, available at https://iapp.org/news/a/on-the-death-of-purpose-limitation/. Retrieved October 24, 2021.

[959] Ira Rubinstein discusses this issue: Big Data – the end of privacy or a new beginning? International Data Privacy Law 2013, vol. 3, no. 2, p. 74.

[960] Omer Tene, Jules Polonetsky: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, p. 239, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Retrieved September 26, 2021.

[961] Daniel Solove: Introduction – Privacy self-management and the consent dilemma. Harvard Law Review 2013, vol. 126:1880, p.1903.

[962] Special conditions apply to special categories of data, but the processing in question triggers impact assessments, meaning that what happens to data is decisive.

[963] Christina Michelekaki: The GDPR and the AI Act interplay – highlights from FPF and Ada Lovelace institute's joint event. Article published November 9 2022, available at https://fpf.org/blog/the-gdpr-and-the-ai-act-interplay-highlights-from-fpf-and-ada-lovelace-institutes-joint-event/. Retrieved March 25, 2023.

[964] Lukas Feiler: Die 69 Öffnungsklauseln der DSGVO. Presentation held on behalf of the law firm of Baker & McKenzie / Diwok Hermann Petsche Rechtsanwälte LLP & Co KG in Vienna during the meeting of JusIT on June 1 2017, available at

within the Articles of the Regulation. It was therefore necessary for Member States to pass GDPR implementation laws.[965] As a result, businesses will have to comply with both, the legal framework of the GDPR and (potentially deviating) national legal frameworks of the specific countries where they operate.[966] In addition, due to GDPR's wider scope, even companies who do not have their seat within the European Union are also required to comply with GDPR. U.S. businesses face further challenges, because they must comply with the so-called Fair Information Practice Principles and various national data privacy laws. In this respect, California is a good example: just like GDPR, the California Consumer Privacy Act[967] may also apply to companies located outside California,[968] but even though both laws share some general features, their actual provisions are not the same.[969] As a result, companies that are subject to multiple jurisdictions will have to make a significant effort to achieve compliance with all relevant regulations to achieve compliance, particularly when sector-specific (e.g., banking, health, etc.) rules have to be obeyed as well. It can therefore generally be said that the problem of (undesired) fragmentation of laws remains significant. Depending on the organization in question, legal uncertainty may worsen, and legal complexity may increase.

5.5.2. U.S. privacy laws

Safe Harbor and the Privacy Shield were common examples of privacy frameworks, and even though the United States at present do not have a uniform federal data protection law comparable to the GDPR, it is certainly wrong to assume that there is no privacy legislation: prominent examples of U.S. privacy laws include (sector-specific) laws like the Health Insurance Portability and Accountability Act (HIPAA)[970] and the Children's Online Privacy Protection Act (COPPA).[971] Many states either already have or are about to introduce laws to establish data privacy (and security) requirements for the

http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf. Retrieved October 24, 2021.

[965] An overview over GDPR implementation is provided b Julia Kaufmann, Michael Schmidl, Holger Lutz (editors) for Baker McKenzie in their GDPR national legislation survey. Survey published January 2018, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en. Retrieved October 3, 2021.

[966] Jan Dhont and Lauren Cuyvers: National variations further fragment GDPR. Article published June 26 2018, available at https://www.alstonprivacy.com/gdpr-fragmentation-may-appear-more-significant-than-intended/. Retrieved October 3, 2021.

[967] The bill text is available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Retrieved October 3, 2021.

[968] Lydia de la Torre: GDPR matchup – the California Consumer Privacy Act. Article published July 31 2018, available at https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/. Retrieved October 3, 2021.

[969] Kristen Mathews and Courtney Bowman: The California Consumer Privacy Act of 2018. Article published July 13 2018, available at https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/. Retrieved October 3, 2021.

[970] The HIPAA bill text is available at https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf. Retrieved October 3, 2021.

[971] The COPPA bill text available at https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim. Retrieved October 3, 2021.

protection of (consumer) data such as financial account numbers, social security numbers as well as health records and medical or other sensitive or personal information, including: Colorado,[972] Connecticut[973] Florida,[974] Hawaii,[975] Indiana,[976] Iowa,[977] Kentucky,[978] Maryland,[979] Minnesota,[980] Mississippi,[981] Montana,[982] Nevada,[983] New Hampshire,[984] New Jersey,[985] New York.[986] Oklahoma,[987] Oregon,[988] Rhode Island,[989] Tennessee,[990] Texas,[991] Utah,[992] Vermont,[993] or Washington[994] and West Virginia.[995] Massachusetts lawmakers have introduced three competing bills, the Massachusetts Data

[972] The bill text is available at https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf. Retrieved October 22, 2021.

[973] Brian Hengesbaugh et al. explain the emerging U.S. privacy landscape: US state laws. Article published May 2 2022, available at https://www.connectontech.com/tag/us-state-laws/. Retrieved January 7, 2023.

[974] The bill text is available at https://www.flsenate.gov/Session/Bill/2022/1864. Retrieved January 19, 2023.

[975] The bill text is available at https://www.capitol.hawaii.gov/session/measure_indiv.aspx?billtype=SB&billnumber=974&year=2023. Retrieved February 28, 2023.

[976] The bill text is available at https://iga.in.gov/legislative/2023/bills/senate/5#document-b95da0f8. Retrieved January 19, 2023.

[977] The bill text is available at https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=HSB12. Retrieved February 28, 2023.

[978] The bill text is available at https://apps.legislature.ky.gov/record/23rs/sb15.html. Retrieved January 19, 2023.

[979] The bill text is available at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0698?ys=2023RS. Retrieved February 28, 2023.

[980] The bill text is available at https://www.revisor.mn.gov/bills/bill.php?b=Senate&f=SF0950&ssn=0&y=2023&keyword_type=all&keyword=privacy. Retrieved February 28, 2023.

[981] The bill text is available at http://billstatus.ls.state.ms.us/2023/pdf/history/SB/SB2080.xml. Retrieved January 19, 2023.

[982] The bill text is available at https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231. Retrieved February 28, 2023.

[983] The bill text is available at https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Text. Retrieved January 19, 2023.

[984] The bill text is available at https://www.gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1. Retrieved February 28, 2023.

[985] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/S332. Retrieved February 28, 2023.

[986] The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S00365&term=2023&Summary=Y&Actions=Y&Committee%26nbspVotes=Y&Text=Y, Retrieved January 19, 2023.

[987] The bill text is available at http://www.oklegislature.gov/BillInfo.aspx?Bill=HB1030&session=2300. Retrieved January 19, 2023.

[988] The bill text is available at https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB619. Retrieved January 19, 2023.

[989] The bill text is available at http://webserver.rilegislature.gov/BillText/BillText23/HouseText23/H5354.pdf. Retrieved February 28, 2023.

[990] The bill text is available at https://www.capitol.tn.gov/Bills/113/Bill/SB0073.pdf Retrieved January 19, 2023.

[991] The bill text is available at https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB1844. Retrieved February 28, 2023.

[992] The bill text is available at https://le.utah.gov/~2022/bills/static/SB0227.html. Retrieved January 19, 2023.

[993] The bill text is available at https://legislature.vermont.gov/bill/status/2024/H.121. Retrieved February 28, 2023.

[994] The bill text is available at https://www.consumerprivacyact.com/washington/. Retrieved October 22, 2021.

[995] The bill text is available at http://www.wvlegislature.gov/Bill_Status/Bills_history.cfm?input=3498&year=2023&sessiontype=RS&btype=bill. Retrieved February 28, 2023.

Privacy Protection Act (MDPPA),[996] the Massachusetts Information Privacy and Security Act (MIPSA)[,997] and the Internet Bill of Rights.[998] In this context, California was a pioneer: the California Consumer Privacy Act (CCPA), the California Online Privacy Protection Act (CalOPPA)[999] and the California Invasion of Privacy Act (CIPA)[1000] positioned California at the top of the list for the toughest data rules in the country. While the emergence of privacy laws in the U.S. shall be welcomed, some describe recent developments as a disparate landscape in need of consolidation,[1001] and the situation is getting more complex since U.S. legislators are also working on data specific and / or processing specific laws, for example, the following states are considering BIPA-like biometric information privacy laws: Arizona,[1002] Hawaii,[1003] Kentucky,[1004] Massachusetts,[1005] Maryland,[1006] Mississippi,[1007] Missouri,[1008] Minnesota,[1009] New York,[1010] Tennessee,[1011] and Vermont.[1012] Other states such as New Jersey,[1013]

[996] The bill text is available at https://malegislature.gov/Bills/193/HD2281. Retrieved February 28, 2023.

[997] The bill text is available at https://malegislature.gov/Bills/193/SD1971. Retrieved February 28, 2023.

[998] The bill text is available at https://malegislature.gov/Bills/193/HD3245. Retrieved February 28, 2023.

[999] The California Online Privacy Protection Act text available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC. Retrieved October 3, 2021.

[1000] James Paulick provides background information on California's "Wiretap" Act: The California Invasion of Privacy Act. Article published September 20 2022, available at https://www.leechtishman.com/insights/blog/the-california-invasion-of-privacy-act-californias-wiretap-act/. Retrieved February 28, 2023.

[1001] Jacob Nix, Pascal Bizarro: U.S. data privacy law – a disparate landscape in need of consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation. Retrieved October 3, 2021.

[1002] The bill text is available at https://apps.azleg.gov/BillStatus/BillOverview/78862. Retrieved February 28, 2023.

[1003] The bill text is available at https://www.capitol.hawaii.gov/session/measure_indiv.aspx?billtype=SB&billnumber=1085&year=2023. Retrieved February 28, 2023.

[1004] The bill text is available at https://apps.legislature.ky.gov/record/23RS/hb483.html. Retrieved February 28, 2023.

[1005] The bill text is available at https://malegislature.gov/Bills/193/HD3053. Retrieved February 28, 2023.

[1006] The bill text is available at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb0033?ys=2023RS. Retrieved January 19, 2023.

[1007] The bill text is available at https://legiscan.com/MS/bill/HB467/2023. Retrieved January 19, 2023.

[1008] The bill text is available at https://www.house.mo.gov/Bill.aspx?bill=HB1047&year=2023&code=R. Retrieved February 28, 2023.

[1009] The bill text is available at https://www.revisor.mn.gov/bills/bill.php?b=Senate&f=SF0954&ssn=0&y=2023&keyword_type=all&keyword=privacy. Retrieved February 28, 2023.

[1010] The bill text is available at https://www.nysenate.gov/legislation/bills/2023/A1362. Retrieved February 28, 2023.

[1011] The bill text is available at https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0339. Retrieved February 28, 2023.

[1012] The bill text is available at https://legislature.vermont.gov/bill/status/2024/H.121. Retrieved February 28, 2023.

[1013] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4811. Retrieved January 19, 2023.

Oregon,[1014] Vermont[1015] and Washington[1016] are working on bills that would regulate data brokers, and other states are considering laws that would regulate the use of automated employment decisions, e.g., New Jersey,[1017] New York[1018] and Vermont[1019], and the following states are working on bills that would create new or additional privacy protections for health data processed by private entities: Illinois,[1020] New York,[1021] Maryland,[1022] Massachusetts,[1023] Virginia,[1024] and Washington.[1025] New Jersey,[1026] Oregon,[1027] Texas,[1028] West Virginia.[1029] are considering legislation to regulate children's privacy, and some state legislators address algorithmic discrimination in their laws and proposals, for example, Minnesota[1030] and Washington, DC.[1031] Two further bills were signed into law in late 2022: one is the National Defense Authorization Act (NDAA)[1032] was enacted into law: the NDAA addresses AI in government with the aim to show circumstances under which AI can be used to modernize agency

[1014] The bill text is available at https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/HB2052. Retrieved January 19, 2023.

[1015] The bill text is available at https://legislature.vermont.gov/bill/status/2024/H.121. Retrieved February 28, 2023.

[1016] The bill text is available at https://app.leg.wa.gov/billsummary?BillNumber=1799&Year=2023&Initiative=false. Retrieved February 28, 2023.

[1017] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4909. Retrieved January 19, 2023.

[1018] The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A00567&term=2023&Summary=Y&Actions=Y&Text=Y. Retrieved January 19, 2023.

[1019] The bill text is available at https://legislature.vermont.gov/bill/status/2024/H.114. Retrieved February 28, 2023.

[1020] The bill text is available at https://www.ilga.gov/legislation/BillStatus.asp?DocNum=1601&GAID=17&DocTypeID=SB&SessionID=112&GA=103. Retrieved February 28, 2023.

[1021] The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S00158&term=2023&Summary=Y&Actions=Y. Retrieved January 19, 2023.

[1022] The bill text is available at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb0995?ys=2023RS. Retrieved February 28, 2023.

[1023] Massachusetts lawmakers filed two health data privacy companion bills, SD 2118, which is available at https://malegislature.gov/Bills/193/SD2118, and HD 3855, which is available athttps://malegislature.gov/Bills/193/HD3855. Retrieved February 28, 2023.

[1024] The bill text is available at https://lis.virginia.gov/cgi-bin/legp604.exe?231+ful+HB2219. Retrieved January 19, 2023.

[1025] The bill text is available at https://app.leg.wa.gov/billsummary?billnumber=1155&year=2023-. Retrieved January 19, 2023.

[1026] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4919. Retrieved January 19, 2023.

[1027] The bill text is available at https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB196. Retrieved January 19, 2023.

[1028] The bill text is available at https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB896. Retrieved January 19, 2023.

[1029] The bill text is available at https://www.wvlegislature.gov/Bill_Status/Bills_history.cfm?input=2460&year=2023&sessiontype=RS&btype=bill. Retrieved January 19, 2023.

[1030] The bill text is available at https://www.revisor.mn.gov/bills/bill.php?b=Senate&f=SF1441&ssn=0&y=2023. Retrieved February 28, 2023.

[1031] The bill text is available at https://lims.dccouncil.gov/Legislation/B25-0114. Retrieved February 28, 2023.

[1032] The bill text is available at https://www.congress.gov/117/bills/hr7776/BILLS-117hr7776enr.pdf. Retrieved January 20, 2023.

operations, leverage commercially available AI technologies, and increase productivity in predictive supply chain and logistics.[1033] The other is the Quantum Computing Cybersecurity Preparedness Act[1034] which intends to address challenges that arise out of the fact that current encryption protocols used by the federal agencies might one day be vulnerable as a result of Quantum Computing.[1035]

5.5.3. Consumer protection laws

U.S. laws show that there is a connection between privacy protection and consumer protection; the title of most privacy bills in the U.S. already indicates that the law is about protecting consumers. Examples in this context are the Gramm-Leach-Bliley Act (GLBA)[1036], the Telemarketing Sales Rule (TSR)[1037] as well as the Telephone Consumer Protection Act (TCPA)[1038] and the CAN SPAM Act[1039]. Another prominent example is the Fair Credit Reporting Act (FCRA)[1040] that applies in the context of housing, insurance, employment and credit: while, for example, traditional credit scoring is based on traditional characteristics such as historical information on how individuals meet their credit obligations, modern scoring works with non-traditional characteristics such as social media usage or shopping behavior: analysis on historical information about the individual in question is replaced by predictive analytics based on a comparison of other consumers' behaviors.[1041]

[1033] Anna Hevia, Jayne Ponder, Olivia Dworkin, Jennifer Johnson, Nicholas Xenakis, Hensey Fenton, Madeline Salinas, Jorge Ortiz: U.S. AI, IoT, CAV, and privacy legislative update – Fourth Quarter 2022. Article published January 20 2023, available at https://www.insideprivacy.com/artificial-intelligence/u-s-ai-iot-cav-and-privacy-legislative-update-fourth-quarter-2022/. Retrieved January 20, 2023.

[1034] The bill text is available at https://www.congress.gov/bill/117th-congress/house-bill/7535/text. Retrieved January 19, 2023.

[1035] Alexander Berengaut, Jayne Ponder, Jorge Ortiz: President Biden signs Quantum Computing Cybersecurity Preparedness Act. Article published January 10 2023, available at https://www.insidetechmedia.com/2023/01/10/president-biden-signs-quantum-computing-cybersecurity-preparedness-act/. Retrieved January 10, 2023.

[1036] The text of the Gramm-Leach-Bliley-Act is available at https://www.sec.gov/about/laws/glba.pdf. Retrieved October 3, 2021.

[1037] The Telemarketing Sales Rule text is available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr310_main_02.tpl. Retrieved October 3, 2021.

[1038] The text of the Telephone Consumer Protection Act text available at https://www.govinfo.gov/content/pkg/FR-2012-06-11/pdf/2012-13862.pdf. Retrieved October 3, 2021.

[1039] The text of the CAN SPAM Act is available at https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf. Retrieved October 3, 2021.

[1040] The text of the Fair Credit Reporting Act text available at https://www.ecfr.gov/cgi-bin/text-idx?SID=2b1fab8de5438fc52f2a326fc6592874&mc=true&tpl=/ecfrbrowse/Title16/16CIsubchapF.tpl. Retrieved October 3, 2021.

[1041] Federal Trade Commission: Big Data – a tool for inclusion or exclusion? Report published January 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Retrieved October 3, 2021.

5.5.4. Competition law

GDPR does not contain a specific article on marketing, but Recital 47 (7) states that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest".[1042] One may thus suggest that contacting individuals via electronic mail for commercial purposes is admissible. However, Article 13 of the ePrivacy Directive obliges Member States to prohibit unsolicited e-mail advertising.[1043] As for the relationship between the PECD and GDPR, GDPR Article 95 says that GDPR applies to all data protection issues unless special provisions with the same regulatory objective result from PECD.[1044] Therefore, the prevailing opinion in Germany is that this provision thus leads to the fact that § 7 UWG is retained with the consequence that e-mail advertising is only possible with the explicit consent of the recipient[1045] - contrary to many jurisdictions with "can-spam-acts"[1046] or "soft opt-in"-concepts.[1047] E-mail-marketing may not be a standard use case of Big Data.[1048] But the legal framework which governs the activity is a good example of how complex the situation for globally active businesses has become. Moreover, harvesting of contact details such as email-addresses from a website or proprietary online service using automated means is a method of data collection in preparation of Big Data analytics, and this is explicitly covered (forbidden) in certain jurisdictions.[1049]

[1042] Provided that a (documented) balancing of interests took place.

[1043] The German legislator has fulfilled this obligation by creating § 7 UWG (Gesetz gegen den unlauteren Wettbewerb, the German Federal law against unfair competition).

[1044] Recital 173 (Relationship to Directive 2002/58/EC) says that "This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council[1], including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation".

[1045] Detailed background information is provided by Katrin Rammo: E-Mail-Werbung künftig auch ohne Einwilligung möglich? Article published March 30 2017, available at https://www.datenschutzbeauftragter-info.de/e-mail-werbung-kuenftig-auch-ohne-einwilligung-moeglich/. Retrieved October 3, 2021.

[1046] In February 2019, the Federal Trade Commission voted to retain the U.S. "Can Spam Act": https://www.lexology.com/library/detail.aspx?g=6379a9eb-e07d-495d-8118-f804647303d5. Retrieved October 3, 2021.

[1047] While the basic rule in many countries is that businesses must not send marketing emails to individuals without specific/prior consent, a typical exception applies for own previous customers. UK's Information Commissioner's Office offers background information on the so-called "soft-opt-in" on their website, available at https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/. Retrieved October 3, 2021.

[1048] Even though email marketing activities are subject to different analyses of click rates and the like.

[1049] Email harvesting without authorization is prohibited under section 5 (b) of the 2003 U.S. Can Spam Act, see https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf. Retrieved October 3, 2021.

5.5.5. IT security laws including cyber security and Internet of Things

It is hardly feasible to provide an overview over all applicable IT-, IoT and cyber-security laws.[1050] However, data protection is not possible without data security, and it is therefore a must to include a brief overview over IT-security laws: against the background of increasing threats like cyber-attacks, industrial espionage and owing to the growing complexity of IT infrastructures, many European countries enacted IT-/cyber-security laws of their own.[1051] Given the importance of the issue, similar laws exist in most jurisdictions, including the U.S.A., where the Internet of Things Cybersecurity Improvement Act has recently been introduced.[1052] The U.S.A. also have specific data breach laws at both, federal[1053] and state level.[1054] With regards to key state data privacy and security laws, all U.S. states have breach notification laws.[1055] In addition, case law confirms and concretizes certain entrepreneurial obligations, for example, in the area of IT-outsourcing, or disaster and recovery management.[1056]

5.5.6. Equal opportunity laws

The U.S.A. are a good example of a country with a multitude of laws that prohibit discrimination based on characteristics such as age, gender, disability, race, origin or marital status: e.g., a lender must not refuse to offer (certain conditions for) loans to a single person as opposed to a married person even if

[1050] There are not only laws, but also recommendations, for instance, European Commission recommendation on cyber-security in the energy sector which builds on EU legislation in this area, including the NIS Directive and EU Cyber-Security Act. The recommendation was issued on April 3 2019, and is available at https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf. Retrieved October 3, 2021.

[1051] For example, Germany with its 2015 IT-Sicherheitsgesetz (German IT Security Act). This act amends and supplements the German federal Energy Industry Act, the Tele-Media Act, the Telecommunications Act, and other laws. Background information is provided by the German Federal Office for Security in Information Technology at their website, available at https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_IT_SiG/neur_IT_SiG_node.html. Retrieved October 3, 2021.

[1052] The bill text of the IoT Cybersecurity Improvement Act of 2020 is available at https://www.congress.gov/bill/116th-congress/house-bill/1668. Retrieved October 3, 2021.

[1053] Federal data breach notification requirements are mostly sector-specific, for instance, the Gramm-Leach-Bliley Act for the financial sector or HIPAA and further laws which govern the health sector. A summary on this topic is provided by Ali Saikali: Federal Data Breach Notification Laws. Article published May 6 2012, available at https://www.datasecuritylawjournal.com/2012/05/06/federal-data-breach-notification-laws/. Retrieved October 3, 2021.

[1054] An overview over state breach notification laws is provided by Steptoe & Johnson LLP: Comparison of U.S. State and Federal Security Breach Notification Laws, available at https://www.steptoe.com/images/content/1/7/v2/175438/Comparison-of-Security-Breach-Notification-Laws-Updated-6-1-201.pdf. Retrieved October 3, 2021.

[1055] BakerMcKenzie: Global Data Privacy & Security Handbook, last updated: 9 February 9 2020, available at https://globaltmt.bakermckenzie.com/data-privacy-security/views/jurisdiction-view?id=4b2271a7b1ef4bbd88e79183b52b3a7c&section=5cfdfd0aa92d44e6848a792f31ddcb67. Retrieved October 3, 2021.

[1056] Jens Bücking: Datenschutzgrundverordnung, NIS-Richtlinie der EU und das IT-Sicherheitsgesetz – ein neues, einheitliches Datensicherheits-/Datenschutzrecht für Europa, working paper provided by SEP Software Corp., available at https://www.sep.de/fileadmin/user_upload/Compliance/SEPsesam_Compliance_de_web.pdf. Retrieved October 3, 2021.

Big Data analytics suggest that single persons are less likely to pay back their mortgage than married individuals.[1057] Other examples of equal opportunity laws are the Age Discrimination in Employment Act,[1058] the Fair Housing Act,[1059] and the Genetic Information Nondiscrimination Act[1060] to only name a few.

5.5.7. Labor law and industrial constitution laws

Variations of the applicable legal framework may also arise in labor law,[1061] especially when company-internal rules arising from works council agreements[1062] have to be considered on top of existing employment law. This can lead to restrictions in the use of data since such agreements can stipulate that certain (performance-relevant) data must not be processed or analyzed. The employment context is generally a good example as regards admissible use of information, including applicable timings: while it may not be permissible to collect data on the fact that an applicant is pregnant, once the employment relationship is established, the same person will have to report this circumstance because the employer has a duty of care and is obliged to implement protective measures if need be (depending on the workplace). However, all such constraints are only relevant to analyses which are carried out based on employee data, a much smaller use case[1063] than in other areas.

5.6. Specific rules for algorithm-based processing, ADM, and AI

In the context of data protection laws which must be taken into consideration when it comes to algorithm-based processing, ADM, and AI, sector-specific rules (e.g., banking) as well as product (e.g., health appliance), incident (e.g., data breach), infrastructure (e.g., certain types of plants) and data-specific (e.g., information relating to children) rules apply. Moreover, data residency rules may require

[1057] Federal Trade Commission: Big Data – a tool for inclusion or exclusion? Report published January 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Retrieved October 3, 2021.

[1058] Background information on the Age Discrimination in Employment Act of 1967 is available at the U.S. Equal Employment Opportunity Commission at https://www.eeoc.gov/statutes/age-discrimination-employment-act-1967. Retrieved October 3, 2021.

[1059] The bill text of the Fair Housing Act is available at https://www.justice.gov/crt/fair-housing-act-1#:~:text=The%20Fair%20Housing%20Act%20prohibits%20discrimination%20on%20the,substantially%20limit%20one%20or%20more%20major%20life%20activities. Retrieved October 3, 2021.

[1060] A factsheet on the Genetic Information Nondiscrimination Act is available at the U.S. Equal Employment Opportunity Commission's website: https://www.eeoc.gov/laws/guidance/fact-sheet-genetic-information-nondiscrimination-act#:~:text=Title%20II%20of%20the%20Genetic%20Information%20Nondiscrimination%20Act,training%20and%20apprenticeship%20programs%2C%20and%20the%20federal%20government. Retrieved October 3, 2021.

[1061] A simple example is that the German Federal Data Protection Law enacted in the course of the introduction of GDPR (as a basic rule with exceptions) requires written consent from employees (see § 26 II 3 BDSG).

[1062] See GDPR Article 88, processing of personal data in the context of employment.

[1063] Those are in many cases due to compliance requirements, for instance, background screenings, analysis of admissible Internet usage.

that (a copy of) data is stored locally also must be considered.[1064] Other provisions may foresee that certain information (e.g., technical data, data worthy of protection for reasons of national security) must be handled in a certain manner and / or stored locally, meaning that trade compliance may also lead to challenges with regards to export controlled data being stored in the Cloud.[1065] To name all relevant provisions would go beyond the scope of this work, so that this section of the Thesis only serves to point out that, depending on the type of business activity, sector-, product and further specific rules may apply which have to be obeyed as well.[1066] This circumstance increases the legal complexity, because sector-specific regulations exist at national (federal) and at EU level, both in the EU and in the US: compliance-rules such as anti-money-laundry provisions and the like typically exist at national level; federal data breach notification requirements for the financial and health sector are a typical example sector-specific U.S. laws at federal level,[1067] whereas the Clinical Trial Regulation[1068] is an example of an industry-specific regulation at EU level. This regulation intends to harmonize the market as regards clinical trials and medicinal products and introduces rules on the protection of individuals, including informed consent and transparency requirements.[1069] It thus contains specific data protection provisions including rules on the secondary use of clinical trial data outside the clinical trial protocol for scientific purposes, which may become relevant in the context of Big Data and AI applications.[1070] The emergence of laws that specifically address algorithm-based processing and automated decision-making are probably best

[1064] Consequently, specialized data-residency-as-a-service vendors emerged as Ryan Chiavetta reports in his 2019 article: Tech vendor looks to tackle data localization compliance. The article was published July 18 2019, and is available at https://iapp.org/news/a/tech-vendor-looks-to-tackle-data-localization-compliance/. Retrieved October 3, 2021.

[1065] Background information on trade and export compliance is provided by Baker McKenzie in their 2020 article: U.S. – DDTC issues ITAR rule affecting technology transfers, encryption and cloud computing. Article published January 31 2020, available at https://www.internationaltradecomplianceupdate.com/2020/01/31/us-ddtc-issues-itar-rule-affecting-technology-transfers-encryption-and-cloud-computing/. Retrieved October 3, 2021.

[1066] Not only in the form of a law: see the "Generally Accepted Privacy Principles" which the Canadian Institute of Chartered Accountants introduced together with the American Institute of Certified Public Accountants. The 2009 version of their GAPPs is available at https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf. Retrieved October 3, 2021.

[1067] For example, HIPAA for the health sector or the Gramm-Leach-Bliley Act for the banking sector. Further details on U.S. data breach notification requirements are provided by Ali Saikali: Federal Data Breach Notification Laws. Article published May 6 2012, available at https://www.datasecuritylawjournal.com/2012/05/06/federal-data-breach-notification-laws/. Retrieved October 3, 2021.

[1068] The text of the Regulation on clinical trials on medicinal products for human use is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014R0536. Retrieved October 3, 2021.

[1069] EDPS Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), p. 3. Opinion published January 23 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf. Retrieved October 3, 2021.

[1070] EDPS opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), p. 8. Opinion published January 23 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf. Retrieved October 3, 2021.

demonstrated by the fact that specific bills have been enacted to regulate the use of automated employment decision tools, e.g., New York's city local law 144,[1071] New Jersey[1072] and New York.[1073]

5.6.1. Regulations at international and sectoral level

5.6.1.1. Vienna Convention on Road Traffic, UN Regulation on Automated Lane Keeping Systems

Even though some consider that the regulation of AI is in its infancy, there are indeed advanced regulations in certain industries, and that is especially true with regard to autonomous driving: the 1968 Vienna Convention on Road Traffic was amended in 2016[1074] in order to allow for transferring driving tasks to autonomous vehicles (AV); AV is considered one of the most remarkable use cases and one of the most critical components in the so-called Fourth Industrial Revolution,[1075] and many countries engage in testing of such vehicles,[1076] or enacted corresponding legislation.[1077] And there is further development in the area of autonomous vehicles: while for example an autopilot system is level 2, new rules on Automated Lane Keeping Systems (ALKS) that come into force in 2021 are the first international binding regulation[1078] on level 3; level 5 is fully automated with features that can drive the vehicle under all conditions.[1079] In recent years, discussions around the (applicable or appropriate)

[1071] The bill text is available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9. Retrieved January 19, 2023.

[1072] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4909. Retrieved January 19, 2023.

[1073] The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A00567&term=2023&Summary=Y&Actions=Y&Text=Y. Retrieved January 19, 2023.

[1074] The corresponding press release: UNECE paves the way for automated driving by updating UN international convention was published March 23 2016, and is available at https://www.unece.org/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/doc.html. Retrieved October 3, 2021.

[1075] World Economic Forum: Filling Legislative Gaps in Automated Vehicles. White Paper in cooperation with Sompo Holdings Inc. Paper published April 2019, available at http://www3.weforum.org/docs/WEF_Filling_Legislative_Gaps_in_Automated_Vehicles.pdf. Retrieved October 3, 2021.

[1076] Australia, Canada, China, Germany, New Zealand, the UK, and the USA have started government-level discourse around autonomous vehicles, see May Bayern: Autonomous vehicles: How seven countries are handling the regulatory landscape. Article published February 5 2020, available at https://www.techrepublic.com/article/autonomous-vehicles-how-7-countries-are-handling-the-regulatory-landscape/. Retrieved October 3, 2021.

[1077] For example, Canada: Sairam Sanathkumar: Artificial Intelligence, autonomous vehicles, and Canadian law. Article published December 16 2022, available at https://www.lexpert.ca/legal-insights/artificial-intelligence-autonomous-vehicles-and-canadian-law/372144. Retrieved January 10, 2023.

[1078] UNECE: UN Regulation on Automated Lane Keeping Systems is milestone for safe introduction of automated vehicles in traffic. Press release published June 24, 2020, available at https://www.unece.org/?id=54669. Retrieved October 3, 2021.

[1079] UNECE: Framework Document for Automated/Autonomous Vehicles. Last updated February 2022, available at https://unece.org/transport/publications/framework-document-automatedautonomous-vehicles-updated. Retrieved January 10, 2023.

regulation of "in-car technology”[1080] and “connected cars”[1081] intensified, be it to allow for automated emergency calls,[1082] to prevent drinking and driving,[1083] or to examine (fatal) crashes in connection with autonomous driving.[1084]

5.6.1.2. Convention on Certain Conventional Weapons[1085] and Lethal Autonomous Weapons Systems

Regulations are also in place with regards to the use of lethal autonomous weapons systems (LAWS).[1086] Many countries enacted laws on autonomous weapons,[1087] and many call for a regular and systematic review in this area to ensure that humans remain in control of such technologies and prevent the creation and use of harmful applications:[1088] in fact in late 2022, for the first time at the United Nations General Assembly, more than 70 countries acknowledged the need for internationally agreed rules and limits on

[1080] Konstantin Demishev: Internet of Things technology for connected cars: the future of automobiles is here. Article published August 6 2020, available at https://www.topdevelopers.co/blog/iot-technology-for-connected-cars-the-future-of-automobiles/. Retrieved July 25 2022.

[1081] Jay Modrall: For connected cars, an evolving EU regulatory landscape – the EU's regulatory landscape for connected cars is evolving, with new functionalities appearing almost daily. Article published April 26 2022, available at https://europe.autonews.com/guest-columnist/connected-cars-evolving-eu-regulatory-landscape. Retrieved July 25 2022.

[1082] Background information on the eCall-System is provided on “Your Europe”, an official website of the European Union: eCall 112-based emergency assistance from your vehicle. Last updated June 5 2022, available at https://europa.eu/youreurope/citizens/travel/security-and-emergencies/emergency-assistance-vehicles-ecall/index_en.htm#abbr-tooltip. Retrieved July 25 2022.

[1083] Autoblog: Congress mandates in-car technology to stop drunk driving, but which tech will most likely be adopted? Blog post published November 10 2021, available at https://www.autoblog.com/2021/11/10/drunk-driving-car-technology-infrastructure-bill/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAANai10U7RrVIKUYgOlns_UzNo5OyatfXZRz9BqHCVuV7oyvYvJeWQRJ7oIAn3bjaJaf2sVpzwabo0H96_k8Mm1ZlHXBOCMLdIgj7CO5zq4PMJMLxz1YK1ab0k1sQEdXA4KQYq_wRcvNOe0BUNvNOR0tGj84BR5uqr7IQ-pf35vao**.** Retrieved July 25 2022.

[1084] Andrew Hawkins: Two new fatal Tesla crashes are being examined by US investigators. Article published July 7 2022, available at https://www.theverge.com/2022/7/7/23198997/tesla-fatal-crashes-california-florida-autopilot-nhtsa. Retrieved July 25 2022.

[1085] The text of the Convention on Certain Conventional Weapons is available at https://www.un.org/disarmament/publications/more/ccwon. Retrieved October 3, 2021.

[1086] Background information on the topic is provided by Kenneth Anderson and Matthew Waxman: Law and ethics for Autonomous Weapon Systems: Why a ban won’t work and how the laws of war can. American University Washington College of Law Research Paper no. 2013-11, available at http://ssrn.com/abstract=2250126. Retrieved October 3, 2021.

[1087] For example, China, South Korea, Israel, Russia, and the UK either use or develop LAWS with decreasing levels of human control. Background information is provided by the Campaign to Stop Killer Robots, Retaining human control of weapons systems. Briefing Note for the Convention on Conventional Weapons Group of Governmental Experts Meeting on Lethal Autonomous Weapons Systems published April 9-13, 2018, available at https://www.stopkillerrobots.org/wp-content/uploads/2018/03/KRC_Briefing_CCWApr2018.pdf. Retrieved October 3, 2021.

[1088] Statement by the EU Group of Governmental Experts Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons published August 27 2018, available at https://eeas.europa.eu/headquarters/headquarters-homepage/49763/convention-certain-conventional-weapons-group-governmental-experts-lethal-autonomous-weapons_en. Retrieved October 3, 2021.

autonomous weapons systems and united in delivering a first-of-its-kind joint statement on the issue.[1089] Human Rights Watch and the Harvard Law School International Human Rights Clinic issued a report[1090] on the matter and have proposed a treaty-making process to safeguard humanity from autonomous weapons systems.

5.6.1.3. MiFID II[1091]

The banking sector is a highly regulated sector[1092] and yet another example of an industry that already has rules for algorithms that are being used for high frequency algorithmic trading,[1093] and this shows that AI regulation is perhaps not any more in its infancy.

5.6.2. Rules at national and state level AI, ADM, and further algorithmic-specific rules

Apart from the fact that the United States seem to be moving towards a comprehensive federal privacy and data protection legislation for some time already[1094] – the Congress also released a draft federal privacy law titled the "American Data Privacy and Protection Act" in June 2022[1095] – the U.S. engaged in numerous legal initiatives in the area of Artificial Intelligence as the following examples show: the

[1089] Mary Wareham: Statement on lethal autonomous weapons systems to the CCW Annual Meeting. Article published November 16 2022, available at https://www.hrw.org/news/2022/11/16/statement-lethal-autonomous-weapons-systems-ccw-annual-meeting-0. Retrieved December 29, 2022.

[1090] The report is entitled Agenda for action – alternative processes for negotiating a killer robots treaty. Report published November 10 2022, available at https://www.hrw.org/report/2022/11/10/agenda-action/alternative-processes-negotiating-killer-robots-treaty. Retrieved December 29, 2022.

[1091] The text of Directive 2014/65/EU is available at https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en.

[1092] The European Commission published its draft Digital Operational Resilience Act (DORA) to streamline the third-party risk management process across financial institutions, see Edward Cost: What is the Digital Operational Resilience Act. Article published June 7 2022, available at https://www.upguard.com/blog/what-is-the-digital-operational-resilience-act. Retrieved July 18, 2022. The text of the proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0595&rid=10. Retrieved July 18, 2022.

[1093] Danny Busch: MiFID II - Regulating high frequency trading, other forms of algorithmic trading and direct electronic market access. Law and Financial Markets Review 2016/2, available at https://ssrn.com/abstract=3068104 or http://dx.doi.org/10.2139/ssrn.3068104. Retrieved October 3, 2021.

[1094] Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published on November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/. Retrieved October 3, 2021.

[1095] Jason Gavejian, Joseph Lazzarotti, Cecilie Read: Congress releases draft federal privacy law with potential traction to pass. Article published June 21, 2022 in the The National Law Review, available at https://www.natlawreview.com/article/congress-releases-draft-federal-privacy-law-potential-traction-to-pass#:~:text=The%20federal%20government%20has%20been%20trying%20to%20reach,released%20by%20the%20Committee%20on%20Energy%20and%20Commerce. Retrieved July 8, 2022.

Advancing American AI Act,[1096] the Future of AI Act,[1097] the National Artificial Intelligence Initiative Act,[1098] the Artificial Intelligence Act[1099], the Algorithmic Accountability Act,[1100] the AI in Government Act,[1101] the Artificial Intelligence Reporting Act,[1102] the Advancing AI Research Act,[1103] the Growing Artificial Intelligence Through Research Act,[1104] the Mind Your Own Business Act,[1105] or the Protecting Americans from Dangerous Algorithms Act.[1106] The country moreover plans for the establishment of a National Security Commission on Artificial Intelligence[1107] and is also very active in the area of Automated Decision Making: many states already have ADM legislation, for example California, Virginia and Colorado, and many others are discussing similar initiatives.[1108] What these laws have in common is that they "borrow some terms and ideas from the EU's General Data Protection Regulation,"[1109] for example, by foreseeing that internal duties include risk assessments and that external duties include meaningful information of individuals. The interesting development in this context is that, for example, the Colorado Privacy Act[1110] says that Data Protection Assessment for high-risk profiling will be required to be made available to the Attorney General upon request. However, unlike the GDPR,

[1096] The bill text of the Advancing American AI Act is available at https://www.congress.gov/bill/117th-congress/senate-bill/1353/text?q=%7B%22search%22%3A%5B%22data+OR+privacy%22%5D%7D&r=27&s=5. Retrieved October 3, 2021.

[1097] The bill text of the Future of AI Act is available at https://www.congress.gov/bill/115th-congress/house-bill/4625. Retrieved October 3, 2021.

[1098] The bill text of the National Artificial Intelligence Initiative Act is available at https://www.congress.gov/bill/116th-congress/house-bill/6216. Retrieved October 3, 2021.

[1099] Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article published on May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/. Retrieved October 3, 2021.

[1100] The bill text of the Algorithmic Accountability Act is available at https://www.congress.gov/bill/116th-congress/senate-bill/1108. Retrieved October 3, 2021.

[1101] The bill text of the AI in Government Act is available at https://www.congress.gov/bill/115th-congress/senate-bill/3502. Retrieved October 3, 2021.

[1102] The bill text of the Artificial Intelligence Reporting Act is available at https://www.congress.gov/bill/115th-congress/house-bill/6090/. Retrieved October 3, 2021.

[1103] The bill text of the Advancing AI Research Act is available at https://www.congress.gov/bill/116th-congress/senate-bill/3891. Retrieved October 3, 2021.

[1104] The bill text of the Growing Artificial Intelligence Through Research Act is available at https://www.congress.gov/bill/116th-congress/house-bill/2202. Retrieved October 3, 2021.

[1105] The bill text of the Mind Your Own Business Act is available at https://www.congress.gov/bill/117th-congress/senate-bill/1444/text?q=%7B%22search%22%3A%5B%22automated+decision-making%22%5D%7D&r=3&s=3. Retrieved October 3, 2021.

[1106] The bill text of the Protecting Americans from Dangerous Algorithms Act is available at https://www.congress.gov/bill/117th-congress/house-bill/2154?q=%7B%22search%22%3A%5B%22algorithmic%22%5D%7D&s=1&r=2. Retrieved October 3, 2021.

[1107] Background information on the National Security Commission on Artificial Intelligence is available at https://www.congress.gov/bill/115th-congress/house-bill/5356/. Retrieved October 3, 2021.

[1108] Pollyanna Sanderson: Automated decision systems legislation update. Presentation held on June 14 2021 during a Future of Privacy Forum meeting.

[1109] Angelique Carson: Colorado Privacy Act (CPA): What is it? Article published June 11 2021, available at https://www.osano.com/articles/colorado-privacy-act-what-is-it.

[1110] The bill text of the Colorado Privac Act is available at https://leg.colorado.gov/bills/sb21-190. Retrieved October 3, 2021.

many of these laws are concerned with consumers[1111] and not addressed towards individuals, which leads to the question if privacy protections do not apply to individuals which do not qualify as consumers. Obviously, such a variety of definitions and such a high degree of fragmentation will lead to challenges at implementation level. But unlike the EU which only has guidance at regulator level,[1112] the U.S. have explicit rules on so-called dark patterns,[1113] i.e., methods to misinform or inappropriately influence users' behavior and manipulate consumer actions, ranging from annoying-but-innocent to unlawful design of websites and applications: this violates existing laws such as Section 5 of the FTC Act, and data privacy laws like the California Privacy Rights Act which explicitly regulates dark patterns.[1114] In June 2022, Canada introduced the Digital Charter Implementation Act[1115]. If passed, this package of laws will reform the Canadian privacy law including a tribunal specific to privacy and data protection – and implement Canada's first AI legislation, the Artificial Intelligence and Data Act (AIDA): AIDA aims at protecting individuals from the harms and biased outputs AI systems are capable of generating and establishes requirements for the design, development, use, and provision of AI systems; it furthermore mandates impact assessments, and foresees administrative monetary penalties, or even criminal offences for certain conduct in relation to AI systems.[1116]

5.7. Purpose and data-(processing) specific rules

5.7.1. Biometric data and facial recognition

Apart from the above-mentioned rules for the finance industry as well as autonomous weapons and vehicles, there are further areas of AI for which specific rules already exist. In this regard, facial recognition technology is a good example: in the US, Illinois passed the Biometric Information Privacy

[1111] For example, Virginia's CDPA or the New Jersey Disclosure and Accountability Transparency Act, see Pollyanna Sanderson: Automated decision systems legislation update.

[1112] EDPB Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognize and avoid them. Guidelines published March 14 2022, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. Retrieved July 25, 2022.

[1113] Harry Brignull coined the term already in the year 2010, see https://www.darkpatterns.org/about-us, a website that has been established with the aim to raise public awareness of deceptive digital practices. It changed its name to https://www.deceptive.design/. Retrieved February 5, 2023.

[1114] Background information on the CPRA is provided by Jennifer King and Adriana Stephan: Regulating privacy dark patterns in practice – drawing inspiration from California Privacy Rights Act. Georgetown Law Technology Review 2021, vol. 5 pp. 251-276, available at https://georgetownlawtechreview.org/regulating-privacy-dark-patterns-in-practice-drawing-inspiration-from-california-privacy-rights-act/GLTR-09-2021/. Retrieved October 24, 2021.

[1115] Background information on the Digital Charter Implementation Act is provided by the Canadian government at their website, available at https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020. Retrieved January 8, 2023.

[1116] Maya Medeiros, Jesse Beatson: Canada's Artificial Intelligence legislation is here. Article published June 28 2022, available at https://www.dataprotectionreport.com/2022/06/canadas-artificial-intelligence-legislation-is-here/. Retrieved July 8, 2022.

Act (BIPA) already in 2008,[1117] and Maryland[1118] and Mississippi[1119] are considering BIPA-like biometric information privacy laws. Several states (for example California, Texas) and numerous cities (for example San Francisco, Seattle or Oakland) either already have or are planning to ban the use of the facial recognition;[1120] ditto for further cities around the globe that are taking joint efforts to defend digital rights at municipal level.[1121] The opposite is true for China: millions of cameras are used for facial (and voice) recognition that can identify people and monitor their behavior for identification[1122] or surveillance purposes.[1123] Some claim that the rollout of biometric identification systems is likely to exacerbate ethnic profiling.[1124] The fact that Clearview, a tool that allows to identify individuals based on a single photo, has been used by police[1125] shows that the wish to use such technology is present in many countries: in the framework of its border management, the European Union decided – without great public impact – to introduce a biometrics database which includes fingerprints and facial scans, the "Common Identity Repository."[1126] The database was designed to allow for better tracking of immigration and criminals and will be one of the largest information systems for retrieving biometric data worldwide, putting Europe "right behind the Chinese government and India's Aadhar system in terms of the size of people-tracking databases". There is fear that the system may be expanded to track people that are not the subject of criminal investigations, for example tourists, and this way, millions of

[1117] Michael Lore: The Illinois Biometric Information Privacy Act. Article published January 31 2020, available at https://www.overtime-flsa.com/illinois-biometric-information-privacy-act-bipa/. Retrieved October 3, 2021.

[1118] The bill text is available at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb0033?ys=2023RS. Retrieved January 19, 2023.

[1119] The bill text is available at https://legiscan.com/MS/bill/HB467/2023. Retrieved January 19, 2023.

[1120] AI Now's 2019 report which is available at https://ainowinstitute.org/AI_Now_2019_Report.pdf. Retrieved October 3, 2021.

[1121] The "Cities Coalition for Digital Rights" is a network of cities helping each other in the greenfield of digital rights based policy-making and was launched by the cities of Amsterdam, Barcelona and New York in 2018 and now has more than 50 cities worldwide, see https://citiesfordigitalrights.org/about. Retrieved October 3, 2021.

[1122] Researchers found a database used to track a certain ethnic group, because the corresponding database was accessible on the Internet for months, see Catalin Cimpanu: Chinese company leaves Muslim-tracking facial recognition database exposed online. Researcher finds one of the databases used to track Uyghur Muslim population in Xinjiang. Article published February 14 2019, available at https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/. Retrieved October 3, 2021.

[1123] Bill Gertz: Social credit score: China set to roll out "Orwellian" mass surveillance tool. Article published December 9 2019, available at https://www.washingtontimes.com/news/2019/dec/9/social-credit-system-china-mass-surveillance-tool-/. Retrieved October 3, 2021.

[1124] Statewatch covers this issue in their 2022 report: Building the biometric state – police powers and discrimination. Report published February 28 2022, available at https://www.statewatch.org/news/2022/february/eu-ongoing-rollout-of-biometric-identification-systems-likely-to-exacerbate-ethnic-profiling/. Retrieved December 28, 2022.

[1125] Ariel Bogle: Australian Federal Police officers trialed controversial facial recognition tool Clearview AI. Article published on April 15 2020, available at https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894. Retrieved October 3, 2021.

[1126] Background information on the common identity repository is provided by the European Council: Interoperability between EU information systems – Council adopts regulations. Press release published May 14 2019, available at https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/. Retrieved October 3, 2021.

EU citizens might be affected, and not only criminals.[1127] Some therefore consider this to be a harmful step and comment on the initiative as “a Big Brother centralized EU database including all existing and future Justice and Home affairs databases.” [1128] Against this background, the campaign “Reclaim Your Face” calls for a ban on mass surveillance with the help of biometric information, demanding that authorities take note of serious risks implied with the use of facial recognition and other biometric technologies in public spaces[1129] - and not only in public spaces: today’s technology shows that the use of static information that would have previously been considered non-sensitive data should be reconsidered, because it became fairly easy to, for example, manipulate pictures by “morphing faces to influence voters”[1130], or by producing a Deep Fake to embarrass or expose someone[1131] or by identifying the individuals behind those photos[1132] – or by erasing them from a group picture.[1133] Recent developments in Iran underlined how important facial recognition may indeed be: the country uses face recognition to identify women breaking Hijab laws.[1134]

5.7.2. Genetic information and health data privacy bills

Florida enacted a new genetic privacy law in October 2021 which establishes four new crimes related to the unlawful use of another person’s DNA, the Protecting DNA Privacy Act.[1135] Florida is only one of many examples within the U.S.A. of a state that demonstrates an increased focus on genetic privacy protections: California, Arizona and Utah have also started developing genetic privacy laws to govern

[1127] Tony Bunyan for Statewatch: The “point of no return” - Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases. Article published June 2018, available at https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf. Retrieved October 3, 2021.

[1128] Tony Bunyan for Statewatch: The “point of no return” - Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases. Article published June 2018, available at https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf. Retrieved October 3, 2021.

[1129] Background information on the campaign is provided at https://reclaimyourface.eu/. Retrieved October 3, 2021.

[1130] Adam Gorlick: Researchers say voters swayed by candidates who share their looks. Stanford University report published October 22 2008, available at https://news.stanford.edu/news/2008/october22/morph-102208.html. Retrieved October 3, 2021.

[1131] Rachel Metz: Researchers can now use AI and a photo to make fake videos of anyone. Article published May 24 2019, available at https://edition.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html. Retrieved October 3, 2021.

[1132] Will Knight: Clearview AI has new tools to identify you in photos. Article published April 10 2021, available at https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/. Retrieved October 3, 2021.

[1133] Kim Lyons: Google Pixel 6 leak teases magic eraser feature, plus five years of Android security updates. Article published October 9 2021, available at https://www.theverge.com/2021/10/9/22718007/google-pixel-6-leak-teases-magic-eraser-camera-five-years-android-security-updates. Retrieved October 3, 2021.

[1134] Khari Johnson: Iran says face recognition will ID women breaking hijab laws. Article published January 10 2023, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment. Retrieved January 20, 2023.

[1135] The bill text is available at https://flsenate.gov/Session/Bill/2021/833. Retrieved October 3, 2021.

privacy practices, for example of direct-to-consumer genetic testing.[1136] Apart from laws on biometric and genetic data or facial recognition, and on top of the well-established Health Insurance Portability and Accountability Act, numerous states started working on laws that would create new or additional privacy protections for health data which are processed by private entities, for example, New York,[1137] Virginia,[1138] and Washington.[1139] This is positive on the one hand, on the other hand, it adds to the fragmentation and lack of consistency since these laws do not apply to the public sector. The development in health data privacy shall be closely monitored given the importance for AI in the health sector, especially in diagnostics.[1140]

5.7.3. Children's privacy bills

In the U.S., the 1998 Children's Online Privacy Protection Act[1141] is not the only legislation that regulates children's privacy. It imposes certain requirements on website operators and online services directed to children under 13 years of age,[1142] which is important because this is exactly the right target group for today's digital world. By now, several U.S. states are considering enacting bills that deal with the protection of minors, for example, New Jersey,[1143] Oregon,[1144] Texas,[1145] West Virginia[1146]. Moreover, there are important age-appropriate design initiatives at EU and national level: the European

[1136] Libbie Canter, Rebecca Yergin: Newly effective Florida law imposing criminal sanctions adds to developing nationwide patchwork of state genetic privacy laws. Article published October 6 2021, available at https://www.insideprivacy.com/health-privacy/newly-effective-florida-law-imposing-criminal-sanctions-adds-to-developing-nationwide-patchwork-of-state-genetic-privacy-laws/. Retrieved October 3, 2021.

[1137] The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S00158&term=2023&Summary=Y&Actions=Y. Retrieved January 20, 2023.

[1138] The bill text is available at https://lis.virginia.gov/cgi-bin/legp604.exe?231+ful+HB2219. Retrieved January 20, 2023.

[1139] The bill text is available at https://app.leg.wa.gov/billsummary?billnumber=1155&year=2023-. Retrieved January 20, 2023.

[1140] Kumar Chebrolu, Dan Ressler, Hemnabh Varia: Smart use of artificial intelligence in health care. Seizing opportunities in patient care and business activities. Article published October 22 2020, available at https://www2.deloitte.com/us/en/insights/industry/health-care/artificial-intelligence-in-health-care.html. Retrieved January 20, 2023.

[1141] The bill text is available at https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. Retrieved January 20, 2023.

[1142] Background information on COPPA is provided by the FTC on their website, available at https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. Retrieved January 20, 2023.

[1143] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4919. Retrieved January 19, 2023.

[1144] The bill text is available at https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB196. Retrieved January 20, 2023.

[1145] The bill text is available at https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB896. Retrieved January 20, 2023.

[1146] The bill text is available at https://www.wvlegislature.gov/Bill_Status/Bills_history.cfm?input=2460&year=2023&sessiontype=RS&btype=bill. Retrieved January 20, 2023.

Commission will facilitate a comprehensive EU Code of conduct on age-appropriate design [1147] which builds on the regulatory framework provided in the GDPR and other laws, and in the UK, ICO[1148] issued an age-appropriate design code for apps, connected toys and devices and news services.

5.7.4. Data broker bills

From a business perspective, it is furthermore worthwhile to have a look at bills that address data brokers since these companies may be valuable for Big Data and AI applications because data brokers may offer services such as enriching datasets; from an individual's perspective, the monetization of such data is not just annoying, it may pose a real threat to their lives, for example when location data about individuals visiting abortion clinics is made available.[1149] It should also not be forgotten that data brokers by definition[1150] are companies that sell data on individuals with whom they have no direct business relationship – which is the opposite of data subjects controlling what happens to their personal data. Therefore, legal initiatives in the context of data broker activities shall be highly welcomed. At present, California addresses data brokers in the CCPA,[1151] and Delaware[1152] and Vermont[1153] are working on bills that would regulate data brokers, and the same applies to New Jersey[1154] and Oregon.[1155]

[1147] Background information on the EU Code of conduct on age-appropriate design is provided by the European Commission on their website, available at https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design. Retrieved January 20, 2023.

[1148] Details on ICO's age appropriate design code are provided by the ICO, available at https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/. Retrieved January 20, 2023.

[1149] Joseph Cox: Data broker is selling location data of people who visit abortion clinics. Article published May 3 2022, available at https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood. Retrieved January 20, 2023.

[1150] Background information on the emergence of data broker bills is provided by Justin Sherman: Examining state bills on data brokers. Article published May 31 2022, available at https://www.lawfareblog.com/examining-state-bills-data-brokers. Retrieved January 20, 2023

[1151] Details on data broker bills in California is provided by Lothar Determann: California data broker registrations: who made the list on Jan. 31? Article published February 11 2020, available at https://iapp.org/news/a/california-data-broker-registrations-who-made-the-list-on-jan-31/. Retrieved January 20, 2023

[1152] The bill text is available at https://legis.delaware.gov/BillDetail/79022. Retrieved January 20, 2023.

[1153] The bill text is available at https://legislature.vermont.gov/statutes/section/09/062/02430**.** Retrieved January 20, 2023.

[1154] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4811. Retrieved January 20, 2023.

[1155] The bill text is available at https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/HB2052. Retrieved January 20, 2023.

5.7.5. Automated employment decision tools bills

Like is already the case with New York's city local law 144,[1156] further states, i.e., New Jersey[1157] and New York[1158] are currently considering laws that would regulate the use of automated employment decisions. This is in fact highly relevant because it reflects applicants' reality as almost 70 percent of all recruiters use some sort of automated decision making in the application process,[1159] but the problem is that ADM tools that are used in the application process and / or in the employment context may lead to discrimination and bias[1160] like the example of Amazon[1161] showed.

5.8. Private sector initiatives

Telecommunication companies like Telefónica,[1162] Vodafone[1163] or German Telekom[1164] were amongst the first ones to think about company-own standards and rules with regards to the use of AI. Other

[1156] The bill text is available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9. Retrieved January 20, 2023.

[1157] The bill text is available at https://www.njleg.state.nj.us/bill-search/2022/A4909. Retrieved January 20, 2023.

[1158] The bill text is available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A00567&term=2023&Summary=Y&Actions=Y&Text=Y. Retrieved January 20, 2023.

[1159] LinkedIn 2018 report on global trends in recruiting. Report published January 2018, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment. Retrieved January 20, 2023.

[1160] Caragh Aylett-Bullock: Automating insecurity – decision making in recruitment. Article published March 13 2022, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment. Retrieved January 20, 2023.

[1161] Jeffrey Dastin: Amazon scraps secret AI recruiting tool that showed bias against women. Article published October 11 2018, available at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. Retrieved January 20, 2023.

[1162] Details on Telefónica's engagement are available at https://www.telefonica.com/en/web/responsible-business/our-commitments/ai-principles. Retrieved October 3, 2021.

[1163] Vodafone Group's Artificial Intelligence Framework is available at https://www.vodafone.com/about-vodafone/how-we-operate/public-policy/policy-positions/artificial-intelligence-framework. Retrieved October 3, 2021.

[1164] Background information on German Telekom's AI initiative is available at https://www.telekom.com/en/company/digital-responsibility/digital-ethics-deutsche-telekoms-ai-guideline. Retrieved October 3, 2021.

companies like SAP,[1165] Sony[1166] or big tech companies like IBM[1167] or China's tech giant Tencent[1168] followed. IBM is very active in AI and AI ethics, and issued a variety of papers, including trust and transparency principles[1169] or everyday AI ethics[1170], and advancing AI ethics beyond compliance.[1171] Further important players like Google[1172] and Microsoft[1173] also issued their own AI principles; together with Meta, Amazon and IBM, Google and Microsoft launched the Partnership on AI "to educate the public, open up dialogue about AI technologies, and identify opportunities to use it to solve problems in the world."[1174] Google announced that it plans to address specific challenges in the area of AI with the help of an Advanced Technology External Advisory Council.[1175] The company moreover published responsible AI practices[1176] and a People & AI Guidebook[1177]. In an effort to embed ethics into codes, the German Bertelsmann foundation together with iRights.lab is working on "AlgoRules"[1178], and the Linux Foundation[1179] took a similar approach by publishing their principles for trusted AI.

[1165] SAP's Guiding Principles for Artificial Intelligenve are available at https://www.sap.com/documents/2018/09/940c6047-1c7d-0010-87a3-c30de2ffd8ff.html. Retrieved December 5, 2022.

[1166] Details on Sony's engagement in AI are available at https://www.sony.net/SonyInfo/csr_report/humanrights/hkrfmg0000007rtj-att/AI_Engagement_within_Sony_Group.pdf#:~:text=The%20%E2%80%9CSony%20Group%20AI%20Ethics%20Guidelines%E2%80%9D%20%28Guidelines%29%20set,and%20services%20by%20Sony%2C%20including%20entertainment%20content%20. Retrieved October 3, 2021.

[1167] Background information on IBM's initiative are available at https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf. Retrieved October 3, 2021.

[1168] Details on Tencent and other companies is provided by Wenjun Wu, TiejunHuang, KeGong: Ethical principles and governance technology development of AI in China. Engineering 2020, vol. 6, issue 3, pp. 302-309, available at https://doi.org/10.1016/j.eng.2019.12.015. Retrieved October 3, 2021.

[1169] IBM's trust and transparency principles are available at https://www.ibm.com/policy/trust-principles/. Retrieved December 5, 2022.

[1170] IBM's Everyday AI Ethics are available at https://www.ibm.com/design/ai/ethics/everyday-ethics/. Retrieved December 5, 2022.

[1171] IBM's document Advancing AI Ethics Beyond Compliance is available at https://www.ibm.com/thought-leadership/institute-business-value/report/ai-ethics. Retrieved December 5, 2022.

[1172] Google's AI principles are available at https://blog.google/technology/ai/ai-principles/. Retrieved October 3, 2021.

[1173] Microsoft's document on responsible AI is available at https://www.microsoft.com/en-gb/ai/responsible-ai?activetab=pivot1%3aprimaryr6. Retrieved October 3, 2021.

[1174] Tas Bindi: Amazon, Google, Facebook, IBM, and Microsoft form AI non-profit. Article published September 29 2016, available at https://www.zdnet.com/article/amazon-google-facebook-ibm-and-microsoft-form-ai-non-profit/. Retrieved October 3, 2021.

[1175] Abner Li: Google names external advisory council to guide artificial intelligence usage. Article published March 26 2019, available at https://9to5google.com/guides/google-ai-principles/#:~:text=Google%20AI%20Google%20AI%20Principles.%20Back%20in%20June%2C,implemented%20to%20ensure%20that%20all%20guidelines%20are%20enforced. Retrieved October 3, 2021.

[1176] Google's responsible AI practices are available at https://ai.google/responsibilities/responsible-ai-practices/. Retrieved December 5, 2022.

[1177] Google's People & AI guidebook is available at https://pair.withgoogle.com/guidebook/. Retrieved December 5, 2022.

[1178] Background information on the initiative is available at the foundation's website: https://www.bertelsmann-stiftung.de/de/unsere-projekte/ethik-der-algorithmen/projektnachrichten/algorules-wie-kriegen-wir-die-ethik-in-den-code/. Retrieved December 5, 2022.

[1179] The Linux foundation's principles for trusted AI are available at https://lfaidata.foundation/blog/2021/02/08/lf-ai-data-announces-principles-for-trusted-ai/. Retrieved December 5, 2022.

Like many others who believe in the future of this technology, Microsoft is involved in research in the topic[1180] and runs a project with the Massachusetts Institute of Technology's Computer Science & Artificial Intelligence Lab on Trustworthy & Robust AI Collaboration.[1181] Given the fact that Microsoft's applications are used by the vast majority of organizations[1182], the company is in the spotlight of the authorities more than others: Microsoft was criticized for some of its AI-based Office 365 applications, for example Delve and Graph: a German regulator conducted two surveys on the use of Microsoft Office 365 in 2019 to find out how local companies use Office 365,[1183] and local labor chambers also dealt with Graph, Delve and MyAnalytics since these applications are relevant for the working environment.[1184] Controversial discussions around associated data protection risks of (Microsoft) Office 365 are still ongoing between regulators.[1185] Moreover, the Dutch Ministry of Security and Justice commissioned a data privacy impact assessment for Microsoft Office ProPlus[1186] which came to the result that the use of Microsoft's Office ProPlus Enterprise indeed involves privacy risks,[1187] and in mid-2020, the European Data Protection Supervisor initiated an own investigation into EU institutions' use of Microsoft products and services.[1188] Apple communicates a different approach: even though not tailored with a specific regard to AI, its consent for IDFA[1189] initiative is an example of how Privacy by Design could be a "game changer for online and mobile privacy and drive change in a way that legislative efforts have so far been unable":[1190] if users cannot be tracked and targeted without

[1180] Background information on Microsoft's activities in this area are available at https://www.microsoft.com/en-us/research/research-area/artificial-intelligence/?facet%5Btax%5D%5Bmsr-research-area%5D%5B0%5D=13556&sort_by=most-recent. Retrieved October 3, 2021.

[1181] Further details on the Microsoft and MIT research collaboration are available at https://trac.csail.mit.edu/#:~:text=The%20Trustworthy%20and%20Robust%20AI%20collaboration%20%28TRAC%29%20between,which%20spans%20safety%20%26%20reliability%2C%20intelligibility%2C%20and%20accountability. Retrieved October 3, 2021.

[1182] Microsoft's use rate in the public sector in Germany is as high as 96 %, see Price Waterhouse Coopers 2019 report: Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Article published August 2019, available at https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile. Retrieved October 3, 2021.

[1183] Background information on the Microsoft Office 365 survey is available at https://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.16021.de. Retrieved October 3, 2021.

[1184] For example, in Austria, see ttps://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf. Retrieved October 3, 2021.

[1185] Jörg Heidrich: Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig. Article published October 23 2020, available at https://www.heise.de/news/Datenschutzbehoerden-erklaeren-den-Einsatz-von-Microsoft-365-fuer-rechtswidrig-4931745.html. Retrieved October 3, 2021.

[1186] That is, for Office 2016 MSI and Office 365 CTR.

[1187] The DPIA was carried out by the "Privacy Company". Background information on their endeavor is available at https://www.privacycompany.eu/blogpost-en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise. Retrieved October 3, 2021.

[1188] The outcome is summarized in a paper the EDPB published on July 2 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html.

[1189] IDFA is an abbreviation for "ID for advertisers", a unique identifier on the Apple iPhone that allows mobile advertisers to track usage of applications on the phone and websites accessed via the mobile browser to use this information for targeting purposes.

[1190] Phil Lee: Why Apple's "Consent for IDFA" announcement is a game changer for online and mobile privacy. Article published on June 24, 2020, available at https://www.fieldfisher.com/en/services/privacy-security-and-their consent, this will necessarily impact further data processing as is the custom nowadays: since consent is only valid if it is obtained in an informed manner, it is questionable whether the implementation of opt-in-mechanisms that are typically tailored as a one-time effort can be considered legally valid as this would mean that one single declaration of intent towards an unknown and / or growing number of legally independent entities that engage in different processing operations could suffice as opposed to the repeated solicitation of consent for various companies and different purposes. Apple recently released the latest version of its iPhone operating system, iOS 15: this new operating system brings a slew of privacy-specific features such as the "Mail Privacy Protection" feature and the "Privacy Report" feature which allows users to check how (often) apps are using (which of) their data.[1191]

5.9. Technical standards

5.9.1. ISO standards

GDPR generally requires appropriate technical and organizational measures to protect personal data, and this is where the International Organization for Standardization (ISO) comes into play: given the complexity and growth of regulatory requirements, compliance is increasingly difficult to achieve, and that is why some companies consider certifications like ISO 27001, the international standard for Information Security Management Systems (ISMS); ISO 27701 is concerned with Privacy Information Management System (PIMS). ISO issued another standard for the protection of personally identifiable information in public clouds. ISO/IEC 27018:2014 is a new code of practice which promotes privacy protection in the cloud. It establishes guidelines "in order to implement measures to protect personally identifiable information in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment".[1192] Key topics include controls, accessibility and portability as well as secondary use of data and data breaches.[1193] Even though some GDPR requirements are not covered, ISO controls[1194] can be a starting point for achieving the necessary technical and operational requirements to reduce risks of data processing activities as those standards deals with e.g. risk assessment, Privacy by Design and supplier relationships. Moreover, ISO intends to establish a

information/privacy-security-and-information-law-blog/why-apples-consent-idfa-announcement-is-a-game-changer. Retrieved October 3, 2021.

[1191] Steven Roosa, Daniel Rosenzweig: iOS 15 – new privacy features industry should note. Article published October 7 2021, available at https://www.ntanalyzer.com/blog/ios-15-new-privacy-features-industry-should-note/. Retrieved October 3, 2021.

[1192] Background information on ISO/IEC 27018:2014 is available at https://www.iso.org/standard/61498.html. Retrieved October 3, 2021.

[1193] Michael Fekete: ISO/IEC 27018 – new code of practice promotes privacy protection in the cloud, 2014. Article published October 20 2014, available at https://www.lexology.com/library/detail.aspx?g=ff6d5e13-1f3e-4539-887e-20dfc12eb8fd. Retrieved October 3, 2021.

[1194] Further details on ISO standards are available at https://www.iso.org/home.html. Retrieved October 3, 2021.

framework for Artificial Intelligence: the joint technical committee of the International Organization for Standardization and the International Electro-technical Commission (IEC) are working on standards to ensure trustworthiness of AI technology.[1195] The first meeting of the ISO AI committee was already held in early 2018, and the following ISO standards address AI: ISO/IEC JTC 1/SC 41 on Internet of Things,[1196] ISO/IEC JTC 1/SC 38 on Cloud computing and distributed platforms,[1197] and ISO/IEC JTC 1/SC 37 on biometrics.[1198] More specifically, in the context of AI, ISO's work furthermore covers the following areas:

- *ISO/IEC 23894 – **AI Risk Management**;*[1199]
- *ISO/IEC WD 42001 – **AI Management systems**;*[1200]
- *ISO/IEC WD 5338 73 – **AI system life cycle processes**;*[1201]
- *ISO/IEC AWI TR 5469 – **Functional safety and AI systems**;*[1202]
- *ISO/IEC AWI TR 24368 – Overview of **ethical and societal concerns**;*[1203]
- *ISO/IEC TR 24027 – **Bias in AI systems and AI-aided decision making**;*[1204]
- *ISO/IEC CD 24668 – **Process management framework for Big Data analytics**;*[1205]
- *ISO/IEC CD 38507 – **Governance implications of the use of AI by organizations**;*[1206]
- *ISO/IEC TR 24028:2020 – Overview of **trustworthiness in Artificial Intelligence**;*[1207]
- *ISO/IEC DTR 24029 and ISO/IEC AWI 24029-2 – **Robustness of neural networks**;*[1208]

[1195] Background information on the IEC's work is available at https://www.iso.org/standard/74438.html. Retrieved October 3, 2021.

[1196] The text of ISO/IEC JTC 1/SC 41 is available at https://www.iso.org/committee/6483279.html. Retrieved October 3, 2021.

[1197] The text of ISO/IEC JTC 1/SC 38 is available at https://www.iso.org/committee/601355.html. Retrieved October 3, 2021.

[1198] The text of ISO/IEC JTC 1/SC 37 is available at https://www.iso.org/committee/313770.html. Retrieved October 3, 2021.

[1199] The text of ISO/IEC 23894 is available at https://www.iso.org/standard/77304.html. Retrieved December 5, 2022.

[1200] The text of ISO/IEC WD 42001 is available at https://www.iso.org/standard/81230.html. Retrieved December 5, 2022.

[1201] The text of ISO/IEC WD 5338 73 is available at https://www.iso.org/standard/81118.html. Retrieved December 5, 2022.

[1202] The text of ISO/IEC AWI TR 5469 is available at https://www.iso.org/standard/81283.html. Retrieved December 5, 2022.

[1203] The text of ISO/IEC AWI TR 24368 is available at https://www.iso.org/standard/78507.html. Retrieved December 5, 2022.

[1204] The text of ISO/IEC TR 24027 is available at https://www.iso.org/standard/77607.html?browse=tc. Retrieved December 5, 2022.

[1205] The text of ISO/IEC CD 24668 is available at https://www.iso.org/standard/78368.html. Retrieved December 5, 2022.

[1206] The text of ISO/IEC CD 38507 is available at https://www.iso.org/standard/56641.html. Retrieved December 5, 2022.

[1207] The text of ISO/IEC TR 24028:2020 is available at https://www.iso.org/standard/77608.html. Retrieved December 5, 2022.

[1208] The text of part 1 (overview: ISO/IEC DTR 24029) is available at https://www.iso.org/standard/77609.html. The text of part 2 (methodology: ISO/IEC AWI 24029-2 is available at https://www.iso.org/standard/79804.html. Retrieved December 5, 2022.

- *ISO/IEC AWI TR 24372 – Overview of* ***computational approaches for AI systems****;*[1209]
- *ISO/IEC WD TS 4213 76 –* ***Assessment of Machine Learning classification performance****;*[1210]
- *ISO/IEC AWI 25059 –* ***Quality model for AI-based systems*** *(Systems and software Quality Requirements and Evaluation: SQuaRE).*[1211]

The ISO is moreover working on several standards for data quality for analytics and Machine Learning: part 1[1212] provides an overview and covers terminology and examples; part 2[1213] deals with quality measures, part 3[1214] governs data quality management, and part 4[1215] provides a data quality process framework. What is truly remarkable is that ISO announced to introduce a new standard for Privacy by Design, ISO/DIS 31700 in early 2023:[1216] fourteen years after its introduction by former Canadian privacy commissioner, Privacy by Design is about to become an international privacy standard for the protection of consumer products and services. However, ISO 31700 will not be a conformance standard.[1217]

5.9.2. CEN, CENELEC and ETSI standards

As regards relevant technical standards, it is vital to know that such standards will play an important role in the context of the draft AI Act, even though technical standards are not mentioned in the EU's draft Artificial Intelligence Act:[1218] technical standards will be jointly developed by the European standardization bodies, the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards

[1209] The text of ISO/IEC AWI TR 24372 is available at https://www.iso.org/standard/78508.html. Retrieved December 5, 2022.

[1210] The text of ISO/IEC WD TS 4213 76 is available at https://www.iso.org/standard/79799.html. Retrieved December 5, 2022.

[1211] The text of ISO/IEC AWI 25059 is available at https://www.iso.org/standard/80655.html. Retrieved December 5, 2022.

[1212] The text of ISO/IEC WD 5259-1 (part 1) is available at https://www.iso.org/standard/80655.html. Retrieved December 5, 2022.

[1213] The text of ISO/IEC WD 5259-2 (part 2) is available at https://www.iso.org/standard/81860.html. Retrieved December 5, 2022.

[1214] The text of ISO/IEC WD 5259-3 (part 3) is available at https://www.iso.org/standard/81092.html. Retrieved December 5, 2022.

[1215] The text of ISO/IEC WD 5259-4 (part 4) is available at https://www.iso.org/standard/81093.html. Retrieved December 5, 2022.

[1216] The text of ISO/DIS 31700 is available at https://www.iso.org/standard/76772.html. Retrieved January 19, 2023.

[1217] Howard Solomon: Privacy by Design to become an ISO standard next month. Article published January 11 2023, available at https://www.itworldcanada.com/article/privacy-by-design-to-become-an-iso-standard-next-month/521415?mkt_tok=MTM4LUVaTS0wNDIAAAGJS0q3vTc2wGOv97CzHvWrfuVuy0g03NHESUYs9hBY2VJUZx2kRq7P8-PHtd90alDmo9rCjwp7I7WYC4fteM6-Dfx4qV5xattmN-4oeH16JcM7. Retrieved January 19, 2023.

[1218] Luca Bertuzzi: AI standards set for joint drafting among European standardization bodies. Article published May 30 2022, updated June 2 2022, available at https://www.euractiv.com/section/digital/news/ai-standards-set-for-joint-drafting-among-european-standardisation-bodies/. Retrieved January 10, 2023.

Institute (ETSI). Providers do not have to follow these standards, but the advantage is that they would enjoy a presumption of conformity.[1219] Despite the fact that the standards are presented as voluntary, that might perhaps not be realistic, for the following reasons: a harmonized approach is a safer option[1220] because the alternative would be that providers would have to interpret the AI Act's essential requirements for themselves, which in effect may lead to far more effort and this way, far more cost. This is especially true given that global industry players prefer international standards over national or regional standards because they create a level playing field in markets throughout the world.[1221] As a result, technical standards will be crucial in bringing down compliance costs that they have been defined as the "real rulemaking".[1222] The standardization bodies will focus on topics like risk management, governance, cybersecurity, documentation requirements, data quality and accuracy, transparency and information to users as well as human oversight, and post-market monitoring; they will also define the validation procedures and methodologies for assessing if an AI system is fit-for-purpose and whether it meets those standards, and, amongst other things, submit a progress report to the European Commission every six months.[1223] From a European perspective, standards are moreover a means of regaining digital sovereignty by engaging in the definition of technological standards for emerging technologies in strategic areas by promoting EU interests in international standardization bodies to counter growing international competition.[1224] The European Telecommunications Standards Institute is also actively engaged in this area:[1225]

- *DGR SAI-001 – **Securing Artificial Intelligence: AI Threat Ontology**;*[1226]
- *DGR SAI-002 – **Securing Artificial Intelligence: Data Supply Chain Report**;*[1227]

[1219] See Art. 40 of the draft AI Act.

[1220] Michael Veale, Frederik Zuiderveen Borgesius: Demystifying the draft EU Artificial Intelligence Act. Article published July 31 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852. Retrieved January 12, 2023.

[1221] Benjamin Larsen: Harmonizing Artificial Intelligence: The role of standards in the EU AI regulation. Article published January 18 2022, available at https://montrealethics.ai/harmonizing-artificial-intelligence-the-role-of-standards-in-the-eu-ai-regulation/.

[1222] Michael Veale, Frederik Zuiderveen Borgesius: Demystifying the draft EU Artificial Intelligence Act. Article published July 31 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852. Retrieved January 12, 2023.

[1223] Luca Bertuzzi: AI standards set for joint drafting among European standardization bodies. Article published May 30 2022, updated June 2 2022, available at https://www.euractiv.com/section/digital/news/ai-standards-set-for-joint-drafting-among-european-standardisation-bodies/. Retrieved January 10, 2023.

[1224] European Commission Directorate General for Internal Market, Industry, Entrepreneurship and SMEs: New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market. press release published February 2 2022, available at https://single-market-economy.ec.europa.eu/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital-2022-02-02_en. Retrieved January 10, 2023.

[1225] The below list is non-exhaustive.

[1226] The text of this work item is available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856. Retrieved December 5, 2022.

[1227] The text of this work item is available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857. Retrieved December 5, 2022.

- *DGS SAI-003 –* ***Securing Artificial Intelligence: Security Testing of AI;***[1228]
- *DGR SAI-005 –* ***Securing Artificial Intelligence: Mitigation Strategy Report;***[1229]
- *TR 103 674 SmartM2M –* ***Artificial Intelligence and the oneM2M architecture****;*[1230]
- *TR 103 675 SmartM2M –* ***AI for IoT: A Proof of Concept****;*[1231]
- *GS/ARF-003* ***Augmented Reality Framework architecture****;*[1232]

5.9.3. IEEE standards

Irrespective of the bodies involved in technical standards to support the conformity of AI systems in the framework of EU's new draft AI law, it is worth looking at other technical standards to complete the picture of standardization in the context of AI. In this regard, the IEEE plays an important role: apart from IEEE's Ethically Aligned Design that has been specifically created to address ethical and human values when it comes to the design and use of AI,[1233] IEEE is also engaged in an impressive number of initiatives in the area of autonomous and intelligent systems such as:

- *IEEE P7003 –* ***Algorithmic Bias Considerations****;*[1234]
- *IEEE P7001 –* ***Transparency of Autonomous Systems****;*[1235]
- *IEEE P7000 –* ***Draft Model Process for Addressing Ethical Concerns During System Design;***[1236]

[1228] The text of this work item is available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58860. Retrieved December 5, 2022.

[1229] The text of this work item is available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59214. Retrieved December 5, 2022.

[1230] The text of this work item is available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57866. Retrieved December 5, 2022.

[1231] The text of this work item is available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57867. Retrieved December 5, 2022.

[1232] The text of this work item is available at https://www.etsi.org/deliver/etsi_gs/ARF/001_099/003/01.01.01_60/gs_ARF003v0101 01p.pdf. Retrieved December 5, 2022.

[1233] IEEE: Ethically aligned design – a vision for prioritizing human well-being with autonomous and intelligent systems, published March 31 2029, available at https://engagestandards.ieee.org/rs/211-FYL-955/images/EAD1e.pdf?mkt_tok=eyJpIjoiWkRVME1UVm1OREE1TVRSbSIsInQiOiIxY3RONFl6YXh0cWxSRUpLNE9taUtwQllpaXNkYktmd3FDM2lOQ1ZNXC9YUURKV3Z4b2dJc3d3ekNDREdTd24zMHNcL0xUTEFqeFFoYTN4NWNqQUZRclY0amMyTzhXeU9VXC9yNjhneWlIeHFHV3lSMU1rRGxmeUJSTU9cL3dDeXZmN1AifQ%3D%3D. Retrieved October 15, 2021.

[1234] The text of IEEE's Algorithmic Bias Considerations (IEEE P7003) is available at https://standards.ieee.org/project/7003.html. Retrieved December 5, 2022.

[1235] The text of IEEE's Transparency of Autonomous Systems (IEEE P7001) is available at https://standards.ieee.org/project/7001.html. Retrieved December 5, 2022.

[1236] The text of IEEE's Draft Model Process for Addressing Ethical Concerns During System Design (IEEE P7000) is available at https://standards.ieee.org/project/7000.html. Retrieved December 5, 2022.

- *IEEE P7009 – **Standard for fail-safe design of autonomous and semi-autonomous systems**;*[1237]
- *IEEE P2863 – **Recommended Practice for Organizational Governance of Artificial Intelligence**;*[1238]
- *IEEE 7010 – **Recommended Practice for assessing the impact of autonomous and intelligent systems on human well-being**.*[1239]

IEEE furthermore offers an ethics certification program for Autonomous and Intelligent Systems (ECPAIS) to create specifications for certification and advance accountability and transparency and this way, reduce algorithmic bias. IEEE says that the "value of this certification process in the marketplace and society at large cannot be underestimated. The proliferation of systems in the form of smart homes, companion robots, autonomous vehicles or any myriad of products and services that already exist today desperately need to easily and visually communicate to consumers and citizens, whether they are deemed "safe" or "trusted" by a globally recognized body of experts providing a publicly available and transparent series of marks."[1240]

5.9.4. ITU standards

The International Telecommunication Union (ITU) is the United Nations agency for information and communication technologies. The ITU is part of the AI for good initiative[1241] and issued the following documents that are relevant for AI:

- *ITU-T Y.3531 **Cloud computing – functional requirements for Machine Learning as a service**.*[1242]
- *Y.Suppl.63 to ITU-T Y.4000 series – **Unlocking Internet of things with Artificial Intelligence**: Where we are and where we could be.*[1243]

[1237] The text of IEEE's Standard for fail-safe design of autonomous and semi-autonomous systems (IEEE P7009) is available at https://standards.ieee.org/project/7009.html. Retrieved December 5, 2022.

[1238] The text of IEEE's recommended practice for Organizational Governance of Artificial Intelligence (IEEE P2863) is available at https://standards.ieee.org/project/2863.html. Retrieved December 5, 2022.

[1239] The text of IEEE's recommended practice for assessing the impact of autonomous and intelligent systems on human well-being (IEEE 7010) is available at https://standards.ieee.org/standard/7010-2020.html. Retrieved December 5, 2022.

[1240] IEEE's statement on the Ethics Certification Program for Autonomous and Intelligent Systems, available at https://standards.ieee.org/industry-connections/ecpais.html. Retrieved October 15, 2021.

[1241] Background information on the initiative is available on ITU's website at https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx. Retrieved October 3, 2021.

[1242] The text of this work item is available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14484. Retrieved December 5, 2022.

[1243] The text of this work item is available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14103. Retrieved December 5, 2022.

- *ITU-T Y. 4470 – **Reference architecture of Artificial Intelligence service exposure for smart sustainable cities**.*[1244]

This chapter demonstrated that there are numerous relevant sources of law at international, European, and national level, including sector and industry specific as well as data and processing specific rules, and regulations that address algorithm-based decision-making and AI. It can generally be said that data protection and data privacy laws are on the rise. Even though the GDPR can be considered a role model law that inspired many legislative initiatives around the globe, GDPR also poses challenges due to unclear protective goals, indeterminate terms, or fragmentation. Another important aspect is that the legal framework for AI shall not be seen in isolation since other relevant sources of law provide for rules that crucial from a data protection perspective as well, for example, with regards to liability, product safety, trade secrets or digital content. In summary, the legal landscape in the context of algorithmic data processing is not in its infancy, and the presumption of conformity gives rise to hope that this circumstance will attract companies to engage in relevant new technical standards.

6. Guidance, recommendations, and initiatives

This chapter provides a detailed overview over existing recommendations, guidance, and initiatives in the context of AI at institutional, international, European, and national level. It includes regulator guidance as well as civil society and multistakeholder recommendations, or expert guidelines. What these recommendations have in common is that they address potential issues when Big Data and AI applications are designed and implemented from an ethics, legal, accountability, societal and individual, including data protection and privacy perspective. Even though these initiatives are non-binding, they are promising and inspiring because they discuss new concepts, new controller obligations, or new data subject rights. They moreover demonstrate that already now, there is an impressive number of initiatives that reflect on the challenges of today's digital world, which is truly useful given that Big Data and AI is being used across the board, for example, in production (robotics), for operations (forecasting), in marketing (analytics), in the finance (scoring) and in the healthcare sector (diagnostics), in "smart cities," "smart homes," and "smart devices" or for tracking and targeting purposes.

[1244] The text of this work item is available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14503. Retrieved December 5, 2022.

6.1. Guidance and recommendations at international level[1245]

6.1.1. OECD AI principles

The 2019 OECD principles on Artificial Intelligence[1246] aim to promote AI that respects democratic values, human rights, the rule of law as well as transparency and diversity and are the first intergovernmental standard that has been adopted by 42 countries. OECD's principles have been developed by a 50+ member expert group on AI who named the following five complementary value-based AI principles:[1247]

I. *"**AI should benefit people and the planet by driving inclusive growth, sustainable development, and well-being**[1248].*

II. ***AI systems should be designed in a way that respects the rule of law, human rights, democratic values, and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society**.*

III. ***There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them**.*

IV. ***AI systems must function in a robust, secure, and safe way throughout their life cycles** and **potential risks should be continually assessed and managed**.*

V. ***Organizations and individuals developing, deploying, or operating AI systems should be held accountable for their proper functioning in line with the above principles**".*

Consistent with these value-based principles, the OECD also adopted recommendations[1249] for national (government) AI policy priorities which shall also be read in the context of OECD's Privacy Principles:

I. *"**Facilitate public and private investment in research & development to spur innovation in trustworthy AI**.*

[1245] Given the fact that there is an intersection between, for instance, civil society and multistakeholder initiatives, it is not always possible to clearly distinguish and properly group various AI recommendations and guidelines.

[1246] Background information on OECD's work in AI is available at http://www.oecd.org/going-digital/ai/principles/. Retrieved October 3, 2021.

[1247] Background information on as well as the text of OECD's AI principles, their AI Policy Observatory, or framework for the classification of AI systems is available at https://www.oecd.org/going-digital/ai/principles/#:~:text=The%20Recommendation%20identifies%20five%20complementary%20values-based%20principles%20for,proper%20functioning%20in%20line%20with%20the%20above%20principles. Retrieved October 3, 2021.

[1248] Bold Italic means emphasis added.

[1249] Further details on OECD's recommendations available at http://www.oecd.org/going-digital/ai/oecd-moves-forward-on-developing-guidelines-for-artificial-intelligence.htm. Retrieved October 3, 2021.

II. ***Foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge****.*

III. ***Ensure a policy environment that will open the way to deployment of trustworthy AI systems****.*

IV. ***Empower people with the skills for AI and support workers for a fair transition****.*

V. ***Co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI****."*

6.1.2. G20, G7 and World Economic Forum recommendations on AI

In 2019, the G20 formulated human-centered AI principles[1250] which are inspired by OECD's AI principles. These guidelines stress that AI shall be fair, transparent, and accountable and that it shall respect privacy, equality, diversity as well as internationally recognized labor rights. The latter is important since the use of AI is believed to create a new virtual workforce.[1251] The G20 statement thus also addresses complementary digital economy issues. In addition, Think20, a task force of the G20 research and policy advice network that is working on the future of work and education in the digital age, focuses on AI-based learning technologies to overcome current educational challenges.[1252] G20 AI principles are split into two sections, the first section deals with principles for responsible stewardship of trustworthy AI and focuses on:

I. *"****Inclusive growth, sustainable development, and well-being****,*

II. ***Human-centered values and fairness****,*

III. ***Transparency and explainability****,*

IV. ***Robustness, security, and safety****,*

V. ***Accountability****."*

The second section is about national policies and international co-operation for trustworthy AI and stresses the need for international co-operation, investing in AI research, fostering a digital ecosystem for AI, shaping a policy environment for AI, and building human capacity and preparing for labor market

[1250] G20 Ministerial Statement on Trade and Digital Economy including human-centered AI published June 9 2019, available at http://www.g20.utoronto.ca/2019/2019-g20-trade.html. Retrieved October 3, 2021.

[1251] Dennis Späth: Artificial Intelligence is transforming the workforce as we know it. Article published March 18, 2019, available at https://workplaceinsight.net/artificial-intelligence-is-transforming-the-workforce-as-we-know-it/. Retrieved October 3, 2021.

[1252] Samed Olukoya: Think20 says Artificial Intelligence based learning technologies can overcome current educational challenges. Article published August 25 2020, available at https://investorsking.com/2020/08/25/think20-says-artificial-intelligence-ai-based-learning-technologies-can-overcome-current-educational-hallenges/. Retrieved October 3, 2021.

transformation.[1253] In 2018, G7 leaders issued the Charlevoix Common Vision for the Future of Artificial Intelligence,[1254] and the World Economic Forum published a White Paper on AI[1255] in which the following four central principles are proposed: fairness and active inclusion as well as the right to understanding and the right to redress. The World Economic Forum moreover suggests that companies take the following steps to prevent discriminatory outcomes: being transparent about efforts to identify, prevent, and mitigate human rights risks; identifying human rights risks linked to business operations, and taking effective action to prevent and mitigate risks.

6.1.3. United Nations

6.1.3.1. IWGDPT's Working Paper and ITU's AI for good initiative

In 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT) issued a working paper[1256] which identified the following main issues regarding data protection: lack of transparency and intelligibility, erosion of consent and purpose limitation, the risk of re-identification as well as risk of detecting sensitive information. Their key recommendations are fairness and respect of fundamental human right, accountability, privacy and ethics by design and non-discrimination. Together with various other UN organizations and the Association for Computing Machinery, the International Telecommunication Union (ITU)[1257] organized the AI for Good Global Summit, the leading United Nations platform to foster the dialogue on beneficial use of AI.[1258] In accordance with the United Nations Sustainable Development Goals (SDG), this initiative is focusing on using AI for sustainable development. The summit established various focus groups, for example AI for Health, Machine Learning for Future Networks (5G), Environmental Efficiency for AI and other Emerging Technologies, AI for Autonomous and Assisted Driving and the AI for Good Repository; the ITU moreover intends to draft technical reports and specifications for Machine Learning.[1259] AI for Good

[1253] G20 AI principles. Paper published June 9 2019, available at https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf. Background information on G20's work in this area is available at http://www.g20.utoronto.ca/2019/2019-g20-trade.html. Retrieved October 3, 2021

[1254] Charlevoix Common Vision for the Future of Artificial Intelligence. Paper published 2018, available at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-artificial-intelligence-artificielle.aspx?lang=eng. Retrieved October 3, 2021.

[1255] The World Economic Forum: How to Prevent Discriminatory Outcomes in Machine Learning. Paper published March 2018, available at http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discriminatory_Outcomes_in_Machine_Learning.pdf. Retrieved October 3, 2021.

[1256] IWGDPT's working paper on privacy and Artificial Intelligence published November 30 2018, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf. Retrieved October 3, 2021.

[1257] ITU is UN's agency for information and communication technologies.

[1258] Background information on the summit series is available on ITU's website at https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx. Retrieved October 3, 2021.

[1259] Background information on ITU's Focus Group on Machine Learning for future networks including 5G is available at https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx. Retrieved October 3, 2021.

focuses on the following key areas: accountability, fairness, transparency, explicability, robustness, safety and security as well as inclusive growth, sustainable development and well-being based on human-centered values.

6.1.3.2. UNESCO: Recommendation on the Ethics of Artificial Intelligence, Beijing declaration on Artificial Intelligence and Education

In 2020, the United Nations Educational, Scientific and Cultural Organization (UNESCO) set up an international expert group composed of "the world's leading experts on the social, economic and cultural challenges of Artificial Intelligence to draft internationally applicable recommendations on ethical issues raised by the development and use of AI".[1260] With the goal to develop the first global normative instrument on this key issue,[1261] UNESCO's Ad Hoc Expert Group (AHEG)[1262] provided a recommendation[1263] on the ethics of Artificial Intelligence in which they stress the importance of human dignity, privacy, fairness, transparency, safety, accountability, human oversight as well as sustainability, diversity and inclusiveness, and the need to address social, economic, employment and environmental consequences of AI; the following areas of policy action have been identified in the framework of their recommendation: governance, ethical stewardship, impact assessments, capacity building and international cooperation for AI Ethics. UNESCO stresses that AI has the potential to address some of the biggest challenges in the field of education by allowing for innovative teaching and learning practices. Against this background, UNESCO published[1264] the Beijing Consensus on Artificial Intelligence and Education.[1265] In addition, UNESCO published an AI Decision Makers' Toolkit[1266] to help address certain issues that arise from AI's role in the context of education, including gender equality as well as challenges in online disinformation and hate speech.

[1260] Background information on UNESCO's international expert group is available at https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 3, 2021.

[1261] Further details UNESCO's international expert group tasked to draft global recommendation on the ethics of AI are available at https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 3, 2021.

[1262] Background information on AHEG is available at https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 3, 2021.

[1263] AHEG's draft text of a recommendation on the ethics of Artificial Intelligence was published May 15 2020, and is available at https://ircai.org/wp-content/uploads/2020/07/Recommendation_first_draft_ENG.pdf. Retrieved October 3, 2021.

[1264] UNESCO: First ever consensus on Artificial Intelligence and Education published by UNESCO. Press release published June 25 2019, available at https://en.unesco.org/news/first-ever-consensus-artificial-intelligence-and-education-published-unesco. Retrieved October 3, 2021.

[1265] The text of the Beijing Consensus on Artificial Intelligence and Education is available at https://unesdoc.unesco.org/ark:/48223/pf0000368303. Retrieved October 3, 2021.

[1266] Background information on UNESCO's decision maker's toolkit for AI is available at https://en.unesco.org/artificial-intelligence/decision-makers-toolkit. Retrieved October 3, 2021.

6.1.3.3. UNICEF: AI for Children

As part of their Artificial Intelligence for Children Policy project,[1267] the United Nations Children's Fund (UNICEF) developed a policy guidance[1268] on "how to promote children's development in AI strategies and practices (…) to bring a balanced perspective to the policy table with clear, usable principles for implementing AI that supports child rights" as a response to the fact that, despite the growing interest in and application of AI, little attention has so far been paid to how it affects children and their rights.[1269]

6.1.3.4. United Nation's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

The report of the United Nation's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression[1270] dealt with implications of AI technologies for human rights and underlined the importance of freedom of opinion and expression, individual autonomy, the right to privacy and to effective remedy, the obligation of non-discrimination and the need for human rights impact assessments and audits.

6.1.3.5. UNICRI's center on AI and Robotics

In 2015, UNICRI, the United Nations Interregional Crime and Justice Research Institute established a center on AI and robotics to "help focus expertise on Artificial Intelligence (AI) throughout the UN in a single agency."[1271] The center's focus is on awareness-raising, exchange of information education, and harmonization of relevant stakeholders.

6.1.4. UNI Global Union top 10 Principles for Ethical Artificial Intelligence

UNI Global Union (UNI) is a global union federation for national and regional trade unions representing 650 trade unions in the fastest growing sectors in the world, skills and services.[1272] UNI is concerned

[1267] Further details on Artificial Intelligence for Children Policy project are available at https://www.unicef.org/globalinsight/featured-projects/ai-children. Retrieved October 3, 2021.

[1268] UNICEF's Policy Guidance on AI for children has been published in September 2020 and is available at https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf. Retrieved October 3, 2021.

[1269] UNICEF provides background information on this issue at https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children. Retrieved October 3, 2021.

[1270] United Nation's Special Rapporteur's report: Promotion and protection of the right to freedom of opinion and expression published August 29 2018, available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf. Retrieved October 3, 2021.

[1271] Background information on UNICRI's center on AI and robotics is available at https://unicri.it/in_focus/on/UNICRI_Centre_Artificial_Robotics. Retrieved October 3, 2021.

[1272] Further details on UNI Global Union are available at https://uniglobalunion.org/. Retrieved October 3, 2021.

with protecting workers' rights and since Artificial Intelligence may change the "Future World of Work",[1273] UNI joined the multi-stakeholder Partnership on AI (PAI)[1274] and developed top 10 principles for ethical AI in order to "put people and planet first"[1275] which demands AI to meet the following criteria: AI systems shall be transparent, equipped with an ethical black box, operate in a genderless and unbiased manner, adopt a human-in-command approach, serve people and planet, and ensure fundamental freedoms and rights. Finally, UNI calls for a ban on the attribution of responsibility to robots and the AI arms race.

6.2. Guidance and recommendations at European level

6.2.1. Ethics Guidelines for trustworthy AI

In 2018, 25 European countries signed a declaration of cooperation on Artificial Intelligence in which they declare their willingness to join forces and engage in a European approach to the topic.[1276] In 2019, the High-Level expert group on Artificial Intelligence presented ethics guidelines for trustworthy Artificial Intelligence.[1277] The High-Level Expert Group on Artificial Intelligence (HLEG) is an independent group of expert that was set up by the European Commission as part of the AI strategy in 2018.[1278] On the one hand, they recognize that AI is a key driver for economic growth through the digitalization of industry; on the other hand, according to these guidelines, AI can only be considered trustworthy if it respects applicable laws and regulations and if it respects certain ethical principles and values. The guidelines explain the following conditions that AI systems must meet to be considered trustworthy:[1279]

I. *"**Human agency and oversight**:[1280] AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper*

[1273] Background information on UNI's work is available at http://www.thefutureworldofwork.org. Retrieved October 3, 2021.

[1274] Further details on the Partnership on AI are available at https://www.partnershiponai.org/. Retrieved October 3, 2021.

[1275] Background information on the Future World of Work, including the Top 10 Principles for Ethical Artificial Intelligence are available at http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf. Retrieved October 3, 2021.

[1276] European Commission: EU Member States sign up to cooperate on Artificial Intelligence. News entry published April 10 2018, available at https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence. Retrieved October 3, 2021.

[1277] European Commission: Ethics guidelines for trustworthy AI. Guideline published April 18 2019, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Retrieved October 3, 2021.

[1278] Background information on the High-Level Expert Group on Artificial Intelligence is available at https://ec.europa.eu/futurium/en/ai-alliance-consultation. Retrieved October 3, 2021.

[1279] Guidelines for trustworthy AI published April 8 2019, available in various languages at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Retrieved October 3, 2021.

[1280] Bold means emphasis added.

oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches

II. ***Technical Robustness and safety**: AI systems need to be resilient and secure. They need to be safe, ensuring a fall-back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented.*

III. ***Privacy and data governance**: besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimized access to data.*

IV. ***Transparency**: the data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system and must be informed of the system's capabilities and limitations.*

V. ***Diversity, non-discrimination and fairness**: Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.*

VI. ***Societal and environmental well-being**: AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.*

VII. ***Accountability**: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes plays a key role therein, especially in critical applications. Moreover, adequate an accessible redress should be ensured."*

To assess whether an AI system that is being developed, deployed, procured or used, complies with HLEG's requirements of Trustworthy AI, the High-Level Expert Group on Artificial Intelligence furthermore issued an Assessment List for Trustworthy AI (ALTAI)[1281] which aims to provide a basic self-evaluation tool for trustworthy AI.

[1281] ALTAI is a self-assessment tool to help assess whether or not an AI system that is being developed, deployed, procured or used, complies with HLEG's requirements for Trustworthy AI. Background information on ALTAI is available at https://altai.insight-centre.org/. Retrieved October 3, 2021.

6.2.2. European Ethical Charter on the Use of AI in Judicial Systems (CEPEJ)

Certain countries have taken steps to introduce algorithmic decisions in the area of justice or policing[1282] for purposes like the prevention of offences, evaluation of the risk of recidivism and the assessment of the level of danger by using AI to ensure a better predictability of crime or decisions. It is therefore necessary to think about a corresponding legal framework. Consequently, the European Commission for the Efficiency of Justice (CEPEJ) came up with an Ethical Charter on the Use of AI in Judicial Systems and their Environment in 2018.[1283] This first charter on AI in judicial systems aims at improving the quality and efficiency of the European judicial systems and at compliance with fundamental rights guaranteed in the European Convention on Human Rights and the Council of Europe Convention on the Protection of Personal Data,[1284] and names five basic principles which have to be obeyed when AI is used in the judicial area:

I. *"**Principle of respect for fundamental rights**:[1285] ensure that the design and implementation of Artificial Intelligence tools and services are compatible with fundamental rights.*

II. ***Principle of non-discrimination**: Specifically prevent the development or intensification of any discrimination between individuals or groups of individuals.*

III. ***Principle of quality and security**: With regard to the processing of judicial decisions and data, use certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment.*

IV. ***Principle of transparency, impartiality and fairness**: Make data processing methods accessible and understandable, authorize external audits.*

V. ***Principle "under user control":** Preclude a prescriptive approach and ensure that users are informed actors and in control of their choice."*

[1282] Orla Lynskey: Criminal justice profiling and EU data protection law: precarious protection from predictive policing. International Journal of Law in Context 2019, vol. 15, issue 2, pp. 162-176.

[1283] Ethical Charter on the Use of AI in Judicial Systems and their Environment published December 4 2018, available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Retrieved October 15, 2021.

[1284] Mie Oehlenschlager: First European ethical charter on AI in judicial systems. Article published on January 16, 2019, available at https://dataethics.eu/first-european-ethical-charter-on-ai-in-judicial-systems/. Retrieved October 15, 2021.

[1285] Bold means emphasis added.

6.2.3. European Commission

6.2.3.1. White Paper on Artificial Intelligence

In early 2020, the European Commission presented its strategy for data and Artificial Intelligence. The EC altogether delivered four papers: a White Paper on Artificial Intelligence,[1286] a report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics,[1287] as well as two communications, one on Europe's digital future[1288] and one on the European strategy for data.[1289] Despite the fact that EC's statements do not constitute a legal regime for AI, they nonetheless provide guidance on the European Commission's priorities and potential next steps. They furthermore show that the Commission aims at positioning the EU as a digital leader in terms of both, trustworthy AI and the wider data economy.[1290] With regard to the future regulation of AI, the EC wants to pursue a uniform approach to avoid divergent member state requirements which may lead barriers within EU's single market.[1291] The EC's White Paper is acknowledging that AI may involve a variety of risks, for example for fundamental rights, privacy protection and non-discrimination as well as risks for safety and the effective functioning of the liability regime,[1292] and that is why the EC wants high-risk systems to meet security, privacy and fairness requirements before they go live by identifying high-risk sectors and applications in advance. The European Commission consequently acknowledges the importance of the seven key requirements that have been identified in HLEG's guidelines:[1293]

[1286] Commission White Paper on Artificial Intelligence published February 19 2020, available at https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Retrieved October 15, 2021.

[1287] Commission report on the safety and liability implications of Artificial Intelligence, IoT and robotics published February 19 2020, available at https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf. Retrieved October 15, 2021.

[1288] Background information on Europe's digital future is provided by the Commission at their website, available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en. Retrieved October 15, 2021.

[1289] The Commission's communication on the European strategy for data is available at is available at https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. Retrieved October 15, 2021

[1290] Lisa Peets, Marty Hansen, Sam Jungyun Choi, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission presents strategies for data and AI. Article published on February 20 2020, available at https://www.covingtondigitalhealth.com/2020/02/european-commissions-white-paper-on-artificial-intelligence-part-2-of-4/. Retrieved October 15, 2021.

[1291] Mark MacCarthy, Kenneth Propp: The EU's White Paper on AI: a thoughtful and balanced way forward. Article published March 5 2020, available at https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward. Retrieved October 15, 2021.

[1292] The Commission's White Paper on Artificial Intelligence is available at https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Retrieved October 15, 2021.

[1293] Background information on HLEG's work on Artificial Intelligence is available at https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai. Retrieved October 15, 2021.

I. *"**Human agency and oversight**.*[1294] *The principle of human agency is that a human should always be in ultimate control of an AI system. For example, an AI vehicle would not start without a human inserting a key and the vehicle can be manually overridden at any point if it malfunctions. The autonomous vehicle sector where the handover of control from human to machine and back again is one of main areas of contention and rife with practical problems,*

II. ***Technical robustness and safety**: The results from AI systems should be reproducible, predictable and accurate and AI systems should also be protected against cyberattacks,*

III. ***Privacy and data governance**: AI systems typically 'learn' from enormous sets of data from which they deduce relationships between the variables in such data. The data may be personal, and AI may be able to infer gender, sexual orientation, race, political and religious views. The sensitivity of this data is obvious and so it is incumbent on developers to ensure that AI systems are do not misuse this data or leak this information,*

IV. ***Transparency**: The inner workings of a AI system should be clearly explainable to all parties so that everyone (even those of a non-technical background) can understand the basic principles to which they work,*

V. ***Diversity non-discrimination and fairness**: An AI system is only as good as the data it uses to learn. If the data fed to the system is inherently biased or not representative then the AI system will make biased and discriminatory decisions. It is therefore necessary to have controls on the quality of the data used,*

VI. ***Societal and environmental wellbeing**: AI systems should be used to benefit society as a whole rather than individuals. In addition, sustainability and ecological impact should be taken into account when developing AI systems, and*

VII. ***Accountability**: If an AI system malfunctions and potentially causes harm then it should be possible to trace the manufacturers of the AI system to bring them to justice. This is a difficult task because there are many parties involved in the creation of AI systems from the beginning to the end of the supply chain. AI systems should be traceable and should be audited at each stage of the supply chain in order to ensure their compliance."*

The EC moreover elaborates on specific requirements for certain AI applications such as "those used for purposes of (remote) biometric identification", however, the latter has been criticized, because the requirements are weaker than the ones suggested in a previous version of the paper which suggested a moratorium on facial recognition in public spaces for five years.[1295] The EC was also criticized for the

[1294] Bold means emphasis added.

[1295] Angela Chen: The EU just released weakened guidelines for regulating Artificial Intelligence. Article published February 19 2020, available at https://www.technologyreview.com/2020/02/19/876455/european-union-artificial-intelligence-regulation-facial-recognition-privacy/. Retrieved October 15, 2021.

fact that the paper’s AI guidelines only address high-risk technologies (e.g. biometrics, surveillance) or certain industries (e.g. energy) but not consumer-relevant (e.g. advertising) technology.[1296]

6.2.3.2. Declaration on European Digital Rights and Principles

In late 2022, the European Commission, European Parliament and the Council of the European Union reached a political agreement on the European declaration on digital rights and principles.[1297] The declaration aims to set out the EU approach to the digital transformation to foster growth, prosperity, competitiveness as well as security and societal well-being, and the declaration furthermore aims at complementing existing rights under the General Data Protection Regulation or the Charter of Fundamental Rights and underlines the importance of freedom of choice in interactions with algorithms and AI systems to ensure a “fair digital environment” by putting people at the center.[1298] The six principles contained in the declaration are:[1299] putting people and their rights at the centre of the digital transformation; supporting solidarity and inclusion; ensuring freedom of choice online; fostering participation in the digital public space; increasing safety, security and empowerment of individuals; promoting the sustainability of the digital future.

6.2.4. HUMANE AI Net

Together with a network of more than 50 academic and industrial partners, the European Commission launched HUMANE AI Net to facilitate “a European brand of trustworthy, ethical AI that enhances Human capabilities and empowers citizens and society to effectively deal with the challenges of an interconnected globalized world.”[1300] The initiative originated in Germany at the German Research Center for Artificial Intelligence[1301] and engages in numerous micro projects such as Defining AI for regulatory and policy purposes, Algorithmic Bias, Strategies for Adaptive User Interfaces or Ethical

[1296] Mark MacCarthy, Kenneth Propp: The EU’s White Paper on AI: a thoughtful and balanced way forward. Article published March 5 2020, available at https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward. Retrieved October 15, 2021.

[1297] The text of the European Declaration on Digital Rights and Principles is available at https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles. Retrieved December 29, 2022.

[1298] European Commission press release: Commission puts forward declaration on digital rights and principles for everyone in the EU. Press release published January 26 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_452. Retrieved December 29, 2022.

[1299] Background information on the European Declaration on Digital Rights and Principles is provided by the European Commission on their website, available at https://data.europa.eu/en/news-events/news/european-declaration-digital-rights-and-principles#:~:text=The%20six%20principles%20contained%20in%20the%20declaration%20are%3A,6%20Promoting%20the%20sustainability%20of%20the%20digital%20future. Retrieved December 29, 2022.

[1300] Background information on the HUMANE AI Net is available at https://www.humane-ai.eu/. Retrieved October 15, 2021.

[1301] Background information on the German Research Center for Artificial Intelligence is available at https://www.dfki.de/en/web/. Retrieved October 15, 2021.

Chat-Bots and published a series of reports on reports on human-centered AI, including a research roadmap[1302] and policy recommendations.[1303] HUMANE AI Net's research agenda for human-centered AI is built on 5 pillars: societal awareness; legal and ethical bases for responsible AI; human-AI collaboration and interaction; multimodal perception and modeling as well as human-in-the-loop Machine Learning, reasoning, and planning.[1304]

6.2.5. Council of Europe Commissioner for Human Rights recommendation

In 2019, the Council of Europe's Commissioner for Human Rights issued a recommendation[1305] which explains that "finding the right balance between technological development and human rights protection is an urgent matter" given the fact that AI-driven applications are nowadays part of everyday life. The document is aimed at Council of Europe (COE) Member States; however, the findings concern anyone dealing with the design, development, or implementation of AI. The document[1306] names the following ten steps to protect human rights and unbox Artificial Intelligence:

I. *"**Human rights impact assessment**,*

II. ***Public consultation**,*

III. ***Obligation of Member States to facilitate the implementation of human rights standards in the private sector**,*

IV. ***Information and transparency**,*

V. ***Independent oversight**,*

VI. ***Non-discrimination and equality**,*

VII. ***Data protection and privacy**,*

VIII. ***Freedom of expression, assembly and association**, and the **right to work***

IX. ***Remedies**,*

X. ***Promotion of AI-literacy**."*

[1302] Details on HUMANE AI: Toward AI systems that augment and empower humans by understanding us, our society, and the world around us are available at https://www.humane-ai.eu/wp-content/uploads/2020/01/D4.1-v3.pdf. Retrieved October 15, 2021.

[1303] HUMANE AI's policy recommendations are available at https://www.humane-ai.eu/wp-content/uploads/2019/11/D21-HumaneAI-Concept.pdf. Retrieved October 15, 2021.

[1304] Detailed information on HUMANE AI's research agenda is available at https://www.humane-ai.eu/research-roadmap/. Retrieved October 15, 2021.

[1305] The Council of Europe's Commissioner for Human Rights recommendation: Unboxing Artificial Intelligence – 10 steps to protect human rights. Recommendation published May 2019, available at https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64. Retrieved October 15, 2021.

[1306] The document includes a checklist with "Dos" and "Don'ts" with actions for each key area to serve as guidance when it comes to operationalizing recommendations.

It is important that the Council of Europe Commissioner for Human Rights recommendation stresses human rights impact assessments, because we are at a turning point for the future of algorithmic accountability: HRIAs are a core element of many recommendations in the frameworks of ongoing AI regulatory debates, including regulatory proposals in many jurisdictions, but even though there is consensus that human rights impact assessments could be good algorithmic governance mechanism, there is no standardized process for conducting such assessments that can be considered truly accountable.[1307]

6.2.6. Council of Europe recommendations

6.2.6.1. Recommendation for a Convention on AI, Human Rights, Democracy, and the Rule of Law

In August 2022, the European Commission issued its recommendation[1308] for a Council Decision Authorizing the Opening of Negotiations on behalf of the European Union for a Council of Europe Convention on Artificial Intelligence (AI), Human Rights, Democracy, and the Rule of Law. The recommendation notes that there is a very significant overlap between the future CoE convention on AI and the proposed AI Act in terms of scope, nature, and content. Consequently, the recommendation underlines the importance of further negotiations in such a way as to ensure the consistency and uniformity of (future) EU rules for AI. The European Data Protection Supervisor believes that the Convention is an important opportunity to complement the European Commission's proposed Artificial Intelligence Act and that this initiative is an "opportunity to develop the first legally binding international instrument on Artificial Intelligence according to EU standards and values on human rights, democracy and the rule of law."[1309] However, the EDPS also made the following key recommendations on the EU's negotiating directives for the Convention:[1310] The EDPS is of the opinion that AI systems that pose unacceptable risks to individuals should be prohibited by default, for example, AI systems that

[1307] European Center for Non-For-Profit-Law: Recommendations for assessing AI impacts to human rights, democracy, and the rule of law. Paper published November 2021, available at https://ecnl.org/publications/recommendations-incorporating-human-rights-ai-impact-assessments. Retrieved December 30, 2022.

[1308] Recommendation for a Council Decision authorizing the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law published August 18 2022, available https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0414.

[1309] Statement by Wojciech Wiewiórowski, European Data Protection Supervisor, provided in the framework of the EDPS press release: AI Convention – stronger protection of fundamental rights is necessary. Statement published October 14 2022, available at https://edps.europa.eu/press-publications/press-news/press-releases/2022/ai-convention-stronger-protection-fundamental-rights-necessary_en. Retrieved December 31, 2022.

[1310] European Data Protection Supervisor Opinion 20/2022 on the recommendation for a Council decision authorizing the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law. Opinion published October 13 2022, available at https://edps.europa.eu/press-publications/press-news/press-releases/2022/ai-convention-stronger-protection-fundamental-rights-necessary_en. Retrieved December 31, 2022.

affect individuals' rights to human dignity, social scoring, biometric identification of individuals in public spaces, or the categorization of individuals based on biometric data (e.g., ethnicity) or according to their perceived emotions. On top of these conditions that shall be explicitly applied in the negotiating directives, the EDPS furthermore recommends the monitoring of AI systems, and the introduction of procedural safeguards to ensure that AI systems are transparent in the sense of clear explicability to both, regulators and individuals, and that they can be audited regularly to limit risks that such tools may present to protect individuals that may be affected by the use of AI systems.

6.2.6.2. Recommendations on Human Rights Impacts of Algorithmic Systems

The Council of Europe, the leading international organization for the protection of human rights as set forth in the European Convention on Human Rights[1311] issued guidelines on how COE Member States – currently 47 out of which 27 are EU Member States – should legislate to make sure that human rights are addressed when Artificial Intelligence is used.[1312] COE's recommendations are similar to HLEG's Ethics Guidelines for Trustworthy AI, but the interesting thing about COE's recommendations is that two sets of guidelines have been issued, one for the private sector which may serve for orientation purposes in the sense of best practices, and one for the public sector that could potentially serve as guidance for future legislation. COE's guidelines on addressing the human rights impacts of algorithmic systems name the following general principles (obligations) for states with respect to the protection and promotion of human rights and fundamental freedoms in the context of algorithmic systems:[1313]

I. *"**Research, innovation, public awareness**[1314] (including rights-promoting technology, human-centric and sustainable innovation as well as independent research),*

II. ***Precautionary measures** (including impact assessments, staff management and interaction of systems / integrations),*

III. ***Legislation** (including ongoing review, democratic participation and awareness, institutional framework),*

IV. ***Transparency, accountability, and effective remedies** (including contestability, oversight),*

V. ***Data management** (including informational self-determination, infrastructure),*

VI. ***Analysis and modelling** (including safeguards, evaluation, testing)."*

[1311] Further background information on the Council of Europe is available at the Council's website https://www.coe.int/en/web/about-us. Retrieved October 15, 2021.

[1312] Council of Europe's recommendation on the human rights impacts of algorithmic systems adopted April 8 2020, and is available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154. Retrieved October 15, 2021.

[1313] COE's guidelines on addressing the human rights impacts of algorithmic systems published April 8 2020, available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154. Retrieved October 15, 2021.

[1314] Bold means emphasis added.

Private sector actors shall consider with the following general principles in order to comply with human rights and fundamental freedoms in the context of algorithmic systems:

I. ***"Transparency, accountability, and effective remedies****,*
II. ***Appropriate privacy settings and consent rules****,*
III. ***Responsibility to respect human rights****,*
IV. ***Contestability and effective remedies****,*
V. ***Avoidance of discrimination****,*
VI. ***Data quality and security****."*

6.2.6.3. Human Rights, Democracy and Rule of Law Impact Assessment / Framework

The Council of Europe's Ad Hoc Committee on Artificial Intelligence (CAHAI)[1315] also proposed to introduce a non-binding mechanism to allow for a "Human Rights, Democracy and Rule of Law Impact Assessment" (HUDERIA) with the following main elements:[1316]

I. ***"Risk Identification****: Identification of relevant risks for human rights, democracy and the rule of law;*
II. ***Impact Assessment****: Assessment of the impact, taking into account the likelihood and severity of the effects on those rights and principles;*
III. ***Governance Assessment****: Assessment of the roles and responsibilities of duty-bearers, rights holders and stakeholders in implementing and governing the mechanisms to mitigate the impact;*
IV. ***Mitigation and Evaluation****: Identification of suitable mitigation measures and ensuring a continuous evaluation."*

The Human Rights, Democracy and Rule of Law Impact Assessment was not the only topic CAHAI had been working on; its policy and development group was also working on a "Rights, Democracy, and the "Rule of Law Assurance Framework for AI Systems" (HUDERAF), which "combines the procedural requirements for principles-based human rights due diligence with the governance mechanisms needed to set up technical and socio-technical guardrails for responsible and trustworthy AI innovation practices. Its purpose is to provide an accessible and user-friendly set of mechanisms for facilitating compliance with a binding legal framework for Artificial Intelligence, based on the Council of Europe's standards on human rights, democracy, and the rule of law, and to ensure that AI innovation

[1315] The CAHAI fulfilled its mandate (2019-2021) and has been succeeded by the Committee on Artificial Intelligence (CAI), see https://www.coe.int/en/web/artificial-intelligence/cahai-1. Retrieved July 25 2022.
[1316] Marten Breuer: The Council of Europe as an AI standard setter. Article published April 4 2022, available at https://verfassungsblog.de/the-council-of-europe-as-an-ai-standard-setter/. Retrieved July 25 2022.

projects are carried out with appropriate levels of public accountability, transparency, and democratic governance."[1317] HUDERAF encompasses four interrelated elements: a preliminary context-based risk analysis, the stakeholder engagement process, the HUDERIA and finally, a "Human Rights, Democracy, and Rule of Law Assurance Case" (HUDERAC) which "enables AI project teams to build a structured argument that provides demonstrable assurance to stakeholders that claims about the attainment of goals established in the HUDERIA and other HUDERAF governance processes are warranted given available evidence."[1318]

6.2.7. European Parliament's resolutions and initiatives

6.2.7.1. Resolution on Civil Law Rules on Robotics

The European Parliament's Legal Affairs Committee dealt with issues surrounding the liability in robotics and published a study to evaluate and analyze a number of future European civil law rules in robotics[1319] from a legal and ethical perspective. EP furthermore issued a resolution on Civil Law Rules on Robotics[1320] which deals, amongst other things, with protecting humans against the risk of harm and manipulation by robots and discusses the establishment of a mandatory insurance scheme for specific categories of robots as well as the creation of a general fund for all intelligent autonomous robots or an individual fund for each category and the establishment of a specific legal status for robots, so that autonomous robots are responsible for any damage they cause.[1321] The European Parliament suggests that robots should not be given a legal personality, even if robots interact with third parties independently.[1322] The European Parliament continued its work and issued three further resolutions:

[1317] David Leslie, Christopher Burr, Mhairi Aitken, Michael Katell, Morgan Briggs, Cami Rincon: Human rights, democracy, and the rule of law assurance framework for AI systems: a proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence. Paper published June 2022, available at https://doi.org/10.5281/zenodo.5981676. Retrieved December 31, 2022.

[1318] David Leslie et al: Human rights, democracy, and the rule of law assurance framework for AI systems: a proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence. Paper published June 2022, available at https://doi.org/10.5281/zenodo.5981676. Retrieved December 31, 2022.

[1319] European Civil Law Rules on Robotics published 2016, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf. Retrieved October 15, 2021.

[1320] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), available at https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. Retrieved October 15, 2021.

[1321] Background information is provided by omitech robot in their blog post "Civil law rules on Robotics: the resolution of the European Union", available at https://robot.omitech.it/en/civil-law-rules-on-robotics-the-resolution-of-the-european-union/. Retrieved October 15, 2021.

[1322] European Parliament: European Civil Law Rules on Robotics. Rules published 2017, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf. Retrieved October 15, 2021.

6.2.7.2. Resolution on a Civil Liability Regime for AI

The European Parliament issued a resolution on a civil AI liability to address key issues like insurances, operator liability and different liability rules for different risks: the European Parliament suggested that those operating high-risk AI should be strictly liable for any resulting damage, material and immaterial harm.[1323] The EP called for a harmonized legal framework for civil liability claims to prevent potential misuses of AI-systems[1324] and the European Parliament also dealt with the issue of Artificial intelligence and civil law liability rules for drones.[1325] Another factor to consider is the fact that the Product Liability Directive has been in place for almost 40 years now, meaning that new challenges arising from AI may not be properly reflected. While the European Commission expressed its belief that the Directive is still fit for purpose,[1326] a new proposal for product liability has been published to address such issues.[1327]

6.2.7.3. Resolution on Intellectual Property Rights

The European Parliament moreover published a resolution on intellectual property rights:[1328] the EP highlighted the benefits of AI development, and given key importance of these rights, the EP stressed the need for a common AI legislation to avoid massive litigation and called on the Commission to carry out an impact assessment regarding the protection of intellectual property rights in the context of AI and related technologies. Furthermore, the European Parliament once more underlined its position that robots or AI technologies should not have legal personality and that only humans have the ownership of intellectual property rights.

[1323] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for Artificial Intelligence (2020/2014(INL), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html. Retrieved October 15, 2021.

[1324] European Parliament Research Service: What is the European Parliament's position on Artificial Intelligence? Blog entry published November 23 2020, available at https://epthinktank.eu/2020/11/23/what-is-the-european-parliaments-position-on-artificial-intelligence/.

[1325] Artificial Intelligence and civil law: liability rules for drones. Paper published November 2018, available at https://op.europa.eu/en/publication-detail/-/publication/b4b77a1e-1554-11e9-81b4-01aa75ed71a1/language-en/format-PDF/source-search. Retrieved October 15, 2021.

[1326] Report on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) published May 7 2018, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525769201372&uri=COM:2018:246:FIN. Retrieved October 15, 2021.

[1327] James Gallagher, Amy Grant: The proposal for a revised EU Product Liability Directive. Article published October 12 2022, available at https://www.mhc.ie/latest/insights/the-proposal-for-a-revised-eu-product-liability-directive#:~:text=The%20Proposal%20has%20several%20stated%20aims%3A%201%20To,on%20making%20claims%20where%20appropriate%2C%20and%20Weitere%20Elemente. Retrieved January 4, 2023.

[1328] European Parliament resolution on intellectual property rights for the development of Artificial Intelligence technologies (2020/2015(INI) published 20 October 2020, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html. Retrieved October 15, 2021.

6.2.7.4. Resolution on Ethical Aspects of Artificial Intelligence

The European Parliament also issued a resolution on the ethical aspects of AI and provided recommendations about the ethics needed in the framework of Artificial Intelligence:[1329] the EP stressed that AI shall be tailored to human needs, values-based and built on safety, transparency as well as accountability and tailored to human needs and shall provide for privacy, sustainability, social responsibility as well as non-discrimination and workers' rights so that AI is always at the service of humans.

6.2.7.5. Special Committee on Artificial Intelligence in the digital age

Last, but not least, the EP established a special committee on Artificial Intelligence in 2020 called AIDA with the goal of setting out a long-term EU roadmap on AI to "study the impact and challenges of rolling out AI, identify common EU-wide objectives, and propose recommendations on the best ways forward."[1330] AIDA's 12-month mandate will pursue a horizontal approach, take third-country approaches to AI into consideration, organize stakeholder workshops and summarize their findings and recommendations in a final report.

6.3. Intergovernmental cooperation

Apart from EU's High level Expert Group on Artificial Intelligence (HLEG)[1331] that delivered Ethics Guidelines for trustworthy AI and UNESCO's Ad Hoc Expert Group (AHEG)[1332] which published a recommendation on the ethics of artificial intelligence, there are further intergovernmental activities that are worthwhile mentioning: OECD's Network of Experts on AI (ONE AI)[1333] which launched the OECD

[1329] European Parliament resolution with recommendations to the Commission on a framework of ethical aspects of Artificial Intelligence, robotics and related technologies (2020/2012(INL) published 20 October 2020, available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html#:~:text=European%20Parliament%20resolution%20of%2020%20October%202020%20with,artificial%20intelligence%2C%20robotics%20and%20related%20technologies%20%282020%2F2012%20%28INL%29%29. Retrieved October 15, 2021.

[1330] Background information on the initiative is available at the European Parliament's website at https://www.europarl.europa.eu/committees/en/aida/about. Retrieved October 15, 2021.

[1331] Further details on HLEG's deliverables are available at the Commission's website https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai. Retrieved October 15, 2021.

[1332] Background information on UNESCO's international expert group to draft global recommendation on the ethics of AI is available at https://en.unesco.org/news/unesco-appoints-international-expert-group-draft-global-recommendation-ethics-ai. Retrieved October 15, 2021.

[1333] Further details on OECD's Network of Experts on AI are available at https://oecd.ai/en/wonk/oecd-network-ai-experts-cooperation-for-trustworthy-beneficial-ai#:~:text=ONE%20AI%20is%20an%20informal%20advisory%20group%20tasked,sector,%20trade%20unions,%20the%20technical%20community,%20and%20academia. Retrieved October 15, 2021.

AI Policy Observatory[1334] and is working on the classification of AI to provide a framework for assessing and classifying AI systems according to their impact.[1335] The Global Partnership on AI (GPAI) was founded by 15 countries from all over the globe to "bring together engaged minds and expertise from science, industry, civil society, governments, international organizations and academia to foster international cooperation".[1336] In summary, HLEG's and AHEG's focus area is AI Ethics, ONE AI's focus is AI classification, whereas GPAI is also concerned with responsible AI and the future of work.

6.4. Expert Guidelines, civil society and multistakeholder recommendations

6.4.1. Universal Guidelines for Artificial Intelligence

The Universal Guidelines for Artificial Intelligence (UGAI)[1337] have been announced at the 2018 International Data Protection and Privacy Commissioners Conference: more than 150 experts and 40 non-governmental organizations representing 30 countries around the world endorsed the guidelines which some consider a "landmark policy"[1338] – for good reason: apart from much-repeated provisions like accountability, transparency and fairness, those guidelines follow a comprehensive approach to protect individuals' rights, and they contain more far-reaching obligations, ranging from existing (but neglected) principles like data quality and accuracy to new requirements like the prohibition of secret profiling and national scoring, making the true operators of an AI system known and a termination obligation when an institution loses control of an AI system. The UGAI require the following:

I. *"**Right to transparency**:[1339] all individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome.*

II. ***Right to human determination**: all individuals have the right to a final determination made by a person.*

[1334] Background information on OECD's AI Policy Observatory is available at https://oecd.ai/about/#:~:text=The%20OECD%20AI%20Policy%20Observatory%20%28OECD.AI%29%20builds%20on,basis%20for%20the%20G20%20AI%20Principles%20endorsed%20. Retrieved October 15, 2021.

[1335] Further details on OECD's Working Party on Artificial Intelligence Governance (AIGO) including their publications are available at https://oecd.ai/network-of-experts/#:~:text=The%20upcoming%20OECD%20AI%20Systems%20Classification%20Framework%20provides,and%20technologies%3B%20labour%20and%20skills%3B%20and%20international%20cooperation. Retrieved October 15, 2021.

[1336] Background information on the Global Partnership on AI is available at https://www.gpai.ai/. Retrieved October 15, 2021.

[1337] The Universal Guidelines for Artificial Intelligence are available at https://thepublicvoice.org/AI-universal-guidelines/. Retrieved October 15, 2021.

[1338] Candace Paul: Universal Guidelines for Artificial Intelligence Announced in Brussels. Article published October 23 2018, available at https://blog.epic.org/2018/10/23/universal-guidelines-artificial-intelligence-announced-brussels/. Retrieved October 15, 2021.

[1339] Bold means emphasis added.

III. ***Identification obligation**: the institution responsible for an AI system must be made known to the public.*

IV. ***Fairness obligation**: institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions.*

V. ***Assessment and accountability obligation**: an AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.*

VI. ***Accuracy, reliability, and validity obligations**: institutions must ensure the accuracy, reliability, and validity of decisions.*

VII. ***Data quality obligation**: institutions must establish data provenance, and assure quality and relevance for the data input into algorithms.*

VIII. ***Public safety obligation**: institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.*

IX. ***Cyber-security obligation**: institutions must secure AI systems against cybersecurity threats.*

X. ***Prohibition on secret profiling**: no institution shall establish or maintain a secret profiling system.*

XI. ***Prohibition on unitary scoring**: no national government shall establish or maintain a general-purpose score on its citizens or residents.*

XII. ***Termination obligation**: an institution that has established an AI system has an affirmative obligation to terminate the system if human control of the system is no longer possible."*

6.4.2. Future of Life Institute: Asilomar AI Principles

The Future of Life Institute hosted a conference in 2017 where numerous researchers and thought leaders in law, economics, ethics as well as philosophy met to discuss beneficial Artificial Intelligence.[1340] The following twenty-three principles, called the AI Asilomar Principles, have been developed during the meeting:

***"Research Issues**[1341]*

I. ***Research Goal**: The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.*

[1340] Background information on the Asilomar AI Principles is available at the Future of Life's website, available at https://futureoflife.org/ai-principles/. Retrieved October 15, 2021.

[1341] Bold means emphasis added.

II. ***Research Funding**: Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:*
   - *How can we make future AI systems highly robust, so that they do what we want without malfunctioning or getting hacked?*
   - *How can we grow our prosperity through automation while maintaining people's resources and purpose?*
   - *How can we update our legal systems to be fairer and more efficient, to keep pace with AI, and to manage the risks associated with AI?*
   - *What set of values should AI be aligned with, and what legal and ethical status should it have?*

III. ***Science-Policy Link**: There should be constructive and healthy exchange between AI researchers and policy makers.*

IV. ***Research Culture**: A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.*

V. ***Race Avoidance**: Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.*

Ethics and Values

VI. ***Safety**: AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.*

VII. ***Failure Transparency**: If an AI system causes harm, it should be possible to ascertain why.*

VIII. ***Judicial Transparency**: Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.*

IX. ***Responsibility**: Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.*

X. ***Value Alignment**: Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.*

XI. ***Human Values**: AI systems should be designed and operated be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.*

XII. ***Personal Privacy**: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.*

XIII. ***Liberty and Privacy**: The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.*

XIV. ***Shared Benefit**: AI technologies should benefit and empower as many people as possible.*

XV. ***Shared Prosperity**: The economic prosperity created by AI should be shared broadly, to benefit all of humanity.*

XVI. ***Human Control**: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.*

XVII. ***Non-subversion**: The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.*

XVIII. ***AI Arms Race**: An arms race in lethal autonomous weapons should be avoided.*

Longer-term Issues

XIX. ***Capability Caution**: There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.*

XX. ***Importance**: Advanced AI could represent a profound change in the history of life on Earth and should be planned for and managed with commensurate care and resources.*

XXI. ***Risks**: Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.*

XXII. ***Recursive Self-Improvement**: AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.*

XXIII. ***Common Good**: Super-intelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization."*

6.4.3. ACM's Statement on Algorithmic Transparency and Accountability

In 2017, the Association for Computing Machinery (ACM) issued a statement on Algorithmic Transparency and Accountability[1342] which included seven principles designed to be consistent with ACM's Code of Ethics[1343] and to address potential harmful bias[1344] the use of AI may involve:

[1342] ACM statement on Algorithmic Transparency and Accountability published January 12 2017, available at https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf. Retrieved October 15, 2021.

[1343] ACM's Code of Ethics pulished in 2018, available at https://ethics.acm.org/. Retrieved October 15, 2021.

[1344] Renee Dopplick: New Statement on Algorithmic Transparency and Accountability by ACM U.S. Public Policy Council. Article published January 14 2017, available at https://techpolicy.acm.org/2017/01/new-statement-on-algorithmic-transparency-and-accountability-by-acm-u-s-public-policy-council/. Retrieved October 15, 2021.

I. *"**Awareness**:*[1345] *Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.*

II. ***Access and redress**: Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.*

III. ***Accountability**: Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.*

IV. ***Explanation**: Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.*

V. ***Data Provenance**: A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.*

VI. ***Auditability**: Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.*

VII. ***Validation and Testing**: Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public."*

6.4.4. The Toronto Declaration

The so-called Toronto Declaration[1346] was announced by coalition of digital and human rights groups, including e.g., Human Rights Watch and Amnesty International. The declaration was the outcome of the RightsCon conference and, unlike many other guidelines and statements that discussed ethical aspects of Artificial Intelligence, the Toronto Declaration aims at embedding basic principles of equality and non-discrimination in Machine Learning.[1347] It named 59 topics and action points altogether that

[1345] Bold means emphasis added.

[1346] Toronto Declaration published May 16 2018, available at https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf. Retrieved October 15, 2021.

[1347] Russell Brandom: New Toronto Declaration calls on algorithms to respect human rights. Article published May 16 2018, available at https://www.theverge.com/2018/5/16/17361356/toronto-declaration-machine-learning-algorithmic-discrimination-rightscon. Retrieved October 15, 2021.

emphasizes the importance of not only transparency and accountability, but also the necessity of human oversight and the right to effective remedy and above all, the right to equality and non-discrimination which means that whenever AI is applied, risks and potential discriminatory outcomes have to be considered so that human rights are respected. Given that algorithms advance in capability and increase in use in nearly all aspects of life,[1348] from employment and education to policing and criminal justice, AI and Machine Learning may impact a variety of human rights such as the right to privacy, the freedom of expression, participation in cultural life, the right to remedy and the right to life,[1349] the Toronto declaration therefore demands that states have the obligation to promote, protect and respect human rights and that private sector actors have a responsibility to respect human rights.

6.4.5. Montreal declaration for a responsible development of Artificial Intelligence

The Montreal Declaration was announced at the conclusion of the 2017 Forum on socially responsible development of AI held in Montreal and aims to promote public debate and "encourage a progressive and inclusive orientation to the development of Artificial Intelligence".[1350] The Montreal Declaration for responsible AI development has three main objectives: to provide an open forum for discussion for AI to achieve equitable, inclusive, and ecologically sustainable AI, to foster the development of an ethical framework for AI, and to provide guidance for this major digital transition for the benefit of all by applying the following basic principles:

I. ***Well-being principle***:[1351] *the development and use of artificial intelligence systems (AIS) must permit the growth of the well-being of all sentient beings.*

II. ***Respect for autonomy principle****: AIS must be developed and used while respecting people's autonomy, and with the goal of increasing people's control over their lives and their surroundings.*

III. ***Protection of privacy and intimacy****: Privacy and intimacy must be protected from AIS intrusion and data acquisition and archiving systems (DAAS).*

IV. ***Solidarity principle****: The development of AIS must be compatible with maintaining the bonds of solidarity among people and generations.*

[1348] Further details are provided in the preamble of the Toronto Declaration, available at https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf. Retrieved October 15, 2021.

[1349] Human Rights Watch: The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems. Blog entry published July 3 2018, available at https://www.hrw.org/news/2018/07/03/toronto-declaration-protecting-rights-equality-and-non-discrimination-machine#. Retrieved October 15, 2021.

[1350] Montreal Declaration published 2018, available at https://www.montrealdeclaration-responsibleai.com/the-declaration. Retrieved October 15, 2021.

[1351] Bold means emphasis added.

V. ***Democratic participation principle**: AIS must meet intelligibility, justifiability, and accessibility criteria, and must be subjected to democratic scrutiny, debate, and control.*

VI. ***Equity principle**: The development and use of AIS must contribute to the creation of a just and equitable society.*

VII. ***Diversity and inclusion principle**: The development and use of AIS must be compatible with maintaining social and cultural diversity and must not restrict the scope of lifestyle choices or personal experiences.*

VIII. ***Prudence principle**: The development and use of AIS must be compatible with maintaining social and cultural diversity and must not restrict the scope of lifestyle choices or personal experiences.*

IX. ***Responsibility principle**: The development and use of AIS must not contribute to lessening the responsibility of human beings when decisions must be made.*

X. ***Sustainable development principle**: The development and use of AIS must be carried out so as to ensure a strong environmental sustainability of the planet."*

6.4.6. FAT/ML's Principles for Accountable Algorithms

Fairness, Accountability, and Transparency in Machine Learning (FAT/ML) is an initiative that brings together "a growing community of researchers and practitioners concerned with fairness, accountability, and transparency in Machine Learning".[1352] FAT/ML discusses the idea that bias might inadvertently be encoded into automated decisions if the complexity of Machine Learning either reduces or replaces the needed justification for AI decisions to "the algorithm made me do it".[1353] FAT/ML is engaged in a series of projects and organizes events that deal with various aspects that have to be obeyed when AI is applied such as Machine Learning and the law, algorithmic bias, explicability of AI decisions or privacy-aware data mining.[1354] FAT/ML also issued Principles for Accountable Algorithms, and they do not simply conclude with these principles, but furthermore provide a "Social Impact Statement for Algorithms" which shall serve as a guiding structure and which shall be used and revisited during all phases of the development process, i.e. design stage, pre-launch and post-launch to stress that only a repeated examination of the requirements ensures adherence to these principles. The Social Impact Statement should (at least) address their corresponding questionnaire that refers to specific steps that can be taken to address the requirements outlined in their principles. For transparency purposes, they

[1352] This includes representatives from Microsoft, Google, and universities.

[1353] Background information on the Fairness, Accountability, and Transparency in Machine Learning initiative is available at their website https://www.fatml.org/. Retrieved October 15, 2021.

[1354] Details on FAT/ML's areas of work are available at https://www.fatml.org/resources/relevant-events. Retrieved October 15, 2021.

propose that the statement shall be published so that the public can voice expectations for social impact of the system. FAT/ML's Principles for Accountable Algorithms[1355] read as follows:

I. *"**Responsibility**:[1356] Make available externally visible avenues of redress for adverse individual or societal effects of an algorithmic decision system, and designate an internal role for the person who is responsible for the timely remedy of such issues.*

II. ***Explainability**: Ensure that algorithmic decisions as well as any data driving those decisions can be explained to end-users and other stakeholders in non-technical terms.*

III. ***Accuracy**: Identify, log, and articulate sources of error and uncertainty throughout the algorithm and its data sources so that expected and worst-case implications can be understood and inform mitigation procedures.*

IV. ***Auditability**: Enable interested third parties to probe, understand, and review the behavior of the algorithm through disclosure of information that enables monitoring, checking, or criticism, including through provision of detailed documentation, technically suitable APIs, and permissive terms of use.*

V. ***Fairness**: Ensure that algorithmic decisions do not create discriminatory or unjust impacts when comparing across different demographics (e.g., race, sex, etc.)."*

6.4.7. IAF's Fair Processing Principles and Fair and Open Use Act

The Information Accountability Foundation (IAF) is a global information policy think tank that focuses on "effective information governance systems to facilitate information-driven innovation respectful of people's fundamental right to fair processing".[1357] Despite the fact that IAF's Fair Processing Principles[1358] have not been written to specifically address Big Data activities or Artificial Intelligence applications, the document is valuable guidance in the area of AI as it addresses key issues of innovative technology. IAF lists the following key elements needed to ensure data is processed and used in a legitimate and responsible manner:

"Individual Rights

I. ***Transparency**,*

II. ***Beneficial purposes**,*

[1355] See FAT/ML's Principles for Accountable Algorithms, available at https://www.fatml.org/resources/principles-for-accountable-algorithms. Retrieved October 15, 2021.

[1356] Bold means emphasis added.

[1357] Background information on the Information Accountability Foundation is available at https://informationaccountability.org/. Retrieved October 15, 2021.

[1358] IAF's Fair Processing Principles published on January 1 2019, available at https://informationaccountability.org/publications/. Retrieved October 15, 2021.

III. ***Access and redress**,*

IV. ***Engagement and appropriate control**.*

Accountable Data Stewardship

V. ***Assessed and mitigated impacts**,*

VI. ***Legitimate and contextual uses**,*

VII. ***Onward responsibility**,*

VIII. ***Remediation**,*

IX. ***Oversight**,*

X. ***Security**."*

The Information Accountability Foundation moreover issued the Fair and Open Use Act[1359] which is a model for privacy legislation that focuses on fair processing: IAF stresses that lessons learned from GDPR and other privacy legislation show that it is "time to place the onus on the organization to first and foremost achieve fair processing rather than placing the burden on the consumer."[1360] IAF's model legislation is based on risk assessment to capture and control potentially bad outcomes and stresses the importance of effective information governance; it wants to break the paradigm that legacy systems placed on the individual instead of organizational responsibility, consequently, IAF's model legislation flips that order[1361] since "the old privacy paradigm that individual control is the keystone for effective fair processing is no longer fit for its purpose."[1362] IAF is convinced that legislation should target risks, and not stick to (the exercise of) individual's rights, because organizations that get value from data must also be responsible stewards of that data:[1363] IAF builds on the FCRA's concept of permissible purpose and requires that personal data only be processed for specific legitimate uses. IAF presents the following eleven legitimate uses:[1364] advertising or marketing purposes (subject to conditions), compliance with a

[1359] IAF's Fair and Open Use Act published May 25 2021, available at https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2021/05/FAIR-and-OPEN-USE-Act-May-26-2021-1.pdf?time=1623678345. Retrieved October 15, 2021.

[1360] Background information on the Fair and Open Use Act is provided by Martin Abrams: 50 year heritage of the Fair and Open Use Act. Article published June 24 2021, available at https://informationaccountability.org/2021/06/50-year-heritage-of-the-fair-and-open-use-act/. Retrieved October 15, 2021.

[1361] Martin Abrams: Time to break the privacy legislative paradigm – IAF Model Legislation. Article published June 3 2021, available at https://informationaccountability.org/2021/06/time-to-break-the-privacy-legislative-paradigm-iaf-model-legislation/. Retrieved October 15, 2021.

[1362] Julie Cohen: How (not) to write a privacy law – disrupting surveillance-based business models requires government innovation. Article published March 23 2021, available at https://knightcolumbia.org/content/how-not-to-write-a-privacy-law. Retrieved October 15, 2021.

[1363] Martin Abrams, Marc Groman, Barb Lawler: Fair and Open Use Act – a demonstration of accountability-based legislation. Paper published May 27 2021.

[1364] Martin Abrams: 50 year heritage of the Fair and Open Use Act. Article published June 24 2021, available at https://informationaccountability.org/2021/06/50-year-heritage-of-the-fair-and-open-use-act/. Retrieved October 15, 2021.

legal obligation, protection against unlawful activity, requested product or service, affirmative express consent, routine business processes, public safety and health, knowledge discovery, information security, as well as journalism and research." On the one hand, this should provide for a "forward looking risk-based model legislation",[1365] on the other hand, it should also allow for innovation by enabling controllers to use data and knowledge they extract from information. Interestingly, IAF distinguishes between several types of data, but not in the traditional sense of sensitive and non-sensitive personal data, but depending on the source and origin of information, that is: personal data – provided data – observed data – inferred data – third party provided data. A similar categorization of data is contained in Microsoft's Online Services Data Processing Addendum[1366] which names the following types of data: "provided data" in the context of customer, support and professional services data; "collected or obtained data" is used for so-called diagnostic data, and "generated or derived data," which refers to service generated data. This distinction is not just a new perspective on types of information or data sets, but significant insofar as it may draw the line between (joint?) controllers.[1367] As a matter of fact, such a categorization seems to be needed, because it is naïve to believe that whatever an individual provides as information, this is not the basis of subsequent processing operations, but only the starting point: in many cases "customer provided data" is likely to be the smallest portion of information, be it in the banking sector where screenings against various sanction lists are mandatory for compliance reasons[1368] or in e-commerce where background checks for fraud prevention purposes are based on legitimate interests: the user thinks his shopping cart is about placing an order, the vendor knows it's where the individual risk profile is created, and depending on the circumstances, not only the user's preferred payment method may be rejected, but the individual as such may get sorted out.[1369] So far, the focus within privacy legislation seems to be predominantly on content-level information, i.e. data which are visible in the frontend but this information is certainly the smaller volume of data in comparison to what is going on in the backend, and it would be interesting to know what the real ratio between these types of data is.

[1365] Martin Abrams: Time to break the privacy legislative paradigm – IAF Model Legislation. Article published on June 3 2021, available at https://informationaccountability.org/2021/06/time-to-break-the-privacy-legislative-paradigm-iaf-model-legislation/. Retrieved October 15, 2021.

[1366] Microsoft's Online Services Data Processing Addendum is available at https://www.microsoft.com/licensing/docs/view/Online-Services-Data-Protection-Addendum-DPA#:~:text=Online%20Services%20Data%20Protection%20Addendum%20%28DPA%29%20When%20you,to%20the%20Product%20Terms%20site%20%28and%20formerly%20OST%29. Retrieved October 15, 2021.

[1367] The "Privacy Company" investigated potential privacy risks related to the use of Microsoft Windows 10 Enterprise, Office 365 ProPlus, and Office Online as well as the mobile Office apps on behalf of the Dutch Ministry of Justice and Security in 2019. Background information on their activities and the impact assessment are available at https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-long-blog. Retrieved October 15, 2021.

[1368] Ernst & Young: Effective screening controls for sanctions and AML risk management. Report published April 12 2018, available at https://www.ey.com/Publication/vwLUAssets/ey-effective-screening-controls-for-sanctions-and-aml-risk-management/$FILE/ey-effective-screening-controls-for-sanctions-and-aml-risk-management.pdf. Retrieved October 15, 2021.

[1369] Omer Tene: Privacy: For the rich or for the poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html. Retrieved October 15, 2021.

6.4.8. IEEE Ethically Aligned Design

The IEEE is a technical professional organization dedicated to the advancement of technology.[1370] Their “Global Initiative” deals with ethical considerations in Artificial Intelligence and autonomous systems (A/IS). Their comprehensive first edition of an Ethically Aligned Design (EAD)[1371] is based on three pillars: universal human values, political self-determination as well as data agency and technical dependability. The latter means that A/IS shall operate reliably and safely and deliver services that can be trusted. IEEE’s initiative is different insofar as it does not only name principles, but explains how to incorporate those principles in practice and how those values can be embedded into systems. IEEE identified the following general principles for autonomous and intelligent systems:

I. *“**Human Rights**:*[1372] *A/IS shall be created and operated to respect, promote, and protect internationally recognized human rights.*

II. ***Well-being**: A/IS creators shall adopt increased human well-being as a primary success criterion for development.*

III. ***Data Agency**: A/IS creators shall empower individuals with the ability to access and securely share their data, to maintain people’s capacity to have control over their identity.*

IV. ***Effectiveness**: A/IS creators and operators shall provide evidence of the effectiveness and fitness for purpose of A/IS.*

V. ***Transparency**: The basis of a particular A/IS decision should always be discoverable.*

VI. ***Accountability**: A/IS shall be created and operated to provide an unambiguous rationale for all decisions made.*

VII. ***Awareness of Misuse**: A/IS creators shall guard against all potential misuses and risks of A/IS in operation.*

VIII. ***Competence**: A/IS creators shall specify and operators shall adhere to the knowledge and skill required for safe and effective operation.”*

6.4.9. Women Leading in AI: 10 Principles for Responsible AI

Women Leading in AI intends to bring together female thinkers, scientists, academics, businesswomen and politicians to influence the future of AI tank of women leaders in AI. The network has been launched

[1370] Background information on the IEEE is available at their website https://www.ieee.org/. Retrieved October 15, 2021.

[1371] IEEE: Ethically aligned design – a vision for prioritizing human well-being with autonomous and intelligent systems. Paper published March 2019, available at https://engagestandards.ieee.org/rs/211-FYL-955/images/EAD1e.pdf?mkt_tok=eyJpIjoiWkRVME1UVm1OREE1TVRSbSIsInQiOiIxY3RONFl6YXh0cWxSRUpLNE9taUtwQllpaXNkYktmd3FDM2lOQ1ZNXC9YUURKV3Z4b2dJc3d3ekNDREdTd24zMHNcL0xUTEFqeFFoYTN4NWNqQUZRclY0amMyTzhXeU9VXC9yNjhneWlIeHFHV3lSMU1rRGxmeUJSTU9cL3dDeXZmN1AifQ%3D%3D. Retrieved October 15, 2021.

[1372] Bold means emphasis added.

in May 2018 at the London School of Economics and has a diverse membership from various backgrounds such as academia, computer programming, ethics, industry, law, politics, policy, privacy, or solutions architecture "giving us a critical mass of expertise that makes our voice listened to as the go-to people to talk about how AI impacts the real world."[1373] Women Leading in AI believe that AI must be accountable, governed, responsible, transparent, and their Whitepaper on responsible AI names the following ten core principles:[1374]

I. *"Establish an* ***AI regulatory function*** *working alongside the Information Commissioner's Office and Centre for Data Ethics – to audit algorithms, investigate complaints by individuals, issue notices and fines for breaches of GDPR and equality and human rights law, give wider guidance, spread best practice and ensure algorithms must be fully explained to users and open to public scrutiny.*

II. *Introduce a new '****Certificate of Fairness for AI systems'*** *alongside a 'kite mark' type scheme to display it. Criteria to be defined at industry level, similarly to food labelling regulations.*

III. *Introduce mandatory* ***AIAs (Algorithm Impact Assessments)*** *for organisations employing AI systems that have a significant effect on individuals.*

IV. *Introduce a mandatory requirement for* ***public sector organisations*** *using AI for particular purposes to* ***inform citizens*** *that decisions are made by machines, explain how the decision is reached and what would need to change for individuals to get a different outcome.*

V. *Introduce a* **'reduced liability*' incentive for companies*** *that have obtained a Certificate of Fairness to foster innovation and competitiveness.*

VI. *To compel companies and other organisations to* ***bring their workforce with them*** *– by publishing the impact of AI on their workforce and offering retraining programmes for employees whose jobs are being automated.*

VII. *Where no redeployment is possible, to compel companies to make a contribution towards a* ***digital skills fund*** *for those employees.*

VIII. *To carry out a* ***skills audit*** *to identify the wide range of skills required to embrace the AI revolution.*

IX. *To establish an* ***education and training programme*** *to meet the needs identified by the skills audit, including content on data ethics and social responsibility. As part of that, we recommend the set up of a solid, courageous and rigorous programme to* ***encourage young women and other underrepresented groups into technology****."*

[1373] Background information on Women Leading in AI, their work, and goals is available at https://womenleadinginai.org/about. Retrieved June 8, 2022.

[1374] Women Leading in AI: 10 principles for responsible AI. Paper published in 2019, available at https://womenleadinginai.org/report2019. Retrieved June 8, 2022.

On top of requirements that are part of most recommendations such as, mandatary audits, and / or impact assessments, transparency, and the need for a regulatory approach, this Whitepaper focuses on two interesting aspects, one from an employee (i.e., affected individual) and one from a company (i.e., controller) perspective: the latter refers to the idea of a reduced liability for those data controllers that have obtained a "Certificate of Fairness" to further develop a responsible AI sector and at the same time demonstrate the company's commitment to fairness. This sounds new but is similar like GDPR's concept of certifications as a means of appropriate safeguards.[1375] The second aspect, the idea of a digital skills fund companies must contribute to if the use of AI leads to redeployment not being possible is important since AI may have a significant impact on workforce: for example, in Hungary, more than 40 % of the nation's current jobs can become automated.[1376] As regards potential negative consequences of AI in the employment context, it was even suggested that specific taxes shall be introduced for AI-performed tasks that have previously been performed by humans – because it could compensate for job loss – or because it could compensate for taxes lost as there is no income tax, social security tax, etc. paid when robots do the job.[1377]

6.4.10. Centre for the Fourth Industrial Revolution & NITI Aayong

The Centre for the Fourth Industrial Revolution, which is hosted by the World Economic Forum,[1378] together with the Indian government's policy think tank NITI Aayog partnered to design an ethics framework to ensure the responsible use of AI.[1379]

I. *"**Principle of Safety and Reliability**: AI should be deployed reliably as intended and sufficient safeguards must be placed to ensure the safety of relevant stakeholders. Risks to all stakeholders should be minimized and appropriate grievance redressal, care and compensation structures should be in place, in case of any unintended or unexpected harm. The AI system needs to be monitored through its lifecycle so it performs in an acceptable manner, reliably, according to the desired goals.*

II. ***Principle of Equality**: AI systems must treat individuals under same circumstances relevant to the decision equally.*

[1375] See GDPR Art. 46, 42.

[1376] Background information on Hungary's AI strategy and the country's AI preparations is provided by Dora Petranyi, Katalin Horvath, Marton Domokos, Gabor Bertok: Hungary adopts new AI strategy. Article published September 18, 2020, available at https://www.cms-lawnow.com/ealerts/2020/09/hungary-adopts-new-ai-strategy. Retrieved June 8, 2022.

[1377] Christina Bonnigton: Bill Gates thinks taxing robots could keep them from stealing jobs. Article published February 20, 2017, available at https://www.dailydot.com/debug/bill-gates-robots-tax/. Retrieved June 8, 2022.

[1378] Background information on the Centre for the Fourth Industrial Revolution is available at the World Economic Forum's website https://www.weforum.org/centre-for-the-fourth-industrial-revolution. Retrieved July 25, 2022.

[1379] Further information on the project is available at the World Economic Forum's website: https://www.weforum.org/projects/ai-ethics-framework. Retrieved July 25, 2022.

III. ***Principle of Inclusivity and Non-discrimination****: AI systems should not deny opportunity to a qualified person on the basis of their identity. It should not deepen the harmful historic and social divisions based on religion, race, caste, sex, descent, place of birth or residence in matters of education, employment, access to public spaces, etc. It should also strive to ensure that unfair exclusion of services or benefits does not happen. In case of an adverse decision, appropriate grievance redressal mechanism should be designed in a manner affordable and accessible to everyone irrespective of their background.*

IV. ***Principle of Privacy and Security****: AI should maintain privacy and security of data of individuals or entities that is used for training the system. Access should be provided only to those authorized with sufficient safeguards.*

V. ***Principle of Transparency****: The design and functioning of the AI system should be recorded and made available for external scrutiny and audit to the extent possible to ensure the deployment is fair, honest, impartial and guarantees accountability.*

VI. ***Principle of Accountability****: All stakeholders involved in the design, development and deployment of the AI system must be responsible for their actions. Stakeholders should conduct risk and impact assessments to evaluate direct and indirect potential impact of AI systems on end-users, set up an auditing process (internal and if required external) to oversee adherence to principles and create mechanisms for grievance redressal in case of any adverse impact.*

VII. ***Principle of protection and reinforcement of positive human values:*** *AI should promote positive human values and not disturb in any way social harmony in community relationships."*

6.5. Regulator and best practice guidelines

6.5.1. International Conference of Data Protection and Privacy Commissioners

During their 40th meeting in 2018, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) issued a Declaration on Ethics and Data Protection in Artificial Intelligence[1380] in which they underline the relevance of the empowerment of individuals and the need for the establishment of common governance principles on Artificial Intelligence. They stress that AI shall be designed in a responsible manner as part of an overall ethics by design approach, and set forth the following principles that must be obeyed when developing and applying AI:

I. *Artificial Intelligence and Machine Learning technologies should be designed, developed and used in respect of fundamental human rights and in accordance with the* ***fairness principle***[1381]

[1380] ICDPPC declaration on Ethics and Data Protection in Artificial Intelligence published October 23 2018, available at https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf. Retrieved October 15, 2021.

[1381] Bold means emphasis added.

II. ***Continued attention and vigilance****, as well as accountability, for the potential effects and consequences of, Artificial Intelligence systems should be ensured (...);*

III. *Artificial Intelligence* ***systems transparency and intelligibility*** *should be improved, with the objective of effective implementation (...);*

IV. *As part of an overall "ethics by design" approach, Artificial Intelligence systems should be* ***designed and developed responsibly****, by applying the principles of* ***Privacy by Default and Privacy by Design*** *(...);*

V. ***Empowerment of every individual*** *should be promoted, and the exercise of individuals' rights should be encouraged, as well as the creation of opportunities for public engagement (...);*

VI. ***Unlawful biases or discriminations*** *that may result from the use of data in Artificial Intelligence should be reduced and mitigated."*

6.5.2. Guidance at authority level

Apart from the above-mentioned (legally binding) instruments which deal with data protection and data subject rights (as part of their human rights), there are also other instruments at international level which shall be considered: back in 2009, data protection authorities from more than fifty countries[1382] approved the so-called Madrid Resolution on international privacy standards.[1383] This joint proposal integrates legislation from five continents and includes various principles and obligations any privacy protection legal system must strive to achieve compliance with laws applicable on data protection matters by implementing certain standards including the need to establish authorities to guarantee and supervise the rights of citizens.[1384] The purpose of the Madrid Resolution was to "define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data (…) and the facilitation of the international flows of personal data needed in a globalized world".[1385] In addition, numerous opinions on various data protection topics the so-called Article 29 Working Party[1386] issued[1387] for many years proved to be particularly useful from a privacy practitioner's point of view. The European Data Protection Board explicitly dealt with the "dark pattern"

[1382] Background information on the International Conference of Data Protection and Privacy Commissioners is available at their website https://icdppc.org/. Retrieved October 15, 2021.

[1383] Madrid Resolution published 2009, available at https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf. Retrieved October 15, 2021.

[1384] Further details on the initiative are available at http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf. Retrieved October 15, 2021.

[1385] Calli Schroeder: When the world's DPAs get together: Resolutions of the ICDPPC. Article published November 28 2017, available at https://iapp.org/news/a/when-the-worlds-dpas-get-together-resolutions-of-the-icdppc/. Retrieved October 15, 2021.

[1386] The Article 29 Working Party ceased to exist as of May 25 2018 and has been replaced by the European Data Protection Board (EDPB): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492. Retrieved October 15, 2021.

[1387] Article 29 Working Party documents are available at http://ec.europa.eu/justice/article-29/documentation/index_en.htm. Retrieved October 15, 2021.

phenomenon and issued guidelines on dark patterns in social media platforms,[1388] and various supervisory authorities discussed the effects of Artificial Intelligence and issued corresponding guidance, for example, the Hambacher Erklärung[1389] was published in Germany; the French regulator CNIL issued a report[1390] on ethical issues in the context of using algorithms and Artificial Intelligence; the Norwegian data protection authority also dealt with AI,[1391] and Latin American and Spanish DPAs issued a joint statement on data processing and Artificial Intelligence.[1392] In Singapore, the Personal Data Protection Commission published an updated (second edition) version of their "Model AI Governance Framework" in 2020 in order to provide "readily-implementable guidance to private sector organizations to address key ethical and governance issues when deploying AI solutions."[1393] The Data Protection Commission moreover launched "A.I. Verify", "the world's first AI governance testing framework and toolkit for companies that wish to demonstrate responsible AI in an objective and verifiable manner," and also provides an implementation and self-assessment guide for organizations.[1394] The model framework and the implementation and self-assessment guide is complemented by a compendium of use cases[1395] to demonstrate how various organizations across different sectors and sizes implemented and / or aligned their AI governance practices with the Model Framework.[1396] Following requests from UK industry to clarify AI requirements, the ICO published their (updated) guidance[1397] on AI and Data Protection in March 2023, which included new chapters on impact assessments, and regarding ensuring fairness and lawfulness of AI.

[1388] Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them published March 2022, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. Retrieved July 20, 2022.

[1389] Hambacher Erklärung issued by the conference of independent data protection supervisory authorities, published April 3 2019, available at https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf. Retrieved October 15, 2021.

[1390] CNIL report on the ethical issues of Algorithms and Artificial Intelligence. Report published May 25 2018, available at https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues. Retrieved October 15, 2021.

[1391] Datatilsynet report published January 2018, available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf. Retrieved October 15, 2021. Norway is the only Scandinavian country that is not a member of the European Union. Therefore, strictly speaking, their recommendations cannot be considered as guidance from an EU regulator. However, their paper may still serve as de-facto guidance, and is thus listed within this section.

[1392] Key recommendations are summarized by Odia Kagan: Latin American and Spanish DPAs Issue Joint Statement on Data Processing and Artificial Intelligence. Article published October 24 2019, available at https://dataprivacy.foxrothschild.com/2019/10/articles/general-privacy-data-security-news-developments/latin-american-and-spanish-dpas-issue-joint-statement-on-data-processing-and-ai/. Retrieved October 15, 2021.

[1393] Background information on Singapore's activities in the area of AI is available at the Personal Data Protection Commission's website https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework. Retrieved July 25, 2022.

[1394] The Data Protection Commission's implementation and self-assessment guide is available at https://go.gov.sg/isago. Retrieved July 25, 2022.

[1395] The compendium of use cases is available at https://go.gov.sg/ai-gov-use-cases. Retrieved July 25, 2022.

[1396] Further details on the compendium are available at the Personal Data Protection Commission's website https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework. Retrieved July 25, 2022.

[1397] ICO guidance on AI and data protection last updated March 25 2013, available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/. Retrieved March 25, 2023.

6.5.3. FTC best practice guidance

The Federal Trade Commission (FTC) that can be considered the de-facto data protection authority for the United States[1398] issued new guidance on Artificial Intelligence and algorithms to explain how businesses can promote truth, fairness and equity in their use of AI.[1399] FTC's new guidance is focusing on best practices and lessons learned, and is based on their previous work in the area of AI which included a report on Big Data analytics and Machine Learning,[1400] and a hearing on algorithms, AI and predictive analytics.[1401] In its series of best practices, FTC provides the following advice for business when using AI:

I. ***"Start with the right foundation;***
II. ***Watch out for discriminatory outcomes;***
III. ***Embrace transparency and independence****;*
IV. ***Don't exaggerate what your algorithm can do or whether it can deliver fair or unbiased results;***
V. ***Tell the truth about how you use data;***
VI. ***Do more good than harm;***
VII. ***Hold yourself accountable – or be ready for the FTC to do it for you."***

6.6. National initiatives

Various countries all over the world started working on national strategies to develop own frameworks and strengthen their competitive position with regards to Artificial Intelligence, for example China,[1402]

[1398] Odia Kagan: FTC filling role of de facto U.S. privacy regulator. Article published March 7 2019, available at https://dataprivacy.foxrothschild.com/2019/03/articles/general-privacy-data-security-news-developments/ftc-filling-role-of-de-facto-u-s-privacy-regulator/. Retrieved October 15, 2021.

[1399] The law firm Hunton Andrews Kurth provides background information on FTC's AI guidance in their blog: FTC Reiterates AI Best Practices. Article published April 23 2021, available at https://www.huntonprivacyblog.com/2021/04/23/ftc-reiterates-ai-best-practices/. Retrieved October 15, 2021.

[1400] FTC Report: Big Data: a tool for inclusion or exclusion? Report published January 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Retrieved October 15, 2021.

[1401] FTC Hearing #7: The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics. The hearing took place November 13-14 2018 the framework of a joint event with the Howard University; corresponding materials are available at https://www.ftc.gov/news-events/events-calendar/ftc-hearing-7-competition-consumer-protection-21st-century. Retrieved October 15, 2021.

[1402] Background information on China's national AI strategy is available at https://futureoflife.org/ai-policy-china/. Retrieved October 15, 2021.

India[1403], the U.S.A.[1404] and France:[1405] even though a regulator initiative is not the same as a legislator initiative, it shall be mentioned that in France, the national data protection supervisory authority CNIL announced to introduce a special department dedicated to AI only.[1406] Some countries issued ethical codes, for example the United Kingdom[1407] and Australia,[1408] while others already took first steps to introduce AI in the area of justice, for example Latvia.[1409] The below initiatives in Asia, the Americas, Europe and Australia shall serve as explanatory examples are not exhaustive since the legal and business landscape is very dynamic:

6.6.1. Asia

Japan's AI R&D Guidelines[1410] have not been specifically designed for the Japanese market, but as a non-regulatory and non-binding international framework. Another factor to consider is that these guidelines are not only concerned with overall consequences of AI applications; they shall also serve as "draft guidelines for developers of AI systems to serve as basis for international discussion" (e.g., G7, OECD):[1411] these guidelines shall ensure a balance between benefits & risks of AI and help achieve a human-centered society. The committee also stressed that those guidelines shall be constantly reviewed to allow for flexibly as necessary. In addition to these R&D Guidelines Japan issued for international discussion, the country was also working on Machine Learning Quality Management Guidelines to

[1403] Details on India's national AI strategy is available at https://futureoflife.org/ai-policy-india/. Retrieved October 15, 2021.

[1404] Background information on the United States national AI strategy is available at https://www.ai.gov/. Retrieved October 15, 2021.

[1405] France developed an AI strategy in 2018. A corresponding paper has been published March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf. Retrieved October 15, 2021.

[1406] CNIL communicated their decision on their website on January 23 2023: Création d'un service de l'intelligence artificielle à la CNIL et lancement des travaux sur les bases de données d'apprentissage
23 janvier 2023, available at https://www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de?mkt_tok=MTM4LUVaTS0wNDIAAAGJiRSkCmROWUr0IGfsi9iK3GBVyCSqWg-BP4yZB5vjXuY5r3bgiauAYQvRsvc_-oDnhhptRve5ojcVqLNSYDDVV6sbr-e_6zoDTy03kbo8WE93. Retrieved January 29, 2023.

[1407] UK data ethics framework for the public sector published June 2018, available at https://dataethics.eu/the-uk-data-ethics-framework-for-the-public-sector/#:~:text=The%20UK%20government%20is%20asking%20the%20public%20sector,such%20as%20the%20General%20Data%20Protection%20Regulation%2C%20GDPR. Retrieved October 15, 2021.

[1408] The Australian government issued a statement on AI Ethics in 2019. The statement and further details about the initiative are available at https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework. Retrieved October 15, 2021.

[1409] On 27 September 2018, the Council of Europe European Commission for the efficiency of justice (CEPEJ) and the Courts Administration of the Latvia organized a conference on "Artificial Intelligence at the Service of the Judiciary" in Latvia; the corresponding presentation as well as background information is available at https://www.coe.int/en/web/cepej/justice-of-the-future-predictive-justice-and-artificial-intelligence. Retrieved October 15, 2021.

[1410] A translation of Japan's 2019 Draft AI R&D Guidelines for international discussion is available at http://www.soumu.go.jp/main_content/000507517.pdf. Retrieved October 15, 2021.

[1411] Background information on OECD's work in this area is available at http://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/conference-agenda/ai-intelligent-machines-smart-policies-hirano.pdf. Retrieved October 15, 2021.

establish a basis for quality goals for Machine-Learning-based products and services.[1412] Japan is traditionally very strong when it comes to robotics,[1413] but competitors do not sleep: already in 2008, South Korea enacted a general law on the "intelligent robot industry" which authorized the government to enact a charter on intelligent robot ethics.[1414] South Korea's government released an AI strategy and wants to position the country that is home to many well-known tech companies like Samsung, Hyundai and LG as a global contender by investing in the creation of at least six new AI schools by 2020.[1415] China has the aim to become a world leader in AI and released draft measures to regulate generative AI[1416] and established an AI Governance Expert Committee.[1417] In addition, China published non-binding AI principles to guide the development of Artificial Intelligence,[1418] and there are also local AI policy initiatives throughout China: Shanghai issued its own implementation plan for AI[1419], Guangzhou launched[1420] an International Institute of AI, and Beijing plans to invest in an AI-focused industrial park[1421] and published their own Principles on AI that have been released by a coalition of universities and companies including big players like Alibaba and Tencent.[1422] Together with numerous research and education institutes as well as AI companies, China's standards administration moreover issued a White Paper on AI standardization which also shows that the country takes strong efforts towards becoming a leader in modern technologies such as Big Data and AI after "functioning as a factory to the

[1412] The original document was published in June 30 2020; the Japanese language version is available at https://www.cpsec.aist.go.jp/achievements/aiqm/ and an English version is available at https://www.cpsec.aist.go.jp/achievements/aiqm/AIQM-Guideline-1.0.1.37-summary-en-1.2.pdf. Retrieved October 15, 2021.

[1413] Valerie Thomas: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 15, 2021.

[1414] Intelligent Robots Development and Promotion Act (Act no. 9014) of 2008 amended in 2016 by Act no. 13744, available at http://elaw.klri.re.kr/eng_service/lawView.do?hseq=39153&lang=ENG. Retrieved October 15, 2021.

[1415] Kathleen Walch: Is South Korea Poised To Be A Leader In AI? Article published September 7 2018, available at https://www.forbes.com/sites/cognitiveworld/2018/09/07/is-south-korea-poised-to-be-a-leader-in-ai/#4a0f3d74fa2f. Retrieved October 15, 2021.

[1416] Yan Luo, Xuezi Dan, Vicky Liu, Nicholas Shepherd: China proposes draft measures to regulate generative AI. Article published April 12 2023, available at https://www.insideprivacy.com/artificial-intelligence/china-proposes-draft-measures-to-regulate-generative-ai/. Retrieved April 26, 2023.

[1417] Generation Artificial Intelligence Development Plan published July 8, 2017. An English version of the Chinese State Council's guideline on the development of AI is available at https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan/. Retrieved October 15, 2021.

[1418] Guidelines published June 17, 2019 by China's Ministry of Science and Technology. An English translation is available at https://perma.cc/V9FL-H6J7. Retrieved October 15, 2021.

[1419] Background information on Shanghai's implementation plan for AI is provided by Zhou Wenting: Shanghai unveils 10-year AI plan. Article published July 12 2021, available at https://english.www.gov.cn/news/topnews/202107/12/content_WS60eb9428c6d0df57f98dcbbb.html. Retrieved October 15, 2021.

[1420] Joanna You, Louis Berney: Guangzhou International Institute of AI launched in Nansha. Article published December 15 2017, available at https://www.lifeofguangzhou.com/whatsNew/content.do?contextId=6987&frontParentCatalogId=199&frontCatalogId=200. Retrieved October 15, 2021.

[1421] Arjun Kharpal: China is building a giant $2.1 billion research park dedicated to developing A.I. Article published January 3 2018, available at https://www.cnbc.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html. Retrieved October 15, 2021.

[1422] Beijing AI Principles published May 25 2019, available at https://www.baai.ac.cn/news/beijing-ai-principles-en.html. Retrieved October 15, 2021.

world for almost four decades".[1423] China also announced the formation of the National Artificial Intelligence Standardization Group and Expert Advisory Group to oversee the nation's AI development.[1424] Singapore introduced principles to promote "Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector." [1425] Singapore's initiative is a good example that it is difficult to classify all those different initiatives appropriately: on the one hand, this is a national initiative, on the other hand, it might have the potential to lead the path forward for that specific industry. India's National Institution for Transforming India (NITI) published the nation's national strategy on Artificial Intelligence back in 2018,[1426] and the strategy focuses, amongst other things, on sectors like health and education as well as (smart city) infrastructure and mobility to increase social inclusion and addresses issues like ethics, bias, and privacy. India's strategy paper proposes the creation of Centers of Research Excellence in AI, and in 2019, India's government formed a committee to push for an organized AI policy to further India's AI mission, and the Ministry of Electronics and Information Technology released its own proposal to set up a national AI program.[1427] Indian government's policy think tank NITI Aayog and the Centre for the Fourth Industrial Revolution partnered to co-design an ethics framework to ensure the responsible use of AI.[1428] These two organizations co-designed principles of AI ethics[1429] and jointly drafted self-

[1423] Rachana Gupta: China making big strides in Artificial Intelligence. Article published on September 6 2019, available at http://www.china.org.cn/opinion/2019-09/06/content_75178964.htm. Retrieved October 15, 2021.

[1424] Meghan Han: China aims to get the jump on AI Standardization. Article published January 25 2018, available at https://syncedreview.com/2018/01/25/china-aims-to-get-the-jump-on-ai-standardization/#:~:text=China%20has%20just%20released%20its%20%E2%80%9CArtificial%20Intelligence%20Standardization,Standardization%20Management%20Committee%20Second%20Ministry%20of%20Industry%20%28%E5%9B%BD%E5%AE%B6%E6%A0%87%E5%87%86%E5%8C%96%E7%AE%A1%E7%90%86%E5%A7%94%E5%91%98%E4%BC%9A%E5%B7%A5%E4%B8%9A%E4%BA%8C%E9%83%A8%29. Retrieved October 15, 2021.

[1425] Singapore's FEAT principles published November 12 2018, available at https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf. Retrieved October 15, 2021.

[1426] NITI strategy on Artificial Intelligence published June 13 2019, available at https://niti.gov.in/national-strategy-artificial-intelligence. Retrieved October 15, 2021.

[1427] Artificial Intelligence Index Report 2021, Chapter 7: AI policy and national strategies. Report published 2021, available at https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf. Retrieved October 15, 2021.

[1428] Background information on the project is provided by the World Economic Forum's, available at https://www.weforum.org/projects/ai-ethics-framework. Retrieved July 25, 2022.

[1429] AI ethics principles published February 2021, available at https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf. Retrieved July 25, 2022.

assessment guides for the public and private sectors.[1430] In recent years, further countries developed national AI initiatives and plans, for example Malaysia,[1431] Indonesia[1432] or Taiwan.[1433]

6.6.2. Australia and New Zealand

In order to build Australia's Artificial Intelligence capability and help raise trust in AI technologies, the country developed an AI ethics framework to guide businesses and governments when they design, develop and implement AI:[1434] the outcome of their program is a set of voluntary AI ethics principles including background information on how it was developed as well as guidance on when and how to apply those principles. Moreover, the country's leading standards organization released a discussion paper on developing standards for Artificial Intelligence which underlines the importance of the development of AI standards for the future use of this cutting-edge technology.[1435] Australia's neighbor New Zealand launched a AI forum[1436] in 2017 to connect the country's AI community including citizens, business, academia, and the government and to advance New Zealand's AI ecosystem through advocacy and collaboration.[1437] Since the forum is a not-for-profit, non-governmental body, the forum's work cannot be considered a national strategy, however, their report[1438] may serve as a basis to shape New Zealand AI landscape. In addition, New Zealand also launched an initiative for the government's data system, the Algorithm Charter for Aotearoa New Zealand.[1439]

[1430] Their self-assessment guidance document for the public and private sectors has been published August 2021, and is available at https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf. Retrieved July 25, 2022.

[1431] Priyankar Bhunia: Plans for cloud-first strategy and national AI framework revealed at 29th MSC Malaysia Implementation Council Meeting. Article published October 28 2017, available at https://opengovasia.com/plans-for-cloud-first-strategy-and-national-ai-framework-revealed-at-29th-msc-malaysia-implementation-council-meeting/. Retrieved October 15, 2021.

[1432] Background information on Indonesia's initiatives in the context of AI are available at https://ai-innovation.id/strategi. Retrieved October 15, 2021.

[1433] Details on Taiwan's national AI initiatives are available at https://ai.taiwan.gov.tw/. Retrieved October 15, 2021.

[1434] Background information on Australia's initiatives in the context of AI are available at https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework#:~:text=To%20help%20build%20trust%20in%20AI%2C%20we%E2%80%99ve%20committed,Australian%20Government%E2%80%99s%20commitment%20to%20build%20Australia%E2%80%99s%20AI%20capabilities. Retrieved October 17, 2021.

[1435] Meaghan Powell, Lesley Sutton: AI regulation: the push for Australian standards. Article published July 29 2019, available at https://www.gtlaw.com.au/insights/ai-regulation-push-australian-standards. Retrieved October 17, 2021.

[1436] Details on New Zealand's AI forum are available at https://aiforum.org.nz/. Retrieved October 17, 2021.

[1437] Further background information on how New Zealand intends to shape the future with AI is available at https://www.mbie.govt.nz/dmsdocument/5754-artificial-intelligence-shaping-a-future-new-zealand-pdf. Retrieved October 17, 2021.

[1438] AI forum's report published September 9 2021, available at https://aiforum.org.nz/2021/09/09/state-of-ai-in-new-zealand-report/. Retrieved October 17, 2021.

[1439] Algorithm Charter for Aotearoa New Zealand published July 2020, available at https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/#:~:text=The%20Algorithm%20charter%20for%20Aotearoa%20New%20Zealand%20is,o%20Te%20M%C4%81tauranga%20%E2%80%94%20The%20Ministry%20of%20Education. Retrieved October 17, 2021.

6.6.3. Europe

It can generally be said that Europe has a growing AI industry presence, for example, Spain,[1440] Sweden,[1441] the Netherlands[1442] and Italy[1443] are actively engaging in AI. Many other countries dealt with the issue of Artificial Intelligence and published action plans and strategies of their own, for example Luxembourg,[1444] Lithuania,[1445] Malta[1446] or Norway.[1447] Finland reviewed the public sector use of automation and evaluated the introduction of mandatory due diligence legislation,[1448] and AI initiatives are starting to emerge at regional level: the autonomous regions of Valencia[1449] and Catalonia[1450] introduced their own AI strategies. France announced their "mission for a meaningful AI"[1451] which stresses that Artificial Intelligence shall be based on human rights and that AI should, among other things, address ethics, employment, and diversity.[1452] For the purposes of this paper, two countries shall be examined in greater detail as regards their national AI strategy: Germany and the UK. The UK has a well-established tech landscape and is traditionally strong in research,[1453] and its AI policy

[1440] Background information on the AI landscape in Spain is available at https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2020/20201202_enia.aspx. Retrieved October 15, 2021.
[1441] Details on the AI landscape in Sweden are available at https://www.government.se/information-material/2019/02/national-approach-to-artificial-intelligence/. Retrieved October 15, 2021.
[1442] Background information on the AI landscape in the Netherlands is available at https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence. Retrieved October 15, 2021.
[1443] Details on the AI landscape in Italy are available at https://ia.italia.it/en/ai-in-italy/. Retrieved October 15, 2021.
[1444] Background information on Luxemburg's national initiatives in the area of AI are available at https://digital-luxembourg.public.lu/initiatives/artificial-intelligence-strategic-vision-luxembourg#:~:text=Luxembourg%20intends%20to%20remain%20at%20the%20forefront%20of,experts%20in%20law%2C%20science%2C%20technology%2C%20ethics%20and%20humanities. Retrieved October 15, 2021.
[1445] Further details on Lithuania's national AI initiative is available at http://kurklt.lt/wp-content/uploads/2018/09/StrategyIndesignpdf.pdf. Retrieved October 15, 2021.
[1446] Details on Malta's national initiatives in the field of AI are available at https://malta.ai/. Retrieved October 15, 2021.
[1447] Background information on Norway's national AI landscape is available at https://www.regjeringen.no/en/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/. Retrieved October 15, 2021.
[1448] AccessNow: Europe's approach to Artificial Intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 15, 2021.
[1449] Background information on Valencia's initiative is available at http://www.presidencia.gva.es/documents/80279719/169117420/Dossier_en.pdf/c943f4aa-2822-4c5e-a3db-63a45cca5bf5. Retrieved October 15, 2021.
[1450] Details on Catalonia's initiative are available at https://www.elnacional.cat/en/tech/artificial-intelligence-digital-strategy-catalonia_471462_102.html. Retrieved October 15, 2021.
[1451] Cedric Villani: For a meaningful Artificial Intelligence – towards a French and European strategy. Report published March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf. Retrieved October 15, 2021.
[1452] Alex Moltzau: The French national strategy on Artificial Intelligence. Article published January 15 2020, available at https://towardsdatascience.com/the-french-national-strategy-on-artificial-intelligence-c8c8fcfdace1. Retrieved October 15, 2021.
[1453] Richard Stirling, Hannah Miller, Emma Martinho-Truswell: Oxford Institute government AI readiness index. Article published in 2017, available at https://www.oxfordinsights.com/government-ai-readiness-

discussions intensified in recent years: [1454] on top of the famous Alan Turing Institute – that is: the National Institute of AI,[1455] the UK introduced a Committee on Artificial Intelligence,[1456] established a Centre for Data Ethics and Innovation (CDEI)[1457] which will be tasked with AI monitoring and testing,[1458] and intends to appoint a Minister for AI.[1459] The UK government moreover announced that it intends to revisit its AI strategy[1460] which might have implications for the overall level of data protection given the discussions around softening the conditions around (re-)use of personal data for research and considerations if the ICO is the right forum (regulator)for determining fairness in profiling and automated decision-making.[1461] The UK introduced data protection law reforms[1462] that will, amongst other things, have consequences for documentation requirements since records of processing activities or impact assessments may no longer be needed.[1463] Moreover, legitimate interest assessments will be axed, and some defined processing activities will be exempt from any formal review.[1464] In its new AI rulebook,[1465] the UK takes a different regulatory approach to the EU whereby AI regulation will

index?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BeJ%2FPpiq8RzyLuLPtyf%2FYoA%3D%3D. Retrieved October 15, 2021.

[1454] Details on the UK's AI initiatives are available at https://futureoflife.org/ai-policy-united-kingdom/. Retrieved October 15, 2021.

[1455] Background information on the UK's National Institute of AI is available at https://instituteofai.org/about/. Retrieved October 17, 2021.

[1456] House of Lords Select Committee on Artificial Intelligence Report of Session 2017–19: HL Paper 100 AI in the UK: ready, willing, and able? Report published 2018, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf. Retrieved October 17, 2021.

[1457] Details on UK's Centre for Data Ethics and Innovation are available at their website: https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation. Retrieved October 17, 2021.

[1458] Background information on CDEI and its tasks are provided in CDEI's 2020 report. Report published February 2020, available at https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations. Retrieved October 17, 2021.

[1459] FTI consulting: The global policy response to Artificial Intelligence. Report published February 2018, available at https://ftiinsights.com/the-global-policy-response-to-artificial-intelligence/. Retrieved October 17, 2021.

[1460] Details on UK's AI strategy are provided atthe UK government's website, available at https://www.gov.uk/government/publications/national-ai-strategy?utm_medium=email&utm_campaign=govuk-notifications&utm_source=d5d1f14b-b826-4931-92a2-706e1e5ee6de&utm_content=immediately. Retrieved October 17, 2021.

[1461] Marcus Evans, Peter McBurney, Michael Sinclair: The UK national AI strategy: Regulation, data protection and IPR in the mix. Article published September 27 2021, available at https://www.insidetechlaw.com/blog/the-uk-national-ai-strategy-regulation-data-protection-and-ipr-in-the-mix. Retrieved October 17, 2021.

[1462] Emma Drake, Ruth Boardman: UK data protection reform: What is in the government's proposals? Article published June 23 2022, available at https://iapp.org/news/a/uk-data-protection-reform-what-is-in-the-governments-proposals/. Retrieved July 8, 2022.

[1463] Marcus Evans, Fiona Bundy-Clarke, Shiv Daddar: UK GDPR Reform: government publishes response to consultation – likely to form basis of forthcoming UK Data Reform Bill. Article published June 22 2022, available at https://www.dataprotectionreport.com/2022/06/uk-gdpr-reform-government-publishes-response-to-consultation-likely-to-form-basis-of-forthcoming-uk-data-reform-bill/. Retrieved July 8, 2022.

[1464] Neil Barnes shares insights into the UK data protection reforms: Data – a new direction. What is it & what is being proposed? Article published July 19 2022, available at https://www.bulletproof.co.uk/blog/data-a-new-direction#:~:text=UK%20government%27s%20new%20proposals%20are%20designed%20to%20reform,need%20for%20DPOs%2C%20DPIAs%2C%20LIAs%2C%20ROPAs%20and%20DSARs. Retrieved July 8, 2022.

[1465] Policy paper "Establishing a pro-innovation approach to regulating AI" published July 20 2022, available at https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement. Retrieved July 20, 2022.

be less centralized and will instead allow existing regulatory bodies to make decisions based on their specific context and underline UK's ambitions to become an AI superpower.[1466] Developments in the context of "BREXIT"[1467] caused further unrest, however, in early 2021, the European Commission launched a "process towards the adoption of two adequacy decisions for transfers of personal data to the United Kingdom, one under the General Data Protection Regulation and the other for the Law Enforcement Directive"[1468], a step that many welcomed and some predicted.[1469] In June 2021, the European Commission adopted these two adequacy decisions, meaning that organizations in the EU can transfer personal data to organizations in the UK without restriction, and with no need to use SCCs to ensure an adequate level of protection.[1470] Germany has an AI strategy of its own,[1471] and the German Data Ethics Commission explained the need for a human-centric approach and confirmed core principles like transparency and explicability and robustness as well as values like non-discrimination in their 2019 recommendation.[1472] The expert opinion of the German Data Ethics Commission distinguishes between algorithm-based (suggestion-only), algorithm-driven (limited leeway) and fully automated decisions. It moreover pursues further ideas by presenting a total of not less than 75 recommendations for the use of Artificial Intelligence, including the call for a regulation for Algorithmic Systems and by suggesting various new approaches to AI: a labeling requirement (e.g., for bots[1473]); licensing procedures; product liability; a risk-based regulatory approach based on a graded model for AI reflecting the degree of criticality involved in the data processing activity; a specific right to access for researchers and journalists in sectors that are of particular interest to society; a specific duty with regard to interconnectivity in certain sectors (e.g., messaging services, social media). The idea of a right to data

[1466] Derek du Preez: UK unveils new 'AI rulebook' that takes different regulatory approach to the EU. Article published July 18 2022, available at https://diginomica.com/uk-unveils-new-ai-rulebook-takes-different-regulatory-approach-eu. Retrieved July 20, 2022.

[1467] The European Data Protection Supervisor: Information note on international data transfers after Brexit published July 18 2019, available at https://edps.europa.eu/sites/edp/files/publication/19-07-16_for_translation_note_on_personal_data_transfers_post-brexit_en.pdf. Retrieved October 22, 2021.

[1468] European Commission Press release: Data protection: European Commission launches process on personal data flows to UK. Press release published February 19 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661. Retrieved October 22, 2021.

[1469] Oliver Patel, Nathan Lea: EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows. Article published May 2020, available at https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf. Retrieved October 22, 2021.

[1470] European Commission press release: Commission adopts adequacy decisions for the UK. Press release published June 28 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183. Retrieved October 22, 2021.

[1471] The country's AI strategy was presented in November 2018. Further details on their strategy is available at https://ec.europa.eu/knowledge4policy/publication/germany-artificial-intelligence-strategy_en. Retrieved October 17, 2021.

[1472] "Gutachten der Datenethikkommission" published October 2019, available at https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92BB855CAF2B68DFB5D0EB3D32FD72E4.2_cid287?__blob=publicationFile&v=5. Retrieved October 17, 2021.

[1473] Or for AI generated content, see Christoph Cemper: 13 AI content detection tools tested and AI watermarks. Article published December 29 2022, available at https://www.linkresearchtools.com/blog/ai-content-detector-tools/. Retrieved January 10, 2023.

ownership which has been discussed in the literature[1474] as one possible way to strengthen individuals' rights but is not recommended by the commission since the introduction of new exclusive rights is believed to complicate the legal framework rather than solving existing problems. On top of the 2019 Data Ethics Commission recommendations, Germany's "Study Commission on Artificial Intelligence" issued its final report which also included specific recommendations.[1475] In 2020, the German Federal Government adopted its AI strategy[1476]and committed to increase the expenditure for the promotion of AI by EUR 5 billion by 2025.[1477] At present, German industry and trade associations are lobbying the EU institutions with the aim to amend the AI Act because "overregulation of AI would discourage the development of innovative applications."[1478]

6.6.4. Hungary

In Hungary, an AI Coalition has been formed in 2018[1479] as a partnership between governmental institutions, academics, and practitioners from leading IT businesses. In 2019, the AI Coalition released an AI Action Plan, and drew up Hungary's AI strategy for the Hungarian Government in 2020. The Hungarian national AI strategy[1480] calls for the development of sector-specific regulatory frameworks to ensure that the regulatory needs for AI development are adapted to the relevant industry areas, it focuses on strengthening of the foundation pillars of its AI ecosystem (for example, with respect to infrastructure deployment, research and development, education and competence development, as well as a regulatory and ethical framework); it is furthermore planned to initiate transformative programs for the benefit of citizens (for example, through automated administration procedures, or data-wallets and personalized services), and aims to ensure a responsible, reliable and human-centered utilization of AI technologies by means of the following policies*:*

[1474] Udo Kornmeier, Anne Baranowski: Eigentum an Daten – Zugang statt Zuordnung. Der Betriebsberater 2019, pp. 1219-1225.

[1475] Executive report summary published October 27 2020, available at https://www.bundestag.de/resource/blob/804184/f31eb697deef36fc271c0587e85e5b19/Kurzfassung-des-Gesamtberichts-englische-Uebersetzung-data.pdf. Retrieved January 20, 2023.

[1476] Background information on Germany's updated AI strategy is available at https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf-. Retrieved January 20, 2023.

[1477] Further details on Germany's economic stimulus and future package is available at https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Konjunkturpaket/2020-06-03-eckpunktepapier.pdf;jsessionid=097AA7D3627F7946A491E341F0C364F4.delivery2-replication?__blob=publicationFile&v=10. Retrieved January 20, 2023.

[1478] Axel Spies: Germany and the EU Artificial Intelligence Act. Article published July 29 2022, available at https://www.aicgs.org/2022/07/germany-and-the-eu-artificial-intelligence-act/. Retrieved January 10, 2023.

[1479] Background information on Hungary's AI Coalition is available at https://ai-hungary.com/. Retrieved January 2, 2023.

[1480] Hungary's Artificial Intelligence 2020-2030 strategy published May 2020, available at https://ai-hungary.com/api/v1/companies/15/files/146074/view. Retrieved January 2, 2023.

- *Creating an ethical framework: developing an AI code of conduct by the first half of 2021 in collaboration between the Ministry of Justice, the Ministry for Innovation and Technology, AI Innovation Hub and the Central Statistical Office;*
- *Establishing a regulatory framework for AI: the objective is to amend the current regulatory system to suit AI and to align it to EU regulations:*
- *Building data management regulation: the objective is to set up regulations for the use and exchange of public and private data and to define rules regarding data monetization*."
- *Setting up an Artificial Intelligence Regulation and Ethics Knowledge Centre: the aim is to create and coordinate an extensive pool of experts to help resolve legal issues and matters of ethics relating to the regulation of AI and the implementation of the strategy;*[1481]

Closely connected to the last point is another important aspect of Hungary's AI strategy: the goal to leverage human competencies and to raise individuals' awareness and knowledge with respect to AI by, amongst other things, providing trainings[1482] and by transforming the educational system to prepare for the digital world, including the future labor market as outlined in the corresponding digital education strategy.[1483] It is important to note that the envisaged reform of the education system not only addresses students to help them develop AI-related skills and competencies, but also foresees specific training for teachers, and the establishment of PhD programs in the field of AI. Overall, the human capital aspect of Hungary's AI strategy is focused on lifelong learning and upskilling of the workforce.

6.6.5. Israel and the Middle East

Despite the fact that Israel is a small country, the nation is determined to be the next major Artificial Intelligence player.[1484] Israel is heavily engaged in AI and launched a national AI program, however, lack of budget threatens its implementation.[1485] In the framework of "Smart Dubai", which is an initiative that fosters digitalization and technologies like Blockchain and Artificial Intelligence, Dubai

[1481] Details on Hungary's national AI strategy and its components are provided by the European Commission in the framework of their AI Watch country pages, available at https://ai-watch.ec.europa.eu/countries/hungary/hungary-ai-strategy-report_en#regulation. Retrieved January 2, 2023

[1482] For example, through the AI Challenge, an initiative that aims to train at least of 1 % of society to learn the basics about Artificial Intelligence by completing an online course. The AI Challenge is available at https://ai-hungary.com/en/content/ai-academy/learn#challenge. Retrieved January 2, 2023.

[1483] Background information Hungary's digital education strategy that was enancted in 2016 is available at https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/hungary/68-media-literacy-and-safe-use-of-new-media#:~:text=The%20Digital%20Education%20Strategy%20of%20Hungary%20The%20strategy,create%20equal%20opportunities%20and%20a%20secure%20digital%20environment. Retrieved January 2, 2023.

[1484] Éanna Kelly: Israel sets out to become the next major Artificial Intelligence player. Article published July 2 2019, available at https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligence-player. Retrieved October 17, 2021.

[1485] Meir Orbach: Israel launches national AI program, but lack of budget threatens its implementation. Article published December 22 2020, available at https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html. Retrieved October 17, 2021.

issued AI ethics principles and guidelines to "deliver detailed guidance for the crucial issues of fairness, accountability, transparency and explainability of the algorithms at the heart of AI systems. We would like to see the Dubai AI Ethics Guidelines evolve into a universal, practical and applicable framework informing ethical requirements for AI design and use."[1486] Dubai's AI principles focus on ethics, humanity, inclusiveness and security[1487] and Dubai moreover offers a free self-assessment AI ethics tool to provide practical help for the public and private sector as well as anyone "interested in how ethical AI is applied in society and city service settings".[1488] Given the importance of AI for various industries and in particular for autonomous weapons and drones, Israel and UAE defense companies partner on Artificial Intelligence.[1489] In recent years, further countries in the Arabian Peninsula engaged in their own national AI strategies, for example Qatar.[1490]

6.6.6. Latin America

Mexico joined many other ambitious nations in their wish to establish themselves as a leader in digital technologies such as Artificial Intelligence and was the first country in Latin America to announce a national AI strategy.[1491] Mexico's approach is unique insofar as it focuses on the social impacts of AI, for example by addressing use cases like combating corruption, reducing crime, improving public health and increasing financial inclusion.[1492] Brazil's Ministry of Science, Technology, Innovations and Communications published the nation's strategy for digital transformation to harmonize and coordinate various governmental initiatives on digital issues.[1493] In addition, the government launched a national

[1486] The "Smart Dubai" website is available at https://www.smartdubai.ae/initiatives/ai-ethics. Retrieved October 17, 2021.

[1487] Dubai's AI principles and guidelines published 2018, available at https://www.smartdubai.ae/pdfviewer/web/viewer.html?file=https://www.smartdubai.ae/docs/default-source/ai-ethics-resources/ai-ethics.pdf?sfvrsn=a9081451_8. Retrieved October 17, 2021.

[1488] Dubai's free self-assessment AI Ethics toolkit is available at https://www.smartdubai.ae/initiatives/ai-principles-ethics. Retrieved October 17, 2021.

[1489] Seth Frantzman: Israel and UAE defense companies partner on Artificial Intelligence. Article published April 21 2021, available at https://nationalinterest.org/blog/buzz/israel-and-uae-defense-companies-partner-artificial-intelligence-183274. Retrieved October 17, 2021.

[1490] Joseph Varghese: Qatar launches strategy to tap AI for future. Article published October 29 2019, available at https://www.gulf-times.com/story/645930/Qatar-launches-strategy-to-tap-AI-for-future#:~:text=The%20National%20AI%20Strategy%20is%20a%20blueprint%20produced,collaboration%20between%20the%20government%20and%20a%20research%20institute. Retrieved October 17, 2021.

[1491] Mexico's 2018 AI strategy is available at https://datagovhub.elliott.gwu.edu/mexico-ai-strategy/#:~:text=Mexico%E2%80%99s%20national%20AI%20strategy%20has%20five%20areas%20of,data%20infrastructure%20...%205%205.%20Ethics%20and%20regulation. Retrieved October 15, 2021.

[1492] Emma Martinho-Truswell, Constanza Gomez Mont: Mexico leads Latin America as one of the first ten countries in the world to launch an Artificial Intelligence strategy. Article published May 24 2018, available at https://www.oxfordinsights.com/insights/2018/5/24/mexico-leads-latin-america-as-one-of-the-first-ten-countries-in-the-world-to-launch-an-artificial-intelligence-strategy. Retrieved October 15, 2021.

[1493] Background information on Brazil's strategy for digital transformation is available at https://www.gov.br/mcti/pt-br. Retrieved October 15, 2021.

plan for the Internet of Things[1494] that will be supported by several AI laboratories[1495] to cover different areas and aspects of AI. Like Mexico, Brazil is also concerned with social impact of Big Data and Artificial Intelligence, which is why their strategy includes a provision "to evaluate such consequences and propose policies which maximize positive results and mitigate potential negative effects."[1496] In the meantime, further South American countries like Colombia,[1497] Chile[1498] and Uruguay[1499] have been working on their own national AI strategies.

6.6.7. North America

Together with France, Canada issued a statement on Artificial Intelligence[1500] with the wish to promote human-centric AI that is based on human rights and values like inclusion and diversity – as well as innovation and economic growth.[1501] Canada issued a Directive on Automated Decision-Making,[1502] and Canada's National Research Council published an advisory statement on human ethics in Artificial Intelligence and Big Data research.[1503] The Canadian government announced the "Declaration of the International Panel on AI"[1504] which states that participants in the IPAI will obey the following values for the development and use of AI:[1505]

[1494] Brazil's national IoT plan is available at https://www.bnamericas.com/en/news/brazil-issues-decree-for-national-iot-plan. Retrieved October 15, 2021.

[1495] Further details on the AI laboratories are available at https://agenciabrasil.ebc.com.br/en/geral/noticia/2019-11/brazil-unveils-eight-new-ai-labs. Retrieved October 15, 2021.

[1496] Brazil's national AI strategy is available at https://futureoflife.org/ai-policy-brazil/. Retrieved October 15, 2021.

[1497] Background information on Colombia's national AI strategy is available at https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf. Retrieved October 15, 2021.

[1498] Details on Chile's national AI strategy are available at https://www.gob.cl/en/news/government-announces-artificial-intelligence-plan-be-developed-science-ministry/. Retrieved October 15, 2021.

[1499] Background information on Uruguay's national AI strategy is available at https://www.gub.uy/participacionciudadana/consultapublica. Retrieved October 15, 2021.

[1500] Canada and France work with international community to support the responsible use of Artificial Intelligence. The corresponding press release has been published May 16 2019 and is available at https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/05/23_cedrico_press_release_ia_canada.pdf. Retrieved October 15, 2021.

[1501] The Canada-France Statement on Artificial Intelligence provides further details in this context. Statement published June 2018, available at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/europe/2018-06-07-france_ai-ia_france.aspx?lang=eng. Retrieved October 15, 2021.

[1502] Canada Directive on Automated Decision-Making published April 2021, available at https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592. Retrieved October 15, 2021.

[1503] Advisory statement on human ethics in AI and Big Data research published in 2017 and last modified in 2019. It is available at https://nrc.canada.ca/en/corporate/values-ethics/research-involving-human-participants/advisory-statement-human-ethics-artificial-intelligence-big-data-research-2017. Retrieved October 15, 2021.

[1504] Meagan Simpson: Canada, France governments announce declaration of the International Panel on AI. Article published May 16 2019, available at http://canada.ai/posts/canada-france-governments-announce-declaration-of-the-international-panel-on-ai. Retrieved October 15, 2021.

[1505] Declaration of the International Panel on Artificial Intelligence published May 16 2019, available at https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/declaration-of-the-international-panel-on-artificial-intelligence.html. Retrieved October 15, 2021.

I. *“**Promote a human-centric and ethical approach to AI that is grounded in human rights**;*
II. ***Support a multi-stakeholder approach to AI;***
III. ***Stimulate innovation, growth and well-being through AI**;*
IV. ***Align efforts on AI with the principles of sustainable development and the goals of the 2030 Agenda for Sustainable Development;***
V. ***Promote and protect democratic values, processes and institutions**;*
VI. ***Promote international scientific collaboration on AI;***
VII. ***Foster transparency and openness of AI systems**,*
VIII. ***Strengthen diversity and inclusion through AI**;*
IX. ***Foster trust and accountability in AI**;*
X. ***Bridge digital divides.**”*

Canada furthermore introduced the Digital Charter Implementation Act,[1506] a package of laws that, if passed, will reform the Canadian privacy law including a tribunal specific to privacy and data protection – and implement Canada’s first AI legislation, the Artificial Intelligence and Data Act (AIDA) which aims at protecting individuals from potential harms and biased outputs AI systems can generate. AIDA establishes requirements for the design, development, use, and provision of AI systems, mandates impact assessments, and foresees administrative monetary penalties, or even criminal offences for certain conduct in relation to AI systems.[1507]

6.6.8. United States

More and more U.S. states are about to introduce privacy bills of their own; developments in the U.S.A. with regards to (consumer) privacy laws are so dynamic that corresponding legal news alerts are delivered on a weekly basis.[1508] To name a few, the following bills establish consumer rights and business obligations related to privacy, including key provisions about transparency, consent, data subject rights, and the designation of Privacy Officers:[1509] the Information Transparency & Personal Data Control Act,[1510] the Deceptive Experiences to Online Users Reduction Act,[1511] the Banning

[1506] The bill text is available at https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading. Retrieved July 8, 2022.
[1507] Maya Medeiros, Jesse Beatson: Canada’s Artificial Intelligence legislation is here. Article published June 28 2022, available at https://www.dataprotectionreport.com/2022/06/canadas-artificial-intelligence-legislation-is-here/. Retrieved July 8, 2022.
[1508] The U.S. law firm Husch Blackwell offers a free online State Privacy Law Tracker with weekly updates. The tracker is available at https://www.huschblackwell.com/2021-state-privacy-law-tracker.
[1509] Müge Fazlioglu: U.S. federal privacy legislation tracker. Article published April 2022, available at https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/. Retrieved July 8, 2022.
[1510] The bill text is available at https://www.congress.gov/bill/117th-congress/house-bill/1816. Retrieved July 8, 2022.
[1511] The bill text is available at https://www.congress.gov/bill/117th-congress/senate-bill/3330. Retrieved July 8, 2022.

Surveillance Advertising Act,[1512] the Social Media Privacy Protection and Consumer Rights Act,[1513] or the Balancing the Rights of Web Surfers equally and responsibly Act.[1514] In addition, democrats from four key Senates released a Privacy and Data Protection Framework[1515] that could serve as the baseline for any comprehensive federal privacy and data protection legislation.[1516] Overall, it truly looks as if the U.S. heavily engages in the AI arms race as there seems to be a strong wish to shape the American AI policy: the U.S.A. engaged in many further initiatives like the Artificial Intelligence Act[1517], the Algorithmic Accountability Act,[1518] the AI in Government Act,[1519] the Future of AI Act,[1520] the Artificial Intelligence Reporting Act,[1521] the National Artificial Intelligence Initiative Act,[1522] the Advancing AI Research Act,[1523] the Growing Artificial Intelligence Through Research Act[1524] as well as the National Security Commission on Artificial Intelligence Act.[1525]

6.6.8.1. NIST AI framework

The White House published the Executive Order on Maintaining American Leadership in Artificial Intelligence[1526] in 2019 which, amongst other things, requires the National Institute of Standards and

[1512] The bill text is available at https://www.congress.gov/bill/117th-congress/house-bill/6416. Retrieved July 8, 2022.

[1513] The bill text is available at https://www.congress.gov/bill/117th-congress/senate-bill/1667. Retrieved July 8, 2022.

[1514] The bill text is available at https://www.congress.gov/bill/117th-congress/senate-bill/113. Retrieved July 8, 2022.

[1515] The text of the Senate’s principles is available at https://www.democrats.senate.gov/imo/media/doc/Final_CMTE%20Privacy%20Principles_11.14.19.pdf. Retrieved October 15, 2021.

[1516] Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/. Retrieved October 15, 2021.

[1517] Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article published May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/. Retrieved October 15, 2021.

[1518] The bill text is available at https://www.congress.gov/bill/116th-congress/senate-bill/1108. Retrieved October 15, 2021.

[1519] The bill text is available at https://www.congress.gov/bill/115th-congress/senate-bill/3502. Retrieved October 15, 2021.

[1520] The bill text is available at https://www.congress.gov/bill/115th-congress/house-bill/4625. Retrieved October 15, 2021.

[1521] The bill text is available at https://www.congress.gov/bill/115th-congress/house-bill/6090/. Retrieved October 15, 2021.

[1522] The bill text is available at https://www.congress.gov/bill/116th-congress/house-bill/6216. Retrieved October 15, 2021.

[1523] The bill text is available at https://www.congress.gov/bill/116th-congress/senate-bill/3891. Retrieved October 15, 2021.

[1524] The bill text is available at https://www.congress.gov/bill/116th-congress/house-bill/2202. Retrieved October 15, 2021.

[1525] The bill text is available at https://www.congress.gov/bill/115th-congress/house-bill/5356/. Retrieved October 15, 2021.

[1526] The bill text is available at https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/. Retrieved October 15, 2021.

Technology (NIST) to release a plan[1527] for federal engagement on AI standards that address both, technical and safety issues, as well as some substantive concerns around AI like data quality and explicability of AI decisions as well as ethical considerations.[1528] In 2021, NIST issued a report on trust and Artificial Intelligence in which they conclude that trust will be necessary for any human-AI collaboration: "if the AI system has a high level of technical trustworthiness, and the values of the trustworthiness characteristics are perceived to be good enough for the context of use, and especially the risk inherent in that context, then the likelihood of AI user trust increases."[1529] The White House's Office of Science and Technology Policy released a draft Guidance for Regulation of Artificial Intelligence Applications[1530] which includes ten principles for agencies to consider when deciding whether and how to regulate AI:[1531]

I. ***"Public trust in AI** – the government's regulatory and non-regulatory approaches to AI promote reliable, robust and trustworthy AI applications, which will contribute to public trust in AI;*

II. ***Public participation** – agencies should provide ample opportunities for the public to provide information and participate in all stages of the rulemaking process;*

III. ***Scientific integrity and information quality** – approaches to AI applications should leverage scientific and technical information and processes;*

IV. ***Risk assessment and management** – approaches to AI should be based on a consistent application of risk assessment and risk management across various agencies and various technologies;*

V. ***Benefits and costs** – [agencies should] … select those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity);*

VI. ***Flexibility** – agencies should pursue performance-based and flexible approaches that can adapt to rapid changes and updates to AI applications;*

[1527] NIST: U.S. Leadership in AI - A plan for federal engagement in developing technical standards and related tools prepared in response to Executive Order 13859. Draft submitted August 9 2020, available at https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf. Retrieved October 15, 2021.

[1528] Duane Pozza, Jacquelynn Ruff: The next phase of AI regulation in the U.S. and abroad. Article published July 19 2019, available at https://www.wileyconnect.com/home/2019/7/19/the-next-phase-of-ai-regulation-in-the-us-and-abroad. Retrieved October 15, 2021.

[1529] National Institute of Standards and Commerce: Trust and Artificial Intelligence. Report published March 2021, available at https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8332-draft.pdf. Retrieved October 3, 2021.

[1530] The draft guidance for the regulation of Artificial Intelligence applications is available at https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf. Retrieved July 25, 2022.

[1531] Background information is provided by Alan Briggs: Government guidance –10 core principles for stewardship of AI apps. Article published January 15 2020, available at https://pubsonline.informs.org/do/10.1287/LYTX.2020.01.18n/full/. Retrieved July 25, 2022.

VII. ***Fairness and nondiscrimination*** *– "agencies should consider … whether the AI application at issue may reduce levels of unlawful, unfair, or otherwise unintended discrimination as compared to existing processes;*

VIII. ***Disclosure and transparency*** *– transparency and disclosure can increase public trust and confidence in AI applications;*

IX. ***Safety and security*** *– agencies should … encourage the consideration of safety and security issues throughout the AI design, development, deployment, and operation process;*

X. ***Interagency coordination*** *– a coherent and whole-of-government approach to AI oversight requires interagency coordination*."

The National Institute of Standards and Technology furthermore released a draft of an AI Risk Management Framework (AI RMF), a set of high-level voluntary guidelines and recommendations that organizations can follow to manage risks in the design, development, use, and evaluation of AI systems.[1532] This framework is still under development, and NIST has posted the latest iterations.[1533] NIST furthermore released an initial draft of a playbook[1534] as a companion to the AI Risk Management Framework. NIST separately released a document titled, "Towards a Standard for Identifying and Managing Bias within Artificial Intelligence"[1535] which aims to provide guidance for mitigating harmful bias in AI systems.

6.6.8.2. Blueprint for an AI bill of rights

In 2022, the White House published a document to open a discussion about a Bill of Rights in an AI-powered world:[1536] the Blueprint for an AI Bill of Rights is a "set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence."[1537] The following ideas are being discussed in the

[1532] Background information on NIST's AI Risk Management Framework is available at https://www.nist.gov/itl/ai-risk-management-framework. Retrieved July 22, 2022.

[1533] Further details on NIST's work with regards to the AI RMF, including latest versions of their publications are available at the National Institute of Standards and Technolog's website at https://www.nist.gov/itl/ai-risk-management-framework. Retrieved January 2, 2023.

[1534] The NIST AI Risk Management Framework Playbook published January 26, 2023, available at https://pages.nist.gov/AIRMF/. Retrieved January 2, 2023. An update of the playbook is expected in early 2023.

[1535] NIST Standard for Identifying and Managing Bias within Artificial Intelligence published March 2020, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf. Retrieved July 22, 2022.

[1536] Background information on the initiative is provided by the White House: Americans need a bill of rights for an AI-powered world: https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/. Retrieved December 31, 2022.

[1537] Details on the Blueprint for an AI bill of rights are available at the White House's website https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/#:~:text=The%20Blueprint%20for%20an%20AI%20Bill%20of%20Rights,American%20public%20in%20the%20age%20of%20artificial%20intelligence. Retrieved December 31, 2022.

framework of the AI bill of rights:[1538] a right to know when AI is impacting civil liberties and a right to meaningful recourse should an algorithm's recommendations harm individuals as well as freedom from being subjected to AI decisions made from biased data sets, and freedom from surveillance (i.e., voice-activated systems, computer-usage monitoring systems, facial recognition, etc.). The "vision for protecting civil rights in the Algorithmic Age" lays out "five common sense protections to which everyone in America should be entitled":[1539]

I. *"**Safe and Effective Systems**: You should be protected from unsafe or ineffective systems.*

II. ***Algorithmic Discrimination Protections**: You should not face discrimination by algorithms and systems should be used and designed in an equitable way.*

III. ***Data Privacy**: You should be protected from abusive data practices via built-in protections, and you should have agency over how data about you is used.*

IV. ***Notice and Explanation**: You should know when an automated system is being used and understand how and why it contributes to outcomes that impact you.*

V. ***Human Alternatives, Consideration, and Fallback**: You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter."*

Even though the Blueprint for an AI bill of rights aims to protect Americans, it shall perhaps not be interpreted as a mere national initiative: tech giants such as Microsoft, Meta, or Google and many other players in the field of AI are headquartered in the U.S., and if all these companies comply with the proposed AI rules, the effects – the scope – of this bill of rights will likely go beyond national borders. Moreover, it shall be noted that the EU and the US are working on a "Joint Roadmap for Trustworthy AI and Risk Management"[1540] to, amongst other things, help build a "common repository of metrics for measuring AI trustworthiness and risk management methods."[1541]

[1538] Glenn Gow: The AI Bill Of Rights: protecting Americans from the dangers of Artificial Intelligence. Article published January 9 2022, available at https://www.forbes.com/sites/glenngow/2022/01/09/the-ai-bill-of-rights-protecting-americans-from-the-dangers-of-artificial-intelligence/. Retrieved December 31, 2022.

[1539] Alondra Nelson, Sorelle Friedler, Ami Fields-Meyer: A vision for protecting our civil rights in the algorithmic age. Article published October 4 2022, available at https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/. Retrieved December 31, 2022.

[1540] EU-U.S.Trade and Technology Council (TTC) Roadmap on evaluation and measurement tools for trustworthy AI and risk management published December 1 2022, available at https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management?utm_source=POLITICO.EU&utm_campaign=3e89ce51a0-EMAIL_CAMPAIGN_2023_01_19_12_30&utm_medium=email&utm_term=0_10959edeb5-3e89ce51a0-%5BLIST_EMAIL_ID%5D. Retrieved January 22, 2023.

[1541] TTC Roadmap on evaluation and measurement tools for trustworthy AI and risk management published December 1 2022, available at https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management?utm_source=POLITICO.EU&utm_campaign=3e89ce51a0-EMAIL_CAMPAIGN_2023_01_19_12_30&utm_medium=email&utm_term=0_10959edeb5-3e89ce51a0-%5BLIST_EMAIL_ID%5D. Retrieved January 22, 2023.

6.7. Other

6.7.1. Rome Call for AI Ethics

Individual and societal implications of certain AI applications are so significant that even the Vatican raised the issue in their 2020 conference "The Good Algorithm", the Vatican Academy for Life concluded the session with the Rome Call for AI Ethics.[1542] Microsoft and IBM are the first signatories to this AI ethics code that calls for a human-centered approach.[1543] The initiative focuses on the responsibility that comes with new digital technologies. The Rome Call for AI Ethics comprises three impact areas ethics, education and rights and names the following six principles:[1544]

I. ***"Transparency**[1545]: In principle, Artificial Intelligence systems must be explainable.*

II. ***Inclusion**: the needs of all human beings must be taken into consideration so that all can benefit form and enjoy the best possible conditions to express themselves and grow.*

III. ***Responsibility**: Designers and developers of Artificial Intelligence solutions must act responsibly and transparently.*

IV. ***Impartiality**: Systems should not be created or operated according to bias, in view to protect human equality and dignity.*

V. ***Reliability**: Artificial Intelligence systems must be able to operate reliably.*

VI. ***Security and privacy**: Artificial Intelligence systems must work securely and respect the privacy of users."*

6.7.2. Hippocratic Oath for Data Scientists

Another noteworthy initiative is the Hippocratic Oath for Data Scientists: the interesting idea behind this voluntary commitment is that, unlike medical staff that is trained on and aware of ethics aspects of their work from the beginning, this is not common in data science – despite the fact that even players like Microsoft say it could make sense to "bind coders to a pledge like that taken by physicians to first do no harm."[1546] Since many activities in the area of data science can have serious consequences for

[1542] Vatican workshop on ethics in AI: Artificial Intelligence 2020 RenAIssance – a human-centric Artificial Intelligence. Presentation held February 28 2020, available at http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/CALL%2028%20febbraio/02_Brad%20Smith_20200228%20Vatican%20AI%20v07.pdf. Retrieved October 17, 2021.

[1543] Joe Fay: Vatican signs up IBM and Microsoft as AI ethics apostles. Article published March 2 2020, available at https://devclass.com/2020/03/02/vatican-signs-up-ibm-and-microsoft-as-ai-ethics-apostles/.

[1544] The Call for AI Ethics is a document signed by the Pontifical Academy for Life, Microsoft, IBM, FAO and the Italian Ministry of Innovation. Paper published February 28 2020, available at https://www.romecall.org/the-call/. Retrieved October 17, 2021.

[1545] Bold means emphasis added.

[1546] Tom Simonite reports about Microsoft's related publication: Should data scientists adhere to a Hippocratic Oath? Article published August 2 2018, available at https://www.wired.com/story/should-data-scientists-adhere-to-a-hippocratic-oath/. Retrieved October 17, 2021.

individuals and society,[1547] data scientists who process data and design algorithms should respect the following three principles:[1548]

I. *“**Responsibility and Neutrality**:[1549] Every data scientist has to assume his responsibilities in the event of breaches or conflicts of interest, and he must alert if any illegal acts related to data are observed. He must also exercise his professional activity respecting the privacy and dignity of people in all their dimensions;*

II. ***Transparency**: As a data scientist, I have the right to inform all stakeholders in an understandable and precise manner about the purposes, modalities, and potential implications of my use of data;*

III. ***Equity**: I will always ensure that individuals or groups are not discriminated on the basis of illegal or illegitimate criteria, directly or indirectly, related to my data work.”*

This chapter has shown that the rapid spread of Artificial Intelligence systems led to a rise in various (best practice, ethics and human rights-based) guidelines and recommendations to help with the use and further development of such applications. In summary, the current legal framework for AI can be grouped as follows: there is legislation for specific processing operations (e.g.) automated decision making, for specific industries (e.g. finance or health), and for specific technology (e.g. facial recognition) as well as rules for accountability for (unintended) consequences by the use of AI (e.g. criminal, civil), and there are moreover numerous voluntary ethics codes.[1550] However, as for the latter, there has been little focus on analyzing these efforts to understand the main principles behind these frameworks. To that end, the Berkman Klein Center for Internet and Society evaluated numerous AI principles documents to detect potential common standards; their research uncovered a growing consensus around eight key thematic trends:[1551]

[1547] Lori Sherer: Data scientists, take a Hippocratic Oath: While the ethics of analytical tools can be tricky to parse, five basic principles can help data scientists address the challenge. Article published June 13 2018, available at https://www.bain.com/insights/data-scientists-take-a-hippocratic-oath-forbes/ Retrieved October 17, 2021.

[1548] Kamal Chouhbi: Hippocratic Oath for data scientists – the ethical checklist that every data scientist must follow. Article published October 6 2020, available at https://towardsdatascience.com/hippocratic-oath-for-data-scientists-407d2db15a78. Retrieved October 17, 2021.

[1549] Bold means emphasis added.

[1550] Maya Medeiros: A legal framework for Artificial Intelligence. Article published November 20 2019, available at https://www.socialmedialawbulletin.com/2019/11/a-legal-framework-for-artificial-intelligence/. Retrieved October 17, 2021.

[1551] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center research publication no. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

I. *“**Privacy**[1552] including control over use of data, consent, privacy by design, recommendations for data protection laws, the ability to restrict processing, as well as the right to erasure and rectification;*

II. ***Accountability** including recommendation for new regulations, impact assessments, evaluation and auditing requirement, verifiability, and replicability as well as liability and legal responsibility and the ability to appeal, environmental responsibility and the creation of a monitoring body and remedies for automated decisions;*

III. ***Safety and security** including reliability, predictability, and security by design;*

IV. ***Transparency and explainability** including open source, data and algorithms, notifications when interacting with AI and whenever AI makes a decision about an individual, regular reporting requirements and the right to information and finally, open procurement (for governments);*

V. ***Fairness and non-discrimination** including the prevention of bias, equality, inclusiveness in design and impact as well as representative and high-quality data;*

VI. ***Human control of technology including human review of automated decisions** and the ability to opt out of automated decisions;*

VII. ***Professional responsibility** including multistakeholder collaboration, responsible design, consideration of long-term effects as well as accuracy and scientific integrity;*

VIII. ***Promotion of human values** including leveraged to benefit society, human flourishing, and access to technology.”*

The researchers stress that, by sharing their observations, they hope that policymakers and others “working to maximize the benefits and minimize the harms of AI will be better positioned to build on existing efforts and to push the fractured, global conversation on the future of AI toward consensus.”[1553] Obviously, such research is very welcome and of great value, but the problem with all these initiatives is that, regardless of whether the guideline or recommendation is issued at international or national level or published by civil society, multi-stakeholder or intergovernmental organizations or if it originated in the private sector – but the problem is that, at present, most of the these initiatives are legally not binding.[1554] Governments around the world are working towards trustworthy AI, but there is no consensus on how to best regulate AI: there is agreement that transparency is a minimum requirement, and discussions started shifting in the direction of human rights protections with growing calls to ban facial recognition, but there is “significant divergence regarding what stakeholders want to see in the

[1552] Bold means emphasis added.

[1553] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center research publication no. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

[1554] See AlgorithmWatch’s AI Ethics Guidelines Global Inventory: https://inventory.algorithmwatch.org/. Retrieved October 17, 2021.

upcoming EU legislation and their respective national policies", and some legislators even expressed the fear of over-regulation.[1555]

In summary, a common feature of most international, intergovernmental, multistakeholder, civil society initiatives and expert guidelines is that they focus on established principles. An analysis of propositions relating to AI applications shows that most proposals suggest that any future AI regulations shall take the following into consideration: accountability and responsibility, human control of technology, safety and security, transparency and explicability, fairness, non-discrimination as well as privacy and the promotion of human values, which contains the following (main principles within each theme):[1556]

I. ***Transparency and explainability**: Right to information, use of open-source data and algorithms, notification requirements when interacting with an AI and when AI makes decisions about individuals, regular reporting, open procurement (for government institutions);*

II. ***Accountability**: Verifiability and replicability, liability and legal responsibility, impact assessments, evaluation and auditing requirement remedy for automated decision, creation of monitoring bodies, social and environmental responsibility;*

III. ***Privacy**: Privacy by Design, control over use of personal data, ability to restrict processing, right to rectification, right to erasure, recommendation for further development of data protection laws;*

IV. ***Human control of technology**: Human control of technology including human review of automated decisions, ability to opt out of automated decision-making;*

V. ***Professional responsibility**: Responsible design, scientific integrity, accuracy, multistakeholder collaboration, consideration of long-term effects;*

VI. ***Fairness and non-discrimination**: Prevention of bias, inclusiveness in design and impact, equality, representative and high-quality data;*

VII. ***Promotion of human values**: access to technology, leveraged to benefit society, human values and human flourishing;*

VIII. ***Safety and security**: Safety and security by design, reliability, predictability.*

[1555] AccessNow: Europe's approach to Artificial Intelligence: How AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 17, 2021.

[1556] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center research publication no. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

However, it is important to note that the nuances within these proposals, even though they are based on existing privacy principles, go beyond the data protection rules as we know them today. Therefore, the new approaches within the recommendations could briefly be summarized as follows:

I. ***Introduction of new obligations****, for example, an identification obligation: the latter intends to make true operators known, meaning that the institution responsible for an AI system must be made known to the public; ditto for the use of AI which could be indicated by using corresponding labels or watermarks for AI generated content. Another idea is that a termination obligation shall apply when human control of the system is no longer possible, or standardized testing procedures as accuracy of datasets is decisive for proper results;*

II. ***Enhancement and further development of existing rules****, for example, around information obligations: transparency could move away from individual-level information in the direction of publicity through the establishment of mandatory public registries or databases; another dimension of this approach is to implement traceability mechanisms and to ensure explainability as well as reproducible results;*

III. ***Widening the scope of reviews and inclusion of further values****, for example, some initiatives deal with the issue of sustainable development of AI and environmental responsibility:*[1557] *others stress the need for taking societal consequences into consideration; ditto for the respect of democratic values given various campaigns haven proven AI's potential for misinformation;*

IV. ***Establishment of a new AI regulatory function*** *that not only audits algorithms, but that acts as a repository of knowledge and this way, allows for setting (industry-specific) best practice recommendations for the public and private sector;*

V. ***Introduction of new types of certifications****, for example, by introducing mandatory certificates of fairness to show the AI system has undergone a corresponding review. This idea goes hand in hand with*

VI. ***The introduction of liability incentives****, for example, such certificates may be favorable in comparison to fines, which, in addition, only work retrospectively, i.e., when errors or damages already occurred;*

VII. ***Introduction of new individual rights****, for example, the right to participation or the right to human intervention or the right to have data replaced instead of processing restricted.*

VIII. ***Further strengthening individual rights****, for example, by establishing adequate redress mechanisms, allowing for overall contestability of AI systems, or the idea of data ownership.*

[1557] Kate Saenko: It takes a lot of energy for machines to learn – here's why AI is so power-hungry. Article published December 14 2020, available at https://theconversation.com/it-takes-a-lot-of-energy-for-machines-to-learn-heres-why-ai-is-so-power-hungry-151825. Retrieved February 28, 2023.

IX. ***Introduction of strict prohibitions****, for example, for unitary scoring, secret profiling, or facial recognition to be clear on inadmissible red lines.*

This chapter provided a detailed overview over existing recommendations, guidance, and initiatives in the context of AI at institutional, international, European, and national level. While it cannot be considered exhaustive, it showed that already by now, even though some legal initiatives have not been enacted yet, there is a variety of civil society and multistakeholder and regulator recommendations that all have in common is that they address potential issues when Big Data and AI applications are designed and implemented from a legal, accountability and liability, as well as societal, individual, and privacy perspective. While most of these initiatives are non-binding, they are promising and inspiring since they discuss new concepts, new controller obligations, and new data subject rights.

7. Future developments to consider

This chapter focuses on proposed regulations at EU level which may be relevant when AI is designed and applied, for example, the proposals for an AI Act and an AI Liability Directive, for a revised Product Liability Directive, for a renewed NIS Directive, a Cyber Resilience Act, a machinery regulation, for the European Health Data Space, or for the re-use of public sector information to only name a few. Given that international data transfers are factually often indispensable for any kind of data processing operations, the chapter furthermore deals with prerequisites and conditions for (alternative) data transfer mechanisms, potential technical solutions as well as data localization requirements. The chapter concludes with considerations about the emerging U.S. legal landscape, which is important because relevant vendors and suppliers are mostly U.S.-based.

7.1. Proposed regulations at EU level

7.1.1. Proposal for a Machinery Regulation

The proposal for a regulation of the European Parliament and of the Council on machinery products (Machinery Regulation) has been published in April 2021[1558] and shall replace the current Machinery Directive[1559] which, amongst other things, is about the protection of workers and citizens.[1560] The

[1558] The text of the Machinery Regulation is available at https://beta.op.europa.eu/en/publication-detail/-/publication/1f0f10ee-a364-11eb-9585-01aa75ed71a1. Retrieved October 17, 2021.

[1559] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (Machinery Directive) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0042#:~:text=%20Text%20%201%20Where%20a%20Member%20State,concerned%20without%20delay.%0AThe%20Commission%20shall%20consider%2C...%20More%20. Retrieved October 17, 2021.

[1560] The European Commission provides background on EU's machinery legislation at their website: https://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en. Retrieved October 17, 2021.

Machinery Directive was thus concerned with safety and health, and the Machinery Regulation is intended to complement the draft regulation on Artificial Intelligence:[1561] while the AI-relevant draft addresses risks of AI systems, the draft of a new Machinery Regulation seeks to ensure the safe integration of AI systems into machinery products such as robots or industrial production lines to safeguard users and consumers. The Machinery Regulation also seeks to provide more legal clarity and at the same time, reduce manufacturers' administrative and financial burden as companies would only need to undertake one conformity assessment for both the AI Regulation and the Machinery Regulation.[1562]

7.1.2. Proposal for a Data Governance Act

The draft Data Governance Act (DGA)[1563] focuses on the availability and sharing of data by allowing for re-use of data, by establishing providers of data sharing services as trusted (i.e. neutral) intermediaries, and by creating a European Data Innovation Board to ensure consistent practice and facilitate cooperation between the competent authorities.[1564] The DGA has been designed to be fully compliant to GDPR, however, the challenge already starts with terminology[1565]: under the Data Governance Act, data means any digital representation of acts, facts or information and any compilation of the same, including sound as well as visual or audiovisual recording. In addition, the DGA uses a novel (unique) set of terms, for example "data holder" and "data user" which is different from the terminology used in the General Data Protection Regulation.[1566] The Data Governance Act moreover introduces the idea of data altruism to make data available for altruistic purposes[1567], and it is questionable whether this truly matches GDPR's requirements with regards to purpose limitation,

[1561] European Commission press release: Europe fit for the Digital Age – Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. Press release published April 21 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682. Retrieved October 17, 2021.

[1562] European Commission press release: New rules for Artificial Intelligence – Questions and Answers. Press release published April 21 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683#3. Retrieved October 17, 2021.

[1563] The text of the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?pk_campaign=todays_OJ&pk_content=Regulation&pk_keyword=data+governance+act&pk_medium=TW&pk_source=EURLEX&uri=CELEX%3A32022R0868. Retrieved July18, 2022.

[1564] Background information on the Data Governance Act is provided by the law firm Hunton Andrews Kurth in their 2020 blog post from December 2 2020: European Commission Publishes Draft Data Governance Act, which is available at https://www.huntonprivacyblog.com/2020/12/02/european-commission-publishes-draft-data-governance-act/. Retrieved October 17, 2021.

[1565] The text of the Data Governance Act is available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:767:FIN. Retrieved October 17, 2021.

[1566] Vagelis Papakonstantinou, Paul De Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available at https://lsts.research.vub.be/en/20210401. Retrieved October 17, 2021.

[1567] Stephanie Lopes: Key insights from the leaked EU Data Governance Act. Article published November 6 2020, available at https://digitalbusiness.law/2020/11/key-insights-from-the-leaked-eu-data-governance-act/. Retrieved October 17, 2021.

transparency and consent as well as rules on compatible re-use of personal information or existing privileges for research purposes. In this context, the European Data Protection Supervisor and the European Data Protection Board adopted a joint opinion on the DGA[1568] in which they recommend aligning the Data Governance Act with present (GDPR) rules on the protection of personal data to ensure that the level of protection of individuals' personal data is not affected, and that obligations set out in applicable data protection legislation are not altered. They furthermore suggest clarifying the data altruism purposes and to define compatible purposes for which further processing of personal information may be lawful. In light of possible risks for data subjects related to the processing of their personal information by data sharing service providers or data altruism organizations, the EDPS and the EDPS consider that envisaged requirements for these entities are not sufficient; the EDPS and the EDPS therefore recommend exploring alternatives such as codes of conduct or certification mechanisms.[1569] The DGA foresees the establishment of a European Data Innovation Board,[1570] together with the two other bodies foreseen by the DSA and the DMA, which altogether creates three new oversight bodies. As much as oversight, enforcement and governance shall be welcomed, this results a multiplicity of supervisors on top of national data protection, consumer protection and competition regulatory agencies – as well as courts[1571] that deal with individual claims[1572] or competition[1573] or antitrust cases.[1574] As part of the trialogue discussions, a political agreement on the DGA was reached between the European Parliament and the Council of the European Union in November 2021.[1575]

[1568] EDPB's and EDPS' joint opinion on the Data Governance Act published March 10 2021, available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinion-data-governance-act-dga_en. Retrieved October 17, 2021.

[1569] EDPB's and EDPS' joint opinion on the Data Governance Act published March 10 2021, available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinion-data-governance-act-dga_en. Retrieved October 17, 2021.

[1570] European Council press release: Council approves Data Governance Act. Press release published May 16 2022, available at https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/. Retrieved October 17, 2021.

[1571] Vincent Manancourt: Have a GDPR complaint? Skip the regulator and take it to court. Article published August 30 2020, available at https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/. October 17, 2021.

[1572] Lars Lensdorf, Robert Henrici, Moritz Hüsch, Nicholas Shepherd: A new day for GDPR damages claims in Germany? Article published February 25 2021, available at https://www.insideprivacy.com/data-privacy/a-new-day-for-gdpr-damages-claims-in-germany/. Retrieved October 17, 2021.

[1573] Daniel Heymann: DSGVO und UWG – Wettbewerbsrecht und Datenschutz. Article published July 26 2019, available at https://www.petersenhardrahtpruggmayer.de/de/news/dsgvo-und-uwg-wettbewerbsrecht-und-datenschutz/. Retrieved October 17, 2021.

[1574] Eva Witzleb, Pascal Schumacher: Datenschutz vs. Kartellrecht - Die nächste Runde. Article published May 6 2021, available at https://www.noerr.com/de/newsroom/news/datenschutz-vs-kartellrecht. Retrieved October 17, 2021.

[1575] European Parliament press release: Data governance – Parliament approves new rules boosting intra-EU data sharing. Press release published April 6 2022, available at https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users. Retrieved July 22, 2022. This agreement was formally approved by the Parliament in April 2022; it enters into force after formal adoption by the Council and 15 months after publication in the Official Journal.

7.1.3. Proposal for a Data Act

The European Commission proposed the Data Governance Act as part of the European Strategy for data,[1576] and the Data Act[1577] is a follow up on that proposal with the objective "to propose measures to create a fair data economy by ensuring access to and use of data, including in business-to-business and business-to-government situations."[1578] Under this initiative, a review of Directive 96/9/EC on the legal protection of databases is also planned in order to ensure continued relevance for the data economy."[1579] The proposed Data Act wants to encourage sharing of data – including non-personal information[1580] – to realize the full potential of EU's data economy by:[1581] promoting fairness (i.e., ensuring fair distribution of usage rights along the value chain; identifying contractual unfairness where there is unequal bargaining power compromising competition), by enabling for greater legal certainty (i.e. safeguarding intellectual property rights; clarifying if database rights can cover machine-generated data; ensuring that the rights under the Database Directive do not impede cross-border data flows and data sharing), and by ensuring portability (i.e. introducing (mandatory?) interoperability requirements in order to allow for easy switching of providers without contractual, technical and / or economic barriers. This legal initiative would thus allow for addressing certain problems that limit data sharing at present: lack of legal clarity, lack of economic incentives, lack of trust and fear of misappropriation by third parties and imbalances in negotiating power.[1582] In the context of data economy, the proposed Data Act was criticized because of its potential clash with the GDPR as some believe that EU citizens could end up with less protection of their data rights,[1583] and the proposal would furthermore need to be coordinated with other legislative measures, such as intellectual property rights or trade secrets.[1584] The Commission

[1576] Background information on the European Strategy for data including the Data Governance Act is provided at the Commission's website, available at https://digital-strategy.ec.europa.eu/en/policies/strategy-data. Retrieved October 19, 2022.

[1577] The text of the proposal for a regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN. Retrieved October 17, 2021.

[1578] Details on the Data Act are provided at the Commission's website, available at https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act. Retrieved October 17, 2021.

[1579] Commission statement in the framework of the public consultation, available at https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act. Retrieved October 17, 2021.

[1580] Trisha Jalan: European Commission proposes Data Act 2021 to increase data sharing between businesses and governments. Article published February 21 2020, available at https://www.medianama.com/2020/02/223-european-commission-data-sharing/. Retrieved October 17, 2021.

[1581] Seiko Hidaka: EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? Article published July 5 2021, available at https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/. Retrieved October 17, 2021.

[1582] Seiko Hidaka: EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? Article published July 5 2021, available at https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/. Retrieved October 17, 2021.

[1583] Douglas Clarke-Williams: Finnish decision foreshadows GDPR and Data Act clash. Article published June 10 2022, available at https://globaldatareview.com/article/finnish-decision-foreshadows-gdpr-and-data-act-clash. Retrieved July 20, 2022.

[1584] Europe's Commissioner for the Internal Market, Thierry Breton said that "The Data Act will unlock vast troves of industrial data and contribute to the emergence of a sovereign single market for data. European data, in published an impact assessment on the Data Act,[1585] and the EDPB and the EDPS issued a joint opinion[1586] on the Data Act in which they raise concerns with regards to the governance architecture in the proposal, for example, the fact that the Data Act[1587] might lead to forum shopping because it does not provide a consistency mechanism or harmonized penalties, or the fact that the relationship between competent authorities remains unclear.[1588]

7.1.4. Proposal for a Digital Services Act

As part of the European Union's digital strategy, the European Commission published[1589] the Digital Services Act package which consists of the Digital Services Act (DSA) and the Digital Markets Act (DMA) in late 2020. DSA and DMA intend to regulate the provision of services over the Internet,[1590] the Digital Services Act and the Digital Markets Act have two main goals:[1591] "to create a safer digital space in which the fundamental rights of all users of digital services are protected, and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally." The Digital Markets Act foresees the creation of a Digital Markets Advisory Committee[1592], and the Digital Services Act provides for the establishment of a European Board for

particular industrial data, needs to be shared, stored and processed in line with European rules such as data protection, respect of intellectual property and trade secrets." Source: https://data.europa.eu/en/news/public-consultation-data-act. Retrieved October 17, 2021.

[1585] Torsten Kraul, Max von Schönfeld, Marvin Bartels: Europäische Datenstrategie: EU-Kommission veröffentlicht Folgenabschätzung zum Data Act. Article published June 24 2021, available at https://www.noerr.com/en/insights/european-data-strategy-eu-commission-publishes-impact-assessment-on-the-data-act. Retrieved October 17, 2021.

[1586] EDPB-EDPS joint opinion 2/2022 on the proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) published on May 4 2022, available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en. Retrieved December 29, 2022.

[1587] The draft legislation has been adopted on March 14 2023, see European Parliament press release dated March 2023: Data Act – MEPs back new rules for fair access to and use of industrial data, available at https://www.europarl.europa.eu/news/en/press-room/20230310IPR77226/data-act-meps-back-new-rules-for-fair-access-to-and-use-of-industrial-data. Retrieved March 20, 2023.

[1588] Background information on the joint opinion is provided by Toby Headdon, Hannah Crowther: Two worlds collide: the Data Act proposal v GDPR. Article published June 14 2022, available at https://www.bristows.com/news/two-worlds-collide-the-data-act-proposal-v-gdpr/. Retrieved December 20, 2022.

[1589] Commission press release: Europe fit for the Digital Age: proposes new rules for digital platforms. Press release published December 15 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347. Retrieved October 17, 2021.

[1590] Vagelis Papakonstantinou, Paul De Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available at https://lsts.research.vub.be/en/20210401. Retrieved October 17, 2021.

[1591] The European Commission provides background information on these legal initiatives at their website, available at https://ec.europa.eu/digital-single-market/en/digital-services-act-package. Retrieved October 17, 2021.

[1592] Details on Digital Markets Act as well as the bill text are provided by the European Commission at their website, available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Retrieved January 29, 2023.

Digital Services,[1593] meaning that new bodies are created at EU level. The DSA applies to intermediary services offering network infrastructure such as Internet access providers and hosting (including cloud) services as well as online platforms and will replace the e-Commerce directive which was adopted in 2000.[1594] Since the Digital Services Act will modernize the e-Commerce Directive that many consider to be the "backbone of EU's Internet legislation",[1595] this initiative represents a major reform of European Internet regulations.[1596] Amongst other things, i.e. from a data subject perspective, the DSA introduces requirements such as enhanced online advertising transparency requirements, notice and action mechanisms, certain safeguards and the possibility to challenge platforms' content moderation decisions.[1597] The European Data Protection Supervisor welcomed the initiative but at the same time stressed the importance of protecting individuals, for example from targeted online advertising or from automated decision making and profiling in the framework of so-called recommender systems.[1598] The European Parliament adopted the Digital Services Act in July 2022:[1599] it imposes a ban on dark patterns and online advertising activities targeting minors, or those based on sensitive personal data, and introduces strict obligations for very large online platforms and very large online search engines[1600] such as the establishment of an independent compliance function, yearly independent audits, systemic risks assessments as regards the design, functioning and use of their services, including algorithmic systems, or granting access to data to the authorities for the purposes of monitoring and assessing compliance with the DSA, including the explanation of the logic, design, testing and functioning of algorithmic systems.[1601]

[1593] Background information on the Digital Services Act including the bill text are provided by the European Commission, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en. Retrieved October 17, 2021.

[1594] Victor Timon, Helen Hart: EU plans changes to e-commerce and competition law. Article published June 10 2020, available at https://www.lewissilkin.com/en/insights/eu-plans-changes-to-e-commerce-and-competition-law. Retrieved October 17, 2021.

[1595] Christoph Schmon: Our EU policy principles: platform liability. Article published July 9 2020, available at https://www.eff.org/deeplinks/2020/07/effs-eu-policy-principles-platform-liability-and-monitoring. Retrieved October 17, 2021.

[1596] Christoph Schmon, Karen Gullo: Euopean's Commission proposed Digital Services Act, got several things right, but improvements are necessary to put users in control. Article published December 15 2020, available at https://www.eff.org/deeplinks/2020/12/european-commissions-proposed-regulations-require-platforms-let-users-appeal. Retrieved October 17, 2021.

[1597] The European Commission explains DSA requirements at their website, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Retrieved October 17, 2021.

[1598] EDPS statement on the Digital Services Package and Data Strategy published November 18 2021, available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en. Retrieved December 20, 2021.

[1599] European Parliament press release: Digital Services – landmark rules adopted for a safer, open online environment. Press release published July 5 2022, available at https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment. Retrieved July 22, 2022.

[1600] Those reaching an average of 45 million or more monthly active users in the EU and designated as such by the Commission.

[1601] Dan Cooper, Laura Somaini, Sam Jungyun Choi: European Parliament adopts DSA. Article published July 6 2022, available at https://www.insideprivacy.com/european-union-2/european-parliament-adopts-dsa/. Retrieved July 22, 2022.

7.1.5. Proposal for a Digital Markets Act

The DMA applies to organizations which qualify as so-called gatekeepers, for example, search engines, social networking and video-sharing platforms, online intermediation services, and cloud computing services, and aims at ensuring a higher degree of competition and a fairer business environment.[1602] The Digital Markets Act and Digital Services Act both have extraterritorial effect, and the DMA will require gatekeepers to refrain from unfair behaviors such as blocking users from uninstalling any pre-installed software or apps or restricting users from accessing services that may have been acquired outside of the gatekeeper's platform.[1603] The Digital Markets Act will furthermore ban the combination and cross-use of personal data collected during the use of a service for the purposes of another service offered by the gatekeeper[1604], ensure access for business users to their marketing or advertising performance data as well as effective portability and continuous and real-time access to data provided or generated by end users, complementing the GDPR's right to (personal) data portability.[1605] The EDPS underlined that the DMA should enhance consent mechanisms, clarify the scope of the data portability obligation, consider effective anonymization, and introduce (minimum) interoperability standards,[1606] and once again called for a structured approach between all authorities responsible for compliance with the Digital Services Act, the Digital Markets Act as well as all other applicable regulations. As part of the trialogue discussions, a provisional political agreement[1607] was reached between the European Parliament and the Council of the European Union in March 2022.

[1602] DMA requirements are summarized by the European Commission at their website, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Retrieved October 17, 2021.

[1603] The law firm of Hunton Andrews Kurth commented on the DMA in their 2021 blog post: EDPS Publishes Opinion on Digital Services Act and Digital Markets Act. Article published February 17 2021, available at https://www.huntonprivacyblog.com/2021/02/17/edps-publishes-opinion-on-digital-services-act-and-digital-markets-act/. Retrieved October 17, 2021.

[1604] Sebastian Louven: Digital Markets Act – Verbot der Datenzusammenführung. Article published July 20 2022, available at https://www.cr-online.de/blog/2022/07/20/digital-markets-act-verbot-der-datenzusammenfuehrung/.
Retrieved July 30, 2022.

[1605] Jetty Tielemans: EU data initiatives in context. Infographic published (last updated) March 22, available at https://iapp.org/resources/article/infographic-recent-eu-data-initiatives-in-context/?mkt_tok=MTM4LUVaTS0wNDIAAAGFbmT22pIZgQLYKokUEfduUMWT7bFxo5xvWxumwh--7YEQwlsG4QbKMQD-kqpMdUBMkR8dCpMAoXQzsLORoDI7IY507c26mwLwi8YYxQBk-B24. Retrieved July 22, 2022.

[1606] EDPS Opinion2/202 on the proposal for a Digital Markets Act is published February 20 2021, available at https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf.

[1607] European Parliament press release: Deal on Digital Markets Act: EU rules to ensure fair competition and more choice for users. Press release published March 24 2022, available at https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users. Retrieved July 22, 2022.

7.1.6. Proposal for a Directive on Copyright

In early 2019, the European Parliament, the Council of the EU and the Commission agreed on new copyright rules[1608] in order to be fit for the digital era and bring tangible benefits to all creative sectors, such as the press, researchers or cultural heritage institutions as well as citizens.[1609] The proposal turns the established notice-and-takedown-principle on its head and introduces a new platform liability regime: service providers have to take certain efforts to ensure the unavailability of copyright protected work, and one of the solutions for this purpose are so-called upload filters. This sounds like a fair distribution of revenues from the online use of copyright works to the benefit of creators and publishers. But this initiative faced a lot of criticism[1610] as it is feared that any such filtering might lead to censorship or even guardianship and disenfranchisement of users as well as further strengthening of data monopolies. Smaller platforms, due to cost and efforts involved with the implementation of upload filters, will likely use centralized filtering mechanisms offered by third parties, i.e., companies which already invested time and money in corresponding technology. Some thus believe that, by requiring Internet platforms to perform automatic filtering all of the content that is uploaded by individuals, this may lead to a transformation of the Internet from an open platform into a tool for automated surveillance and control.[1611] Given the specific technology needed for such filters and owing to the fact that a volume of data has to be processed, it seems likely that a huge part of the data traffic will run through the hands of a few large providers,[1612] which is why some fear that this would lead to the emergence of a data oligopoly.[1613] Another concern is that, because content filter technology is costly, small platforms might opt for data-for-service collaborations with Big Tech players in such a way that user data is offered in return for filtering services – an agreement that would probably be justified by the fact that a compliance requirement must be met. Finally, one further option has already been communicated by certain content-

[1608] The text of the proposal for a copyright directive is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0593:FIN. Retrieved October 17, 2021.

[1609] European Commission press release: Digital Single Market – EU negotiators reach a breakthrough to modernise copyright rules. Press release published February 13 2029, available at http://europa.eu/rapid/press-release_IP-19-528_en.htm. Retrieved October 17, 2021.

[1610] An overview over the debate is provided by the Electronic Frontier Foundation, available at https://www.eff.org/de/deeplinks/2018/06/internet-luminaries-ring-alarm-eu-copyright-filtering-proposal. Retrieved October 17, 2021.

[1611] More than 70 Internet and computing luminaries including Tim Berners-Lee and co-founders of Mozilla, Wikipedia and many other have spoken out against this concrete provision. On June 12 2018, they wrote a joint letter for president of the European Parliament, which is available at https://www.eff.org/files/2018/06/13/article13letter.pdf. Retrieved October 17, 2021.

[1612] Statement by Ulrich Kelber, Germany's Federal Data Protection Commissioner, who concludes that upload filters are "dangerous and wrong", see Michael Schäfer: EU-Urheberrechtsreform – Kelber bekräftigt Ablehnung von Upload-Filtern. Article published March 16 2019, available at https://www.computerbase.de/2019-03/eu-urheberrechtsreform-kelber-ablehnung-upload-filtern/. Retrieved October 17, 2021.

[1613] Intersoft Consulting Services: EU-Urheberrechtsreform: Upload-Filter und Datenschutz. Article published March18 2019, available at https://www.datenschutzbeauftragter-info.de/eu-urheberrechtsreform-upload-filter-und-datenschutz/. Retrieved October 17, 2021.

service-providers: the exclusion of European users with the help of so-called Geo-Blocking.[1614] Moreover, filters will have to be programmed in a manner to also take into consideration relevant specific legal exceptions such as quotations, criticism, or parody[1615] to function properly. They will also be able to distinguish whether film material was used by a film critic, which is legal, or by a user attempting to illegally distribute the film, which is inadmissible. Either way – the collection of such meta-data leads to the fact that platforms using such filters would be considered controllers that process personal data.[1616] The question that arises in this context is the legality of such processing activities and the compatibility of centralized filtering mechanisms with the Charta of Fundamental rights. In line with the principle of proportionality laid down in Article 52 (1) of the Charta, the Regulation requires all legal obligations to be proportionate with respect to the legitimate aim which is pursued.[1617] But if one compares the filtering obligation under Article 17 (4b, c) of the Copyright Directive to existing CJEU case law with regard to fundamental rights as stipulated in Article 7 (the right to private life) and Article 8 (the right to protection of personal data) of the Charta, it is questionable whether the obligation to use upload filters meets the requirements of a balance between the right to intellectual property, the freedom to conduct business and the right to protection of personal data.[1618] In the famous Schrems decision,[1619] the CJEU stressed that legislation which grants public bodies generalized access to the content of communication violates both, the principle of proportionality and the right to private life. The CJEU concluded that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter." Since the Copyright Directive deals with the processing of communication between a user and the platform, some claim that this directive may conflict with the freedom of expression because copyright mechanisms do not respect fair use as they are often unable to recognize parody or quotation, i.e., existing freedoms and / or legal

[1614] Twitch's CEO brought the exclusion of EU users into play. Statement published April 3 2019, available at https://www.golem.de/news/uploadfilter-twitch-erwaegt-ausschluss-von-eu-nutzern-1904-140416.html?utm_source=nl.2019-04-03.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter. Retrieved October 17, 2021.

[1615] Today's upload filter technology does not seem to be able to recognize parody. Challenges with upoload filters are summarized by Eva Simon: Upload filters are back, and we are strongly against them. Article published November 3 2020, available at https://www.liberties.eu/en/stories/uploa-filter-back-eu-2020/18938 . Retrieved December 20, 2022.

[1616] Sebastian Louven, Malte Engeler: Copyright Directive – does the best effort principle comply with GDPR? Article published March 23 2019, available at https://www.telemedicus.info/copyright-directive-does-the-best-effort-principle-comply-with-gdpr/. Retrieved October 17, 2021.

[1617] See GDPR Article 6 (3).

[1618] In their article, Sebastian Louven and Malte Engeler argue that the filtering obligation in the Copyright Directive violates the Charta: Copyright Directive – does the best effort principle comply with GDPR? Article published March 23 2019, available at https://www.telemedicus.info/copyright-directive-does-the-best-effort-principle-comply-with-gdpr/. Retrieved October 17, 2021.

[1619] Recital 94 of the decision available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN. Retrieved October 17, 2021.

exceptions.[1620] Another problem is that the CJEU addressed public bodies, but the Copyright Directive takes private companies into duty, this way shifting the protection of individual freedoms to the private sector or, rather algorithms that shall have the capacity to decide upon the admissibility of uploading content.

7.1.7. Proposal for a renewed NIS Directive

Only two years after its implementation, the EU Commission proposed[1621] an update of the Directive on Security of Network and Information Systems, also known as "NIS2 Directive". Like the present Directive on Security of Network and Information Systems, the new NIS2 Directive aims at strengthening security requirements, but it also aims at streamlining reporting obligations and introduces more stringent supervisory measures and stricter enforcement requirements, including harmonized sanctions across the EU, and furthermore addresses the management of supply chains risks.[1622] The current NIS Directive[1623] (also known as the Cyber-security Directive) applies to operators of essential services such as water supply or energy as well as digital service providers, including providers of cloud computing services and online services. The present NIS Directive has been criticized for its scope and application,[1624] and the proposed[1625] NIS2 Directive takes up this criticism and does not distinguish between operators of essential services and digital service providers: it expands the scope of the present Directive by adding new sectors in accordance with their criticality for the economy and society. Cloud service providers are now categorized as essential entities, which is a major change and adds to the fact that the use of cloud computing for Big Data and AI is governed by many data privacy and security laws. Moreover, fines of up to 10 million Euro or 2 % of the total worldwide turnover (whichever is

[1620] Timothy Vollmer: Copyright filtering mechanisms don't (and can't) respect fair use. Article published February 22 2017, available at https://creativecommons.org/2017/02/22/copyright-filtering-mechanisms-dont-cant-respect-fair-use/. Retrieved October 17, 2021.

[1621] Background information is provided by the European Commission at https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union. Retrieved October 17, 2021.

[1622] Mar Negreiro: The NIS2 Directive: A high common level of cybersecurity in the EU. Article published February 22 2021, available at https://epthinktank.eu/2021/02/22/the-nis2-directive-a-high-common-level-of-cybersecurity-in-the-eu-eu-legislation-in-progress/. Retrieved October 17, 2021.

[1623] The text of the Directive on Security of Network and Information Systems is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. Retrieved October 17, 2021.

[1624] Matthew Buckwell: EU Commission proposes to update the NIS/Cybersecurity Directive only two years after implementation. Article published January 2021, available at https://www.twobirds.com/en/news/articles/2021/global/eu-commission-proposes-to-update-the-nis-cybersecurity-directive-only-two-years-after-implementation. Retrieved October 17, 2021.

[1625] Dora Petranyi, Marton Domokos: EU adopts NIS2 directive to enhance cybersecurity and resilience. Article published January 4 2023, available at https://www.cms-lawnow.com/ealerts/2023/01/eu-adopts-nis2-directive-to-enhance-cybersecurity-and-resilience. Retrieved January 7, 2023.

higher) are foreseen, and non-compliant entities risk that their relevant authorizations are suspended or have senior management suspended from exercising managerial functions.[1626]

7.1.8. Proposal for a Directive on the Resilience of Critical Entities

The proposed NIS2 Directive should not be seen in isolation, but in the context[1627] of other initiatives to enhance the resilience of critical systems, and for which the European Union established the European Program for Critical Infrastructure Protection (EPCIP) already in 2006[1628] with the overall goal to increase the level of security and decrease the number and severity of incidents including data breaches. Consequently, the European Commission proposed another directive to replace the current Critical Infrastructure Directive,[1629] the Directive on the resilience of critical entities:[1630] under this directive EU Member States must, among other things, designate authorities, identify nationally critical infrastructures and services and evaluate their vital functions which are in scope of the directive; critical entities would be subject to specific oversight and would have to implement appropriate technical and organizational measures and conduct risk assessments.[1631]

7.1.9. Proposal for a Cyber Resilience Act

The proposal for a "Regulation on horizontal cybersecurity requirements for digital products and ancillary services" (Cyber Resilience Act)[1632] has been proposed against the background that hardware and software products are increasingly subject to successful cyberattacks, which may be due to a variety of reasons, ranging from insufficient user knowledge, preventing users from either choosing products with appropriate cybersecurity properties or using products in a secure manner, to inadequate and / and

[1626] Thomas Declerck: New EU Cybersecurity Strategy: European Commission accelerates push for EU to lead in cybersecurity regulation. Article published December 24 2020, available at https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/. Retrieved October 17, 2021.

[1627] Background information is provided by the European Commission's in their roadmap and impact assessment information published June 25 2020, available at https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/06/090166e5d0c95543-1.pdf. Retrieved October 17, 2021.

[1628] Commission communication on a European Programme for Critical Infrastructure Protection published December 12 2006, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33260&from=EN. Retrieved October 17, 2021.

[1629] The text of the current European Critical Infrastructure Directive is available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. Retrieved October 17, 2021.

[1630] Text of the proposed Directive on the resilience of critical entities is available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_impact_assessment_swd-2020-358_en.pdf. Retrieved October 17, 2021.

[1631] Further details are provided on the European Commission's website available at https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en. Retrieved October 17, 2021.

[1632] The text of the proposed Cyber Resilience Act is available at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act#:~:text=Cyber%20Resilience%20Act%20The%20proposal%20for%20a%20regulation,to%20ensure%20more%20secure%20hardware%20and%20software%20products. Retrieved December 29, 2022.

inconsistent provision of security updates which cause vulnerabilities, or.[1633] From a legal perspective, the problem was that, while "existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs."[1634] This new proposal is highly relevant in practice, because products with digital elements are on the rise, consequently, "new cybersecurity requirements would apply to all products that are either directly or indirectly connected to another device or network, including non-embedded software. Heightened requirements would apply to critical and highly critical products with digital elements. Requirements would include providing security support, software updates, and enhanced consumer information and transparency."[1635]

7.1.10. Proposal for a Cyber Solidarity Act

The proposal for a "Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents" (Cyber Solidarity Act)[1636] has been published in April 2023. The Cyber Solidarity Act wants to establish a "European Cyber Shield" and focuses on incident detection, response capabilities, and situational awareness. It aims to improve the cyber resilience of critical entities, to promote information sharing about cyber incidents and vulnerabilities, and to create an EU-wide resource for incident management.[1637] The CSA will moreover promote the establishment of cross-border Security Operation Centers that shall serve as hubs for the collection and analysis of information on cybersecurity threats, incidents and tools from public bodies and private entities, and requires the European Commission to populate an "EU Cybersecurity Reserve" comprising a bench of "trusted providers" of private managed security services.[1638] In addition, the CSA requires private providers of

[1633] An overview of common cybersecurity threats is provided by the Open Web Application Security Project in their report: OWASP Top 10 Vulnerabilities in 2022. Report published May 2022, available at https://owasp.org/Top10/. Retrieved December 29, 2022.

[1634] Background information on the Cyber Resilience Act is provided by the European Commission, available at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act#:~:text=Cyber%20Resilience%20Act%20The%20proposal%20for%20a%20regulation,to%20ensure%20more%20secure%20hardware%20and%20software%20products. Retrieved December 29, 2022.

[1635] Jenny Gesley: European Union: Commission proposes new cybersecurity rules for products with digital elements. Article published December 2 2022, available https://www.loc.gov/item/global-legal-monitor/2022-12-01/european-union-commission-proposes-new-cybersecurity-rules-for-products-with-digital-elements/. Retrieved December 29, 2022.

[1636] The EU Cyber Solidarity Act is available at https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act. Retrieved May 5, 2023.

[1637] Background information on the proposed EU Cyber Solidarity Act has been provided by the European Commission in their Questions and Answers: Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience. Q&As published April 18 2023, available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_2244. Retrieved May 5, 2023.

[1638] Mark Young, Paul Maynard, Anna Oberschelp de Meneses: Three interesting features of the proposed EU Cyber Solidarity Act. Article published April 29 2023, available at managed security services to support member states in the response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents and the CSA foresees the testing of certain entities that are subject to NIS2 for potential vulnerabilities based on EU risk assessments.[1639] As a result, the Cyber Solidarity Act adds another layer to the increasingly complicated legal landscape of EU cybersecurity laws, and it remains to be seen how the CSA will intersect with other legal initiatives such as the revised Network and Information Security Directive, the Cyber Resilience and Cybersecurity Act.

7.1.11. 5G Security and Internet of Secure Things

As part of their cyber-security strategy, the European Union is also dealing with IoT and 5G, which many believe to be the next big[1640] thing despite increased infrastructure cost: this future mobile network will allow for better performance by processing a much higher volume of data and by connecting more devices to a single source,[1641] and connectivity and capacity are key to Big Data applications. This initiative shows that the EU wants to lead efforts for a secure digitalization[1642] and that there is awareness of the importance of security and resilience of IoT and investment in trustworthy digital technologies: this is truly needed since the number of cyber-attacks continues to rise and because society's digital transformation has been intensified by the COVID-19 crisis.[1643] The importance of security cannot be stressed enough: a hack by researchers affected numerous car manufacturers like BMW, Ferrari, Ford, Honda, Hyundai, Infiniti, Jaguar, Land Rover, Mercedes-Benz, Nissan, Porsche, Rolls Royce, Toyota, and others showed truly critical vulnerabilities, because it was possible to take full (remote) control over user accounts, access personal data, change ownership, or lock users out, to only name a few of the detected problems.[1644]

https://www.insideprivacy.com/cybersecurity-2/stronger-cybersecurity-reducing-cyber-incidents-greater-eu-strategic-autonomy-three-interesting-features-of-the-proposed-eu-cyber-solidarity-act/. Retrieved May 5, 2023.

[1639] Mark Young, Paul Maynard, Anna Oberschelp de Meneses: Three interesting features of the proposed EU Cyber Solidarity Act. Article published April 29 2023, available at https://www.insideprivacy.com/cybersecurity-2/stronger-cybersecurity-reducing-cyber-incidents-greater-eu-strategic-autonomy-three-interesting-features-of-the-proposed-eu-cyber-solidarity-act/. Retrieved May 5, 2023.

[1640] Gina Roos: 5G – the next big thing is here. Article published September 25 2020, available at https://www.electronicproducts.com/5g-the-next-big-thing-is-here/. Retrieved October 17, 2021.

[1641] Rohith Bhaskar: 5G: Why is it the next big thing? Article published February 22 2021, available at https://www.moneycontrol.com/news/technology/5g-why-is-it-the-next-big-thing-6555881.html. Retrieved October 17, 2021.

[1642] Thomas Declerck: New EU Cybersecurity Strategy: European Commission accelerates push for EU to lead in cybersecurity regulation. Article published December 24 2020, available at https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/. Retrieved October 17, 2021.

[1643] Information on EU's cyber-security strategy is provided by the European Commission, available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Retrieved October 17, 2021.

[1644] Sam Curry: Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More. Article published January 3 2023, available at https://samcurry.net/web-hackers-vs-the-auto-industry/. Retrieved January 4, 2023.

7.1.12. Proposal for a review of the Directive on the Re-use of Public Sector Information

In the framework of Big Data discussions and the use of Artificial Intelligence in Industry 4.0, people tend to forget that not only Big Tech companies are data-driven; truth is, the public sector is one of the most data-intensive sectors. This erroneous perception is confirmed by the fact that this proposal attracted much less attention in contrast to the proposal for a copyright reform. The reason for this new proposal was the intention to create a "common data space"[1645] within the European Union, and consequently, the European Commission adopted a new proposal[1646] for a revision of the PSI Directive. This proposal aims to overcome existent (market entry) barriers which prevent the re-use of public sector information, especially for data which are generated by utilities and the transport sector as well as research data resulting from public funding. Such (real-time) data has tremendous re-use potential, and that is particularly true for dynamic data since this type of data is believed to be one of the most commercially valuable types of data.[1647] Due to the fact that the proposal suggests a full re-use of public sector information, it is questionable how this relates to the principle of purpose limitation GDPR sets forth. The protection of personal data is recognized as a fundamental right and therefore, it cannot be simply overruled. But the proposal addresses this problem as it provides for an exception to the scope of the PSI Directive for reasons relating to the protection of personal data.[1648] However, problems may arise given that other terms are used[1649] and because definitions of terms are not the same.[1650] It was moreover suggested to introduce mandatory data protection impact assessments for specific sectors dealing with sensitive data such as the health sector which take the conditions for re-use into account.[1651] Even though further developments have to be awaited, it seems already clear at this stage that certain (foreseeable) challenges prevail in the context of re-use of public sector information, for example, the potential weakening of purpose limitation and the risk of loss of transparency.

[1645] Details are provided by the European Commission, available at https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive. Retrieved October 17, 2021.

[1646] The proposal for a directive on the re-use of public sector information is available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0234:FIN. Retrieved October 17, 2021.

[1647] The European Commission provides further background information on the initiative at their website https://digital-strategy.ec.europa.eu/en/policies/psi-open-data. Retrieved October 17, 2021.

[1648] See article 1 (2 g) of the PSI proposal.

[1649] For instance, the term document. GDPR does not address documents, but personal data.

[1650] EDPS opinion 5/2018 on the proposal for a Directive on the re-use of Public Sector Information (PSI), published July 10 2018, available at https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf. Retrieved October 17, 2021.

[1651] EDPS opinion 5/2018 on the proposal for a Directive on the re-use of Public Sector Information (PSI), published July 10 2018, available at https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf. Retrieved October 17, 2021.

7.1.13. Proposal for a Public Sector Interoperability Act

Another initiative is important in the context of the use and handling of public sector information: In late 2022 the European Commission adopted a proposal[1652] for an "Interoperable Europe Act" to reinforce the interoperability of the public sector in the EU. It aims to enhance the ability of administrations to cooperate and make public services function across borders, sectors, and organizations, in brief: make EU legislation fully digital-ready and interoperable-by-design.[1653] The Commission published Questions and Answers on the proposal,[1654] and a press release[1655] in which the Commission explains that the Interoperable Europe Act introduces:

- *"A structured EU cooperation where public administrations, supported by public and private actors, come together in the framework of projects co-owned by Member States, as well as regions and cities;*
- *Mandatory assessments to evaluate the impact of changes in information technology (IT) systems on cross-border interoperability in the EU;*
- *The sharing and reuse of solutions, often open source, powered by an 'Interoperable Europe Portal' – a one-stop-shop for solutions and community cooperation;*
- *Innovation and support measures, including regulatory sandboxes for policy experimentation, GovTech projects to develop and scale up solutions for reuse, and training support."*

7.1.14. Proposal for a European Health Data Space

In early 2022, the European Commission published a proposal[1656] for the creation of the "European Health Data Space" (EHDS). If adopted, the proposal would foresee the creation of an EU-wide

[1652] The text of the proposal for a regulation of the European Parliamant and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) is available at https://op.europa.eu/en/publication-detail/-/publication/f53505b9-672f-11ed-b14f-01aa75ed71a1/language-en. Retrieved January 4, 2023.

[1653] Athina Chroni: Why is the Interoperable Europe Act proposal important for digital-ready policymaking and our community? Article published December 20 2022, available at https://joinup.ec.europa.eu/collection/better-legislation-smoother-implementation/news/interoperable-europe-act-proposal-and-digital-ready-policymaking#:~:text=On%2018%20November%202022%20the%20European%20Commission%20adopted,public%20services%20function%20across%20borders%2C%20sectors%20and%20organizations. Retrieved January 4, 2023.

[1654] European Commission: Questions and Answers: Interoperable Europe Act published November 21 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6908. Retrieved January 7, 2023.

[1655] European Commission press release: New Interoperable Europe Act to deliver more efficient public services through improved cooperation between national administrations on data exchanges and IT solutions published November 21 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6907. Retrieved January 7, 2023.

[1656] The text of the proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197&from=EN. Retrieved July 30, 2022.

infrastructure[1657] that allows to link health data sets for practitioners, researchers, and industry.[1658] The proposal aims to facilitate the creation of a "European Health Union" and to "enable the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data."[1659] The European Commission stresses the aim of creating an "internal market for personal health data and digital health products and services" by promoting "the free, cross-border flows of personal data."[1660] The European Data Protection Board and the European Data Protection Supervisor issued a joint opinion[1661] on the EHDS proposal which expresses concerns in relation to the proposal from a data protection perspective, which underlines that the secondary use of personal information shall be subject to prior consent of the data subject. The EDPB Chair said that the description of individuals' rights the proposal is not consistent with the GDPR and that it is of utmost importance that data subject rights are by no means undermined by this proposal, and that there may be a substantial risk of legal uncertainty if the interplay of the different rights between the proposal and the GDPR is not clarified. [1662] The EDPS Supervisor added that health data processed by wellness apps may reveal particularly sensitive information such as religious orientation and that digital health applications should therefore be excluded from being made available for secondary use.[1663] The fact that the use of health data may even put individuals at risk of prosecution shows that this type of information truly is of sensitive nature.[1664]

[1657] However, not all Member States are maintaining electronic patient records, meaning that corresponding steps towards digitalization would be a prerequisite.

[1658] The law firm Kinast reports on the EHDS in their July 21, 2022 blog post: The Commission's Proposal for the European Health Data Space raises data protection concerns, available at https://www.privacy-ticker.com/the-commissions-proposal-for-the-european-health-data-space-raises-data-protection-concerns/. Retrieved July 30, 2022.

[1659] EDPB: European Health Data Space must ensure strong protection for electronic health data published May 3 2022, available at https://edpb.europa.eu/news/news/2022/european-health-data-space-must-ensure-strong-protection-electronic-health-data_en. Retrieved July 30, 2022.

[1660] EC's corresponding "Communication from the Commission - A European Health Data Space: harnessing the power of health data for people, patients and innovation" published May 3 2022, available at https://health.ec.europa.eu/publications/communication-commission-european-health-data-space-harnessing-power-health-data-people-patients-and_en. Retrieved July 30, 2022.

[1661] Joint opinion of the European Data Protection Board and the European Data Protection Supervisor on the Joint Opinion on the European Commission's Proposal for the European Health Data Space published on July 12 2022, available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en. Retrieved July 30, 2022.

[1662] Statement of the EDPB chair published July 14 2022, available at https://edpb.europa.eu/news/news/2022/european-health-data-space-must-ensure-strong-protection-electronic-health-data_en. Retrieved July 30, 2022.

[1663] Statement of the EDPS supervisor published July 14 2022, available at https://edpb.europa.eu/news/news/2022/european-health-data-space-must-ensure-strong-protection-electronic-health-data_en. Retrieved July 30, 2022.

[1664] Michela Moscufo, MaryAlice Parks, Jeca Taudte: Period-tracking apps may help prosecute users, advocates fear. Article published July 2 2022, available at https://abcnews.go.com/Health/abortion-advocates-fear-period-tracking-apps-prosecute-abortion/story?id=85925714. Retrieved July 30, 2022.

7.1.15. Proposal for a revised Product Liability Directive

In September 2022, the European Commission published its proposal[1665] for a directive on liability of defective products. The reason is that the existing Product Liability Directive[1666] was adopted in 1985, nearly 40 years ago, at a time where Big Data and AI applications as we know them today did not exist. Consequently, the proposal aims to bring the EU's liability regime up to speed with the digital age by introducing new provisions addressing the liability of a category of products emerging from new digital technologies such as Internet of Things or Artificial Intelligence. For example, the proposal*:*

- *clarifies that software must be considered a product in the scope of the directive;*
- *alleviates the burden of proof for victims under certain circumstances;*
- *introduces liability for defective products when refurbished and placed back on the market as well as when manufactured outside the European Union;*
- *extends the nature of damage to psychological health and loss or corruption of data; and*
- *considers as product defectiveness the lack of software updates under the manufacturer's control as well as the failure to address cybersecurity vulnerabilities."*[1667]

The review of this directive shall be welcomed, because the legal framework needs to reflect specific implications Big Data and AI applications may have. The same applies to the General Product Safety Directive[1668] which should also be reviewed against modern threats as well as present cyber-security standards.[1669] AI-driven products should be examined in the light of product liability to properly address the risk of accidents and damage.[1670]

[1665] The text of the proposal for a new Product Liability Directive is available at https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-new-product-liability-directive#:~:text=The%20European%20Commission%20published%20a%20proposal%20for%20a,and%20global%20value%20chains%20on%2028%20September%202022. Retrieved January 7, 2023.

[1666] The text of the Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374. Retrieved January 7, 2023.

[1667] Background information on this initiative is provided by the European Parliament, including the Legislative Train Schedule, available at https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-new-product-liability-directive#:~:text=The%20European%20Commission%20published%20a%20proposal%20for%20a,and%20global%20value%20chains%20on%2028%20September%202022. Retrieved January 7, 2023.

[1668] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety is available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095. Retrieved October 2, 2021.

[1669] See also rules on Internet-connected devices. Background information on the IoT regulatory framework for Europe is provided by Vodafone in their White Paper: A new IoT regulatory framework for Europe. White Paper published June 2019, available at https://www.vodafone.com/content/dam/vodcom/files/public-policy/iot-whitepaper/IoT_whitepaper_.pdf. Retrieved October 2, 2021.

[1670] For example, self-driving car fatalities. Wired reported about the latest Tesla car crash on May 16 2019, available at https://www.wired.com/story/teslas-latest-autopilot-death-looks-like-prior-crash/. Retrieved October 2, 2021.

7.1.16. Proposal for an Artificial Intelligence Act

Following their above-mentioned White Paper on AI and a public consultation period, the European Commission published its proposal for a regulation[1671] on a European approach for Artificial Intelligence in early 2021:[1672] "The Commission is proposing the first ever legal framework on AI which addresses the risks of AI and positions Europe to play a leading role globally." These landmark rules are an ambitious attempt to regulate AI and represent a major step towards a comprehensive legal framework for Artificial Intelligence, setting out a cross-sectoral regulatory approach for the use of AI with the aim to pave a way to both, ethical use of AI technologies and ensuring that the EU remains competitive in this regard.[1673] It is important to note that the new regulation shall not replace existing rules; the Commission stresses that the present legal framework however should be improved.[1674] As any regulation, the rules would apply directly with no need for further implementation at member state level, and this shows that the Commission wants to establish consistent rules for AI and improve legal certainty. However, the fact that the regulation will have to pass the European Parliament and the European Council makes it likely that there will be adjustments, also because various stakeholders' standpoints and interests on such a complex topic as AI will have to be considered; another factor to consider is that the regulation will come into force 24 months after it has been adopted, it is questionable whether some of the provisions will be overtaken by technological progress before they even apply, meaning that the regulation, or parts thereof, would perhaps not be future-proof.[1675] The Artificial Intelligence Act defines AI as: "any software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs, such as content, predictions, recommendations, or decisions influencing the environments they interact with." This definition can be questioned from a technical point of view,[1676] and there is no agreed definition of AI amongst experts in industry or law, there are only common elements in various

[1671] If adopted by the European Parliament and Council, the Artificial Intelligence Act would apply directly across the EU.

[1672] Background information on the proposal for a regulation laying down harmonized rules on Artificial Intelligence is provided by the Commission, available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence. Retrieved October 22, 2021.

[1673] Commission press release: Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. Press release published April 21 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682. Retrieved October 22, 2021.

[1674] Brahim Benichou, Jan De Bruyne, Thomas Gils, Ellen Wauters: Regulating AI in the European Union: seven key takeaways. Article published February 25 2020, available at https://ai-laws.org/2020/02/regulating-ai-in-the-european-union-seven-key-takeaways/. Retrieved October 22, 2021.

[1675] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1676] Jay Modrall: EU proposes new Artificial Intelligence regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation. Retrieved October 22, 2021.

definitions (such as digital, technology, learning, reasoning),[1677] and another factor to consider is the dual-use characteristics of AI: as much as AI can serve the good, it can also serve the bad.[1678] It also must not be forgotten that what was considered AI ten years ago might not be considered AI today. This broad definition is intended to determine the scope of regulation and to be technology-neutral and as future-proof as possible[1679], but that also means that software which is traditionally not necessarily classified as AI would be covered by the new regulation. The extent to which the terms "software", "AI system", etc. currently proposed in the AI Regulation can be further clarified is likely to be of crucial importance to the success of the AI Regulation Act since this will reduce remaining ambiguities.[1680] Moreover, just like GDPR, the Artificial Intelligence Act will apply to the private and public sector, and more importantly, the draft AI Regulation intends to capture all parties involved in the AI value chain,[1681] that is:

- *"Providers (i.e., entity / person that develops or has an AI system developed) who place AI systems on the EU market or put them into service in the EU irrespective of whether they are established within the EU. (...) Where the provider is not established in the EU and where an importer cannot be identified, an authorized representative in the EU must be appointed;*
- *Users of AI systems (i.e., the entity / person using an AI system) established in the EU – except where the AI system is used in the course of a personal non-professional activity;*
- *Providers and users of AI systems established outside the EU where the output produced by the AI system is used in the EU;*[1682]
- *Manufacturers of products are covered and are responsible for compliance as if they were the provider of the high-risk AI system;*
- *Distributors, importers, users and other third parties will also be subject to providers' obligations if they place a high-risk AI system on the market or into service under their name*

[1677] Valerie Thomas: Report on Artificial Intelligence on behalf of the Regulatory Institute, Part I: The existing regulatory landscape. Article published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 22, 2021.

[1678] Miles Brundage et al: The malicious use of Artificial Intelligence: forecasting, prevention, and mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Retrieved October 22, 2021.

[1679] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1680] Jens Peter Schmidt: European Commission proposes world's first ever regulatory framework on Artificial Intelligence. Article published March 23 2021, available at https://www.noerr.com/en/newsroom/news/european-commission-proposes-worlds-first-ever-regulatory-framework-on-artificial-intelligence-ai. Retrieved October 22, 2021.

[1681] Jay Modrall: EU proposes new Artificial Intelligence regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation. Retrieved October 22, 2021.

[1682] William Long, Francesca Blythe, Lauren Cuyvers, Monika Zdzieborska: EU Commission issues draft AI regulation. Article published April 23 2021, available at https://datamatters.sidley.com/eu-commission-issues-draft-ai-regulation. Retrieved October 22, 2021.

> *or trademark, modify the intended purpose of a high-risk AI system already on the market or in service or make a substantial modification to a high-risk AI system. In that case, the original provider is relieved of responsibility*."[1683]

The implications that come with further terminology and definitions should not be underestimated: there are voices that say that, once all of EU's legal initiatives enter into force, one and the same company could be both, "controller" and "processor" under GDPR, "data holder" under the DGA and "distributor" under the AI regulation, meaning that consistency would be substantially hampered.[1684] Like GDPR, Article 71 of the new regulation allows for high fines of up to 30,000,000 Euro or of up to 6% of total annual worldwide turnover, whichever is higher, depending on the type of violation: the highest fines will apply to infringements on prohibited practices, medium-range fines are foreseen for non-compliance, and the lowest fines apply to the supply of incorrect, incomplete or misleading information to notified bodies and competent authorities. Unlike the GDPR, the draft regulation does not provide for a right to compensation, which, on the one hand, may provide comfort. On the other hand, that does not mean that a private right of action is not given if the conditions of GDPR Art. 82 are met. Like the GDPR, the Artificial Intelligence Act will have extraterritorial effect, the regulation will apply to users of AI systems located within the EU as well as providers and users of AI systems located outside the EU where the output is used in the EU and providers which place on the market or put into service AI systems in the EU regardless of where they are located.[1685] This may lead to the so-called "Brussels-effect"[1686] which guides the way companies are doing business, because multinational organizations would adjust their global operations to EU standards to be compliant. Apart from the extraterritorial scope and high fines, various other provisions of the regulation echo the GDPR, for example the fact that the Artificial Intelligence Act foresees for incident notifications or the fact that certain accountability, documentation and enforcement provisions apply:[1687] as for the latter, the Commission's proposal foresees for the creation of the European AI Board that would be entrusted with various tasks such as sharing of best practices, ensuring consistent application and harmonized implementation of the

[1683] Jay Modrall: EU proposes new Artificial Intelligence regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation. Retrieved October 22, 2021.

[1684] Vagelis Papakonstantinou, Paul De Hert: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Article published April 1 2021, available https://lsts.research.vub.be/en/20210401. Retrieved October 22, 2021.

[1685] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1686] Anu Bradford: The Brussels Effect - How the European Union rules the world, Oxford University Press 2020.

[1687] Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act. Paper published May 2021, available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf. Retrieved October 22, 2021.

regulation and issuance of opinions and recommendations.[1688] It is important to note that the Board will be complemented by a public database of all stand-alone high risk AI systems: this is an interesting development many welcome as it represents a new dimension of transparency[1689] different from mere information obligations under GDPR that can typically be described as one-time efforts addressed to data subjects as opposed to official bodies. The regulation is the first piece of legislation that is solely focused on Artificial Intelligence, i.e., identification, classification, documentation and monitoring of AI with a specific emphasis on high-risk AI. Even though the proposal does not define high risk, the proposal provides for criteria[1690] to be used to determine whether a system shall be classified as a high-risk application of AI, and the draft regulation also explains that risk shall be interpreted in line with existing product safety legislation. Content and structure of the proposal can be described as follows:[1691] first, the scope of the new proposed rules is defined; second, the draft proposal explains which AI systems are considered unacceptable, for example due to violation of fundamental rights. Title III of the draft contains specific rules for high-risk AI systems. Title IV of the draft AI Act is concerned with transparency obligations for systems that interact with humans; title V explains the objective of the creation of an innovation-friendly legal framework, which demonstrates that the European Commission is aware of the potential of Artificial Intelligence. Title VI is about governance; title VII addresses the work of the Commission and national authorities. Title VIII and IX set forth reporting obligations for AI providers and promote the voluntary application of requirements that are applicable to high-risk systems to providers of non-high-risk AI systems. Finally, title XII foresees that the Commission regularly evaluates the need for a revision of Annex III and prepares regular reports on the review of the regulation.[1692] In the explanatory memorandum within the draft proposal of the Artificial Intelligence Act, the Commission explains that the European Commission "puts forward the proposed regulatory framework on Artificial Intelligence with the following specific objectives:

- *Ensure that AI systems placed on the Union market are safe and respect existing law on fundamental rights and Union values;*

[1688] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1689] Friederike Reinhold, Angela Müller for AlgorithmWatch: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – a major step with major gaps. Article published April 22 2021. AlgorithmWatch's response is available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Retrieved October 22, 2021.

[1690] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1691] Nikita Lukianets: A (more) visual guide to the proposed EU Artificial Intelligence Act. Article published May 3 2021, available at https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act. Retrieved October 22, 2021.

[1692] Nikita Lukianets: A (more) visual guide to the proposed EU Artificial Intelligence Act. Article published May 3 2021, available at https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act. Retrieved October 22, 2021.

- *Ensure legal certainty to facilitate investment and innovation in AI;*
- *Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;*
- *Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation."*

The Artificial Intelligence Act thus wants to balance between protecting individuals and allowing for technological innovation[1693] based on balancing of risk. Unlike the low risk vs. high risk approach that was discussed in the Commission's 2020 White Paper on AI, the regulation differentiates between various levels of potential risks posed by AI: the Artificial Intelligence Act sets forth a four-tiered risk framework that recognizes the varying levels of risk posed by AI systems to one's health, safety, and / or fundamental rights and sets out proportionate requirements and obligations per risk level; in accordance with possible risks, each tier aims to set adequate requirements for providers and users of AI applications.[1694] The proposal starts with listing types of AI practices that are prohibited:[1695]

- *"Placing on the market, putting into service, or using an AI system that deploys subliminal techniques beyond a person's consciousness to materially distort a person's behavior in a manner that causes that person or another person physical or psychological harm;*
- *Placing on the market, putting into service, or using an AI system that exploits vulnerabilities of a specific group of persons due to their age, physical or mental disability to materially distort the behavior of a person pertaining to the group in a manner that causes that person or another person physical or psychological harm;*
- *Placing on the market, putting into service, or using an AI system by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons with the social score leading to detrimental or unfavorable treatment that is either unrelated to the contexts in which the data was originally generated or unjustified or disproportionate;*
- *Use of "real-time" remote biometric identification (read: facial recognition) systems in publicly accessible spaces for law enforcement purposes, subject however to broad exemptions that, in turn, are subject to additional requirements, including prior authorization for each individual*

[1693] Jamie Humphreys, Edward Turtle: European Parliament publishes its proposals for new AI laws. Article published October 28 2020, available at https://products.cooley.com/2020/10/28/regulating-ai-eu-proposes-legal-framework-for-artificial-intelligence/. Retrieved October 22, 2021.

[1694] Cailean Osborne: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/. Retrieved October 22, 2021.

[1695] Jens Peter Schmidt: European Commission proposes world's first ever regulatory framework on Artificial Intelligence. Article published March 23 2021, available at https://www.noerr.com/en/newsroom/news/european-commission-proposes-worlds-first-ever-regulatory-framework-on-artificial-intelligence-ai. Retrieved October 22, 2021.

> *use to be granted by a judicial authority or an independent administrative body in the member state where the system is used*."

It is foreseeable that the latter point will lead to controversial discussion: fighting crimes is an argument that is regularly used in the context of technologies like video surveillance and more sophisticated techniques like (real-time) facial recognition, however, this needs to be balanced against individuals' fundamental rights and freedoms. The European Data Protection Supervisor commented on the Artificial Intelligence Act that this is a welcomed initiative, but that ban on remote biometric identification in public space – a provision which was included in a previous leaked version of the regulation[1696] – is necessary.[1697] Moreover, this particular section of the draft has numerous exceptions, for example, targeted search for victims and prevention, detection, localization or prosecution of certain crimes.[1698] In addition, the draft does not cover other purposes (e.g. non-law-enforcement), other uses (e.g. non-publicly accessible spaces) or other players (e.g. private sector uses of biometric identification technologies), which leads to legal uncertainty in relation to other existing laws, namely GDPR and the Law Enforcement Directive as well as national laws.[1699] Finally, the example of Clearview AI, which is an app developed by a private company that allows to identify individuals based on a single picture, shows how controversial the discussion around the use of biometric information is when it comes to data protection: Clearview's technology has been used by police in many countries (e.g., Australia[1700]), but at the same time, data protection supervisory authorities in several countries including the United Kingdom, France, Italy, Greece and Austria are dealing with complaints[1701] or already issued fines (e.g.,

[1696] AccessNow: Europe's approach to Artificial Intelligence: how AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf. Retrieved October 22, 2021.

[1697] EDPS press release: Artificial Intelligence Act – a welcomed initiative but ban on remote biometric identification in public space is necessary. Press release published April 23 2021, available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en#:~:text=The%20European%20Commission%E2%80%99s%20legislative%20proposal%20for%20an%20Artificial,according%20to%20the%20EU%E2%80%99s%20values%20and%20legal%20principles. Retrieved October 22, 2021.

[1698] Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act. Paper published May 2021, available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf. Retrieved October 22, 2021.

[1699] Theodore Christakis, Mathis Becuywe: Pre-market requirements, prior authorisation and lex specialis – novelties and logic in the facial recognition-related provisions of the draft AI Regulation. Article published May 4 2021, available at https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/. Retrieved October 22, 2021.

[1700] Ariel Bogle: Australian Federal Police officers trialed controversial facial recognition tool Clearview AI. Article published April 15 2020, available at https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894. Retrieved October 22, 2021.

[1701] Background information is provided by Privacy International: Challenge against Clearview AI in Europe. Blog post published May 27 2021, available at https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe Retrieved October 22, 2021.

Sweden)[1702] or ordered the (partial) deletion of individual's biometric information (e.g., Germany).[1703] Against this background, this particular section within the draft AI Regulation faced harsh criticism; some institutions comment that the draft Act "missed an opportunity to clearly draw red lines and close loopholes".[1704] Others point to the fact that facial recognition has already been banned in many U.S. states,[1705] which is remarkable insofar as the U.S.A and the EU historically took a different approach on privacy: not the European principle of prohibition subject to permission but the idea that everything is allowed as long as it is not forbidden. As for high-risk AI applications, these can roughly be divided into high-risk sectors (e.g., healthcare, employment, finance) and high-risk purposes (e.g., automated driving, energy distribution, recruitment), for example:[1706]

- *Management and operation of critical infrastructures such as traffic and electricity;*
- *Education or Vocational training, for example determining access to education;*
- *Employment (i.e., during the recruitment, promotion, or termination process;*
- *Evaluation of access to essential resources, benefits, and services;*
- *Law enforcement (e.g., assessing risks of re-offending);*
- *Immigration and border control and asylum.*

The following general requirements will apply to high-risk AI:[1707] human oversight, adequate risk management, appropriate transparency obligations, documentation to allow for compliance assessments, logging of activities to ensure traceability as well as a high level of accuracy, robustness and security

[1702] Natasha Lomas: Sweden's data watchdog slaps police for unlawful use of Clearview AI. Article published February 12 2021, available at https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAALgmrj2j7lIqtPjUw9cgbbjI_LwuKoMDVdLqwxaBB4vNzCgFK7Pbz7Ez_PA0oQOMd7Csz70S7acDJmzPURaBLxCvcCrHG9kAiK1112tsVuo1yTd_vtJ3XMiwQYkT2_yofnTUP6pgIpte0masI6OagPfoQ91ZjZA16T2v7bBqJRwp. Retrieved October 22, 2021.

[1703] Background information on this German regulator's enforcement actions is provided by NOYB, available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF. Retrieved October 22, 2021.

[1704] Friederike Reinhold, Angela Müller for AlgorithmWatch: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – a major step with major gaps. Article published April 22 2021, available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Retrieved October 22, 2021.

[1705] Melissa Heikkila: AI: Decoded: U.S. states move to ban facial recognition -AI and structural racism. Article published May 12 2021, available at https://www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-ai-gov-us-states-move-to-ban-facial-recognition-ai-and-structural-racism/. Retrieved October 22, 2021.

[1706] The law firm Hunton Andrews Kurth provides details on the proposed AI Act in their 2021 blog post: European Commission publishes proposal for Artificial Intelligence Act. Article published April 22 2021, available at https://www.huntonprivacyblog.com/2021/04/22/european-commission-publishes-proposal-for-artificial-intelligence-act/. Retrieved October 22, 2021.

[1707] Diletta De Cicco, Charles-Albert Helleputte: The EU Artificial Intelligence Act, paper prepared on behalf of Steptoe in May 2021, and is available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf. Retrieved October 22, 2021.

and the use of high-quality training, validation and testing data sets.[1708] High risk AI will be subject to certain restrictions; in particular, conformity assessments will be required, meaning that certification will become mandatory for such AI applications.[1709] In this regard, the EU takes a “cradle to grave approach:”[1710] high-risk AI systems will be subject to review throughout their life cycle, including mandatory risk management, documentation requirements, as well as post-market monitoring and incident reporting. Many welcomed the draft AI’s proposal to create an EU database on high-risk AI systems[1711] that includes information on (see Annex VIII) the AI system (including status, trade name and any other additional reference allowing for identification as well as information on the Member States in which the AI system is to or has been placed on the market, put into service or made available; the type, number and expiry date of the certificate issued by the notified body including; a description of the intended purpose of the AI system; a copy of the conformity certificate (where required); a URL for additional information (optional); electronic use instructions and provider information. It is important to note that the majority of obligations applies to so-called providers, but Chapter 2 and 3 of Title III also establish obligations for importers (covered under Article 26 of the draft AI Act) and distributors (covered under Article 27 of the draft AI Act) as well as users (covered under Article 29 of the draft AI Act),[1712] and this shows that the regulation aims at capturing all parties involved in the making available in the market and use of AI.[1713] AI systems that are used as a products or safety components, for example in medical devices, are listed in Annex II and will require to third-party ex-ante assessments, meaning that external entities will review the AI application before it can be put into service;[1714] other high risk AI systems specified in Annex III of the draft regulation will require first-

[1708] Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission launches proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration. Retrieved October 22, 2021.

[1709] Brahim Benichou, Jan De Bruyne, Thomas Gils, Ellen Wauters: Regulating AI in the European Union: seven key takeaways. Article published February 25 2020, available at https://ai-laws.org/2020/02/regulating-ai-in-the-european-union-seven-key-takeaways/. Retrieved October 22, 2021.

[1710] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1711] Krzysztof Izdebski: Comment on AI regulation proposal. EU database on high-risk AI systems. Article published April 28 2021, available at https://epf.org.pl/en/2021/04/28/comment-on-ai-regulation-proposal-eu-database-on-high-risk-ai-systems/. Retrieved October 22, 2021.

[1712] Keily Blair, James Hall, Christian Schröder, Heather Sussman, Shannon Yarovsky: The new EU approach to the regulation of Artificial Intelligence. Article published on May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/. Retrieved October 22, 2021.

[1713] Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission launches proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration. Retrieved October 22, 2021.

[1714] Cailean Osborne: The European Commission’s Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/. Retrieved October 22, 2021.

party ex-ante conformity assessments (i.e. self-assessments prior to their use), as well as ex-post quality and risk management assessments and post-market monitoring. As regards conformity assessments, reference is made to existing requirements in EU product safety laws (see Annex II),[1715] however, the AI Regulation's self-assessment-approach faced criticism: while industry often prefers a deregulated landscape when it comes to using technology, because it is believed that regulation stifles innovation,[1716] legislative history in the course of industrial revolutions and across various sectors, be it transportation, chemical engineering, communications, aviation or biotechnology and digitization has shown that voluntary codes or self-regulation may simply not work, and that regulatory discussions should not primarily focus on specific harms or individual risks but also take the systemic and structural risk of Artificial Intelligence into consideration.[1717] Some say that time will tell whether voluntary codes and ethics standards will be sufficient to mitigate the risks posed by AI but some believe that where AI applications have an impact on human rights, legislation is required to protect those human rights.[1718] Finally, the Artificial Intelligence Act furthermore sets forth that minimal or no risk AI (e.g., spam filters) will be permitted with no restrictions, but providers of such AI applications are encouraged to adhere to voluntary codes of conduct or apply voluntary labeling schemes.[1719] AI systems which pose a limited risk (e.g. chat-bots) – perhaps the majority of applications – will be subject to transparency obligations to allow for informed decisions.[1720]

7.1.17. Proposal for an AI Liability Directive

In late 2022, the European Commission published a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence, the AI Liability Directive,[1721] which is intended to complement the EU AI Act. For consistency purposes, the AI Liability Directive uses the same

[1715] Jetty Tielemans: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/. Retrieved October 22, 2021.

[1716] Valerie Thomas: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/. Retrieved October 22, 2021.

[1717] Julia Black, Andrew Murray: Regulating AI and Machine Learning: setting the regulatory agenda. European Journal of Law and Technology 2019, vol. 10, issue 3, available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 22, 2021.

[1718] Alan Turing Institute: AI, ethics, and the law: what challenges and what opportunities. Article published January 18 2018, available at https://aticdn.s3-eu-west-1.amazonaws.com/2018/03/140318-Ai-ethics-and-the-law-public-panel-report.pdf. Retrieved October 22, 2021.

[1719] Lisa Peets, Marty Hansen, Sam Jungyun Choi, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission Presents Strategies for Data and AI. Article published February 20, 2020, available at https://www.covingtondigitalhealth.com/2020/02/european-commissions-white-paper-on-artificial-intelligence-part-2-of-4/. Retrieved October 22, 2021.

[1720] Cailean Osborne: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/. Retrieved October 22, 2021.

[1721] The text of the AI liability directive is available at https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en. Retrieved January 7, 2023.

definitions[1722] as the AI Act. In the explanatory memorandum on the AI Directive, the Commission shared the reasons underlying the choice to use the directive as the selected legislative instrument:[1723] "non-binding soft law (e.g., recommendations) would not be complied with as intended and therefore not have the desired effect. A set of rules directly applicable to all Member States (regulation), comparatively, would be too strict in relation to the scope of tortious liability, which is based on specific and long-established legal traditions of each Member State. The choice of the directive therefore leaves more flexibility for the internal transposition to the Member States while requiring more rigid compliance than its soft-law counterparts." The purpose of the AI Liability Directive proposal is to ensure uniform rules apply for "certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems."[1724] If adopted, the proposals will change the liability rules for AI software and systems: the draft AI Liability Directive will apply to damages that occur two years or more after the Directive enters into force; five years after its entry into force, the Commission will consider the need for rules on no-fault liability for AI claims.[1725] The proposal intends to "respond to the challenges identified and to improve the functioning of the internal market by laying down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems. The proposal addresses the specific difficulties of proof linked with AI and ensures that justified claims are not hindered. The Commission asked for feedback on its proposal."[1726] Prior to this initiative, the Commission discussed[1727] specific safety and liability implications of Artificial Intelligence; the European Parliament called for a legal framework for civil liability claims and for imposing a regime of strict liability on operators of high-risk AI systems.[1728] The AI Liability Directive AI Directive aims to ease the claimant's burden of proof with the help of two new key rules for attributing liability in non-contractual fault-based claims where an AI system is intrinsically

[1722] See AI Liability Directive Art. 2.

[1723] Giacomo Lusardi, Coran Darling: The AI liability directive: EU improves liability protections for those impacted by AI. Article published December 6 2022, available at https://www.technologyslegaledge.com/2022/12/the-ai-liability-directive-eu-improves-liability-protections-for-those-impacted-by-ai/. Retrieved January 7, 2023.

[1724] The European Commission provides background information on liability rules for Artificial Intelligence, available at https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en. Retrieved January 10, 2023.

[1725] Dan Cooper, Lisa Peets, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission publishes directive on the liability of Artificial Intelligence systems. Article published October 12 2022, available at https://www.insideprivacy.com/artificial-intelligence/european-commission-publishes-directive-on-the-liability-of-artificial-intelligence-systems/. Retrieved January 7, 2023.

[1726] Background information on the initiative is provided by the European Parliament, including the Legislative Train Schedule, available at https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive. Retrieved January 7, 2023.

[1727] Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics published February 19 2020, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064. Retrieved January 7, 2023.

[1728] European Parliament draft report with recommendations to the Commission on a civil liability regime for AI published September 28 2020, available at available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/09-28/VL_Civilliabilityregimeforartificialintelligence_ams_EN.pdf. Retrieved January 7, 2023.

involved:[1729] a rebuttable presumption of causality, and a right to evidence. This means that under the new AI Liability Directive, courts will have the power to order providers or users of high-risk AI systems to disclose and / or preserve information about their systems. If such a disclosure conflicts with trade secrets, the court will may take measures necessary to preserve the confidentiality of that information during the proceedings.[1730] This approach shall be highly welcomed from an individual's perspective: Claims for harm caused by AI applications can be difficult, because AI systems are opaque, users do not have enough insight into how that AI system works, meaning that they are unable to provide proof that a specific defect or malfunction was the cause of the harm. While the AI Act sets out certain documentation and information requirements for AI systems, there is no specific right under the AI Act for a person injured by that system to access that information, which would be critical in substantiating a claim for compensation.[1731] Therefore, easing the burden of proof through a (rebuttable) presumption of causality together with increased transparency through disclosure of AI-related evidence will be truly helpful as it would significantly lower evidentiary hurdles for victims injured by AI-related products or services to bring civil liability claims.[1732] However, the problem is that the rebuttable presumption "only applies if a national court finds it excessively difficult for the victim-claimant (or any other claimant) to prove the causal link and a number of specific conditions are met. These include that:

- *the claimant has proven, or the court has presumed, the fault of the defendant, or of a person for whose behavior the defendant is responsible, consisting in the failure to comply with a duty of care intended to protect against the damage that has occurred (e.g., a duty of care under the AI Act or other national or European legislation);*
- *it is reasonably likely that, based on the circumstances of each case, the defendant's negligent conduct affected the output produced by the AI system or the AI system's inability to produce an output; and*
- *the claimant has proved that the output produced by the AI system or the AI system's inability to produce an output caused the damage*.[1733]

[1729] See AI Liability Directive Art. 3.

[1730] Dan Cooper, Lisa Peets, Nicholas Shepherd, Anna Oberschelp de Meneses: European Commission publishes directive on the liability of Artificial Intelligence systems. Article published October 12 2022, available at https://www.insideprivacy.com/artificial-intelligence/european-commission-publishes-directive-on-the-liability-of-artificial-intelligence-systems/. Retrieved January 7, 2023.

[1731] Ralph Giles: The AI Liability Directive. Key points to be aware of for businesses that use AI. Article published November 17 2022, available at https://www.bristows.com/news/the-ai-liability-directive/. Retrieved January 7, 2023.

[1732] Avi Gesser, Robert Maddox, Anna Gressel, Frank Colleluori, Michael Pizzi: Debevoise & Plimpton discusses the EU AI liability directive's impact on Artificial Intelligence legal risks. Article published November 21 2022, available at https://clsbluesky.law.columbia.edu/2022/11/21/debevoise-plimpton-discusses-eu-ai-liability-directives-impact-on-artificial-intelligence-legal-risks/. Retrieved January 7, 2023.

[1733] Giacomo Lusardi, Coran Darling: The AI Liability Directive: EU improves liability protections for those impacted by AI. Article published December 6 2022, available at https://www.technologyslegaledge.com/2022/12/the-ai-liability-directive-eu-improves-liability-protections-for-those-impacted-by-ai/. Retrieved January 7, 2023.

And there are further challenges when claims relate to a high-risk AI system:[1734] "to satisfy the first condition above, the claimant has to demonstrate the defendant did not comply with these requirements, including high quality training data sets, transparency and human oversight of the system, and appropriate levels of accuracy, robustness and cybersecurity. In addition, if the defendant can demonstrate there is sufficient evidence and expertise accessible to the claimant so that it can prove the causal link, the presumption is also rebutted." Lastly, the presumption will only apply where the court considers it excessively difficult for the claimant to prove the causal link. From an individual's perspective, the question is "how is an injured party supposed to know in advance when evidence is excessively difficult to adduce, or that he reasonably has evidence and expertise to prove causation?"[1735] It therefore seems that civil procedural law with its complex relationship between burden of proof and presentation, facilitation of evidence, etc. will be decisive in the end;[1736] even though the reasoning behind the choice to use the directive as the selected legal instrument is comprehensible, it involves a risk of fragmentation and legal uncertainty due to national legal latitudes which contradicts the overall goal to harmonize the legal landscape in the context of AI.

7.2. Considerations for international data transfers

Owing to the fact that processing of personal data in many cases cannot be limited to a single country or the European Union / the European Economic Area and a small number of non-EU countries,[1737] rules are needed to serve as standards and safeguards for international data transfers.[1738] At present, a diversified toolkit of mechanisms to transfer data to third countries exists such as, for example, a set of Standard Contractual Clauses (SCCs),[1739] Binding Corporate Rules[1740] as well as several adequacy decisions.[1741] GDPR Article 45 (9) makes clear that pre-GDPR adequacy decisions remain in force. One

[1734] Ralph Giles: The AI Liability Directive. Key points to be aware of for businesses that use AI. Article published November 17 2022, available at https://www.bristows.com/news/the-ai-liability-directive/. Retrieved January 7, 2023.

[1735] Fritz-Ulli Pieper, Alexander Schmalenberger: AI Liability Directive – Welche Haftungsregeln erwarten uns zukünftig für KI? Article published October 4 2022, available at https://www.taylorwessing.com/de/insights-and-events/insights/2022/10/ai-liability-directive-haftungsregeln. Retrieved January 10, 2023.

[1736] Fritz-Ulli Pieper, Alexander Schmalenberger: AI Liability Directive – Welche Haftungsregeln erwarten uns zukünftig für KI? Article published October 4 2022, available at https://www.taylorwessing.com/de/insights-and-events/insights/2022/10/ai-liability-directive-haftungsregeln. Retrieved January 10, 2023.

[1737] Further details are available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en. Retrieved October 17, 2021.

[1738] Background information is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0007&from=EN. Retrieved October 17, 2021.

[1739] Standard Contractual Clauses are available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Retrieved October 17, 2021.

[1740] Details on the respective process are available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en. Retrieved October 17, 2021.

[1741] Background information on adequacy decisions is available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%C2%A0European%20Commission%20has%20the%20power%20to%20determine%

of the well-known legal instruments in this regard was the so-called Privacy Shield.[1742] The EU-US Privacy Shield was adopted in 2016[1743] and reviewed on an annual basis[1744] to ensure a constant level of adequacy for the protection of personal data. One the one hand, businesses this framework as it brings legal clarity; on the other hand, the EU-US Privacy Shield, like its precursor "Safe Harbor",[1745] faced criticism – already the European Parliament passed a non-binding resolution in which it asked the European Commission to suspend the Privacy Shield framework as it fails to provide an adequate level of protection.[1746] Interestingly, even though the discussion around data transfers is going on for many years, it is often overlooked that the GDPR does not provide for a legal definition of the notion transfer of personal data to a third country or to an international organization. Therefore, the EDPB issued guidelines to clarify when the requirements of GDPR chapter V shall be applied and identified three cumulative criteria to qualify a processing operation as a transfer:[1747]

- *A controller or a processor ("exporter") is subject to the GDPR for the given processing;*
- *The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller, or processor ("importer");*
- *The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3 or is an international organization.*

If the three criteria as identified by the EDPB are met, there is a transfer and Chapter V of the GDPR is applicable. This means that the transfer can only take place under certain conditions, such as in the context of an adequacy decision from the European Commission (Article 45) or by providing appropriate safeguards (Article 46).

2C%20on,an%20opinion%20of%20the%20European%20Data%20Protection%20Board. Retrieved October 17, 2021.

[1742] Details on the Privacy Shield are available at https://www.privacyshield.gov/eu-us-framework. Retrieved October 22, 2021.

[1743] Commission press release: European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Press release published July 12 2016, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461. Retrieved October 22, 2021.

[1744] The 2018 second annual review report available at https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf. Retrieved October 22, 2021.

[1745] It was struck down by the European Court of Justice on July 17 2014 in case C-362/14, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=2393. Retrieved October 22, 2021.

[1746] Chris Cwalina, Jeewon Kim Serrato, Susan Ross, Tristan Coughlin: The European Parliament asks for the suspension of the privacy shield. Article published July 17 2018, available at https://www.dataprotectionreport.com/2018/07/european-parliament-asks-for-suspension-privacy-shield/. https://www.dataprotectionreport.com/2018/07/european-parliament-asks-for-suspension-privacy-shield/. Retrieved October 22, 2021.

[1747] EDPB Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per chapter V of the GDPR Version 2.0 published 14 February 2023, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en. Retrieved February 28, 2023.

7.2.1. EU-US Privacy Shield framework

The Privacy Shield has in fact been invalidated by the European Court of Justice in summer 2020[1748] because the U.S. does not have an adequate level of data protection given that authorities have administrative access powers and due to the lack of legal protection options for EU citizens. While the appropriateness of Standard Contractual Clauses has been confirmed, the protection of personal data in the context of U.S. national security has been questioned.[1749] Consequently, a coalition of civil society groups sent a letter to President Biden "urging the administration to ensure that any new transatlantic data transfer deal is coupled with the enactment of surveillance reforms and comprehensive data protection legislation" since otherwise, concerns about data transfers to the United States will remain.[1750] As a reaction to the invalidation of the Privacy Shield, many national supervisory authorities issued (divergent) guidance[1751] to help with "transfer impact assessments".[1752] Companies are left with a lot of homework with regards to vendor screenings to demonstrate that they evaluated service suppliers processing their (employee, customer) data abroad, because there are more and more regulator decisions which underline the inadmissibility of data transfers to the U.S.: already in April 2021, the supervisory authority of Portugal, who specifically referred to the "Schrems II" decision, issued a resolution which required the National Institute of Statistics to suspend, within twelve hours, the transfer of data collected as part of the 2021 census surveys to the U.S. or any other third country without adequate data protection.[1753] The European Data Protection Supervisor issued a decision against the European Parliament after EP Members alleged that the Parliament's use of cookies violated data protection law, including requirements regarding the transfer of personal data outside of the EU.[1754] Shortly after the EDPS' decision, the Austrian regulator took a similar position in the framework of Google Analytics in

[1748] The judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems is available at https://curia.europa.eu/juris/liste.jsf?num=C-311/18. Retrieved October 22, 2021..

[1749] Background information on the issue behind Case C-311/18 is provided by the Advocate General, available at http://curia.europa.eu/juris/document/document.jsf?docid=221826&doclang=EN. Retrieved October 22, 2021.

[1750] Electronic Privacy Information Center letter issued June 10 2021, available at https://epic.org/international/Data-Flows-Negotiations-Coalition-Letter-June2021.pdf. Retrieved October 22, 2021.

[1751] The International Association of Privacy Professionals (IAPP) provides an overview on this topic, including government guidance on "Schrems II", available at https://iapp.org/resources/article/dpa-and-government-guidance-on-schrems-ii-2/. Retrieved October 22, 2021.

[1752] The term refers to recommendations issued by the European Data Protection Board regarding supplementary measures to ensure compliance with data protection laws when transferring personal data from Europe. Recommendations published June 21 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. Retrieved July 20, 2022.

[1753] Nigel Parker: Schrems II – Portuguese DPA suspends data transfer to the U.S. by public entity that relied on standard contractual clauses. Article published May 7 2021, available at https://www.allenovery.com/en-gb/global/blogs/digital-hub/schrems-ii-portuguese-dpa-suspends-data-transfer-to-the-us-by-public-entity-that-relied-on-standard-contractual-clauses. Retrieved July 20, 2022.

[1754] Natasha Lomas: European parliament found to have broken EU rules on data transfers and cookie consents. Article published January 11 2022, , available at https://techcrunch.com/2022/01/10/edps-decision-european-parliament-covid-19-test-website/. Retrieved January 20, 2022.

a complaint that was initiated by Max Schrems' NGO "None of Your Business".[1755] Meanwhile, the EDPB also provided their opinion on the EU-US Data Privacy Framework.[1756] However, what is often overlooked in the context of the Schrems II decision, is that the decision not only affects data transfers to the USA: in the absence of an adequacy decision by the European Commission, the ECJ requires data exporters to assess whether an equivalent level of protection for personal data exists in the respective third country prior to the transfer, and in this context, the question arises as to what significance Convention No. 108 and No. 108+ plays in the examination of the level of protection in third countries that are party to this international agreement.[1757] It therefore makes sense to compare GDPR requirements with respect to an „equivalent level of protection" with the provisions of Convention No. 108+.[1758]

7.2.2. Binding Corporate Rules and Standard Contractual Clauses

Together with Binding Corporate Rules which some consider the "gold standard for international data transfers",[1759] Standard Contractual Clauses have been and will be a major legal instrument for international data transfers. As a follow-up to the Privacy Shield decision, SCCs have been updated – and widely commented at local[1760] and EU level[1761] – to reflect some of the concerns that were raised in the context of the decision. However, the path forward may still not be crystal clear as the European Commission and Ireland's data regulator are investigating if the proposed new Standard Contractual

[1755] NYOB's statement: Austrian DSB: EU-US data transfers illegal. Statement published January 12 2022, available at https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal. Retrieved July 20, 2022.

[1756] EDPB opinion 5/2023 on the European Commission draft implementing decision on the adequate protection of personal data under the EU-US Data Privacy Framework published February 28 2023, available at https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf. Retrieved February 28, 2023.

[1757] Carlo Piltz, Philipp Quiel: The role of „Convention No. 108" and "Convention No. 108+" as part of the examination of the level of protection in third countries under the GDPR. Article published September 1 2020, available at https://www.delegedata.de/2020/09/the-role-of-convention-no-108-and-convention-no-108-as-part-of-the-examination-of-the-level-of-protection-in-third-countries-under-the-gdpr/. Retrieved July 20, 2022.

[1758] A detailed comparison of the individual regulations within „Convention No. 108" and "Convention No. 108+" is provided by Carlo Piltz, Philipp Quiel: The role of „Convention No. 108" and "Convention No. 108+" as part of the examination of the level of protection in third countries under the GDPR. Article published September 1, 2020, available at https://www.delegedata.de/2020/09/the-role-of-convention-no-108-and-convention-no-108-as-part-of-the-examination-of-the-level-of-protection-in-third-countries-under-the-gdpr/. Retrieved June 8, 2022.

[1759] Lukas Feiler, Wouter Seinen: BCRs as a robust alternative to Privacy Shield and SCCs. Article published July 23 2020, available at https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/. Retrieved October 22, 2021.

[1760] For example, one of the German regulators recommended actions and amendments to SCCs. Guidance published August 25, updated September 9 2020, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf. Retrieved October 22, 2021.

[1761] EDPB and EDPS joint opinion on two sets of SCCs (one on SCCs for contracts between controllers and processors, and one on SCCs for transfer of personal data to third countries) published January 15 2021, available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en. Retrieved October 22, 2021.

Clauses could cause complications when used under Irish law.[1762] Developments are generally very dynamic in this area: the EDPB and EDPS commented on the European Commission's new framework and issued a joint statement in which they requested various amendments[1763] which some consider substantial revisions.[1764] The EU is not the only institution that deals with SCCs; the UK prepared a bespoke set of Standard Contractual Clauses to facilitate transfers of personal data,[1765] and Brazil's data protection law is another example of a legal framework that allows for international transfers of personal data based on contractual instruments such as binding corporate rules and standard clauses.[1766] China also worked on a "standard contract" as a means for cross-border data transfers,[1767] and there are further new data transfer mechanisms such as the Global CBPR Forum.[1768] Even though companies will have 18 months to substitute the European Commission's new SCCs,[1769] it is very likely to become more difficult for controllers in future to match all requirements and fulfill all contractual obligations.

7.2.3. Derogations, Codes of Conduct, certifications

Apart from specific legal frameworks like the Privacy Shield or instruments like BCRs and SCCs, there are other legal possibilities for international data transfers:[1770] despite the exceptional character of

[1762] Sam Clark for Global Data Review: Draft SCC clash with Irish law reaches European Commission. Article published February 25 2021, available at https://globaldatareview.com/data-privacy/draft-scc-clash-irish-law-reaches-european-commission. Retrieved October 22, 2021.

[1763] EDPB and EDPS joint opinion on two sets of SCCs (one on SCCs for contracts between controllers and processors, and one on SCCs for transfer of personal data to third countries) published January 15 2021, available at https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en. Retrieved October 22, 2021.

[1764] Molly Martinson: Work in progress – substantial revisions recommended to the European Commission's draft new Standard Contractual Clauses. Article published January 28 2021, available at https://practicalprivacy.wyrick.com/blog/work-in-progress-substantial-revisions-recommended-to-the-european-commissions-draft-new-standard-contractual-clauses. Retrieved October 22, 2021.

[1765] Cynthia O'Donoghue, Asel Ibraimova: ICO announces it is working on bespoke UK set of Standard Contractual Clauses. Article published 5 May 2021, available at https://www.technologylawdispatch.com/2021/05/privacy-data-protection/ico-announces-it-is-working-on-bespoke-uk-set-of-standard-contractual-clauses/. Retrieved October 22, 2021.

[1766] Renato Leite Monteiro: The new Brazilian General Data Protection Law — a detailed analysis. Article published August 15 2018, available at https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/. Retrieved October 22, 2021.

[1767] Todd Liao, Judy Wang, Sylvia Hu: China releases Standard Contractual Clauses for cross-border data transfers. Article published July 11 2022, available at https://www.morganlewis.com/pubs/2022/07/china-releases-standard-contractual-clauses-for-crossborder-data-transfers. Retrieved July 20, 2022.

[1768] Mark Young, Sam Jungyun Choi, Jiayen Ong: Global CBPR Forum – a new international data transfer mechanism. Article published May 2 2023, available at https://www.insideprivacy.com/cross-border-transfers/global-cbpr-forum-a-new-international-data-transfer-mechanism/. Retrieved May 5, 2023.

[1769] Cynthia O'Donoghue, Andreas Splittgerber, Asel Ibraimova: European Commission issues New Standard Clauses for data transfers outside the EEA: Act within 18 months. Article published June 4 2021, available at https://www.technologylawdispatch.com/2021/06/global-data-transfers/european-commission-issues-new-standard-clauses-for-data-transfers-outside-the-eea-act-within-18-months/. Retrieved October 22, 2021.

[1770] Centre for Information Policy Leadership White Paper: Essential legislative approaches for enabling cross-border data transfers in a global economy. White Paper publishesd September 25 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf. Retrieved October 22, 2021.

derogations under GDPR Art. 49 which require a restrictive application, it is worthwhile noting that derogations are being discussed as a further option for international data transfers.[1771] As regards derogations under GDPR Art. 49, the International Association of Privacy Professionals published on overview in which they first explain that already the judge-rapporteur in the "Schrems II" case elaborated on the possibility of reliance on the GDPR Article 49 derogations; second, they stress that organizations must be aware of additional considerations in the context of derogations provided in various GDPR Recitals, and finally, they summarize how likely various derogations may be applicable as alternative ways of transferring personal data in particular scenarios.[1772] If exemptions for certain processing activities become recognized, this could lead companies to abandon their current reluctance to rely on such derogations and, to some extent, amend their documented set of data transfer mechanisms. GDPR furthermore allows for other mechanics to justify international transfers, for example an approved Code of Conduct pursuant to GDPR Article 40 and an approved certification mechanism pursuant to GDPR Article 42,[1773] in each case together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards including as regards data subjects' rights. The European Union Agency for Cyber-security ENISA offers a certification framework for products, processes, and services[1774] and the European Data Protection Board issued guidelines on certification as a tool for transfers in 2022.[1775] In addition, the European Commission completed a study on GDPR certification mechanisms pursuant to GDPR Art 42, 43[1776] in which more than one hundred certification schemes have been identified, but only two schemes were highlighted as potential candidates to provide formal certification: the first one is ISDP 10003 offered by ACCREDIA, a scheme that is in line with ISO 17065:2012 and "provides principles and lines of control for a complete compliance assessment of an organization's internal processes regarding protection of personal data with particular reference to proper risk management."[1777] The second is the

[1771] Francesca Gaudino: International data transfer solutions under GDPR. Article published April 19 2020, available at https://globalcompliancenews.com/international-data-transfer-solutions-under-gdpr-23032020/. Retrieved October 22, 2021.

[1772] Ruth Boardman, Louise Hutt, Antonia Boyce at Bird & Bird for IAPP: Article 49 derogations – summary table with examples. Article published May 12 2021, available at https://iapp.org/media/pdf/resource_center/article_49_derogations_summary_table_with_examples_iapp.pdf. Retrieved October 22, 2021.

[1773] See GDPR Article 46 (2e) and (2f).

[1774] The European Commission provides background information on the Cyber-Security Act and ENISA's certification framework at https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en. Retrieved October 22, 2021.

[1775] Guidelines 07/2022 on certification as a tool for transfers published June 2022, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en. Retrieved July 20, 2022. Version 2.0 of EDPB Guidelines 07/2022 on certification as a tool for transfers was adopted on 14 February 2023, and is available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en. Retrieved February 28, 2023.

[1776] European Commission: Data Protection Certification Mechanisms. Study on Articles 42 and 42 of the Regulation EU 2016/679. Final study report published February 2019, available at https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_final.pdf. Retrieved October 22, 2021.

[1777] Background information is provided by the consultancy Inveo (Italian language, only), available at https://in-veo.com/en/certification/isdp-10003-2020-data-protection. Retrieved October 22, 2021.

"European Privacy Seal" offered by EuroPrise for products, services and websites.[1778] As for Codes of Conduct pursuant to GDPR Article 40, the EDPB adopted two Codes of Conduct for cloud providers,[1779] which certainly helps to demonstrate compliance but cannot be considered a formal (GDPR) certification. The same applies to various other certifications, for example ISO 27001 on information security management, ISO 27017, a complementary standard to ISO 27001 for could services, or ISO 27018 which is yet another complementary standard that contains guidelines applicable to cloud service providers that process personal data.[1780] However, developments with cloud providers should be closely monitored: the invalidation of the Privacy Shield lead to additional compliance efforts in the framework of vendor screenings, and it is a positive signal that various stakeholders are working on an EU Cloud Code of Conduct[1781] to propose a legal solution for the transfer of personal data outside the EU as an alternative to the annulled EU-U.S. Privacy Shield. Such a Code of Conduct must of course be approved by data protection authorities, but the Belgian regulator already expressed that they are "impressed by the efforts and resources dedicated by this industry-group to implement best practices for the cloud industry that are both hands-on and respectful of the data subjects."[1782]

7.2.4. Data trustee models

Further promising initiatives to help face challenges with (undesired) international transfer of personal data had been discontinued[1783], for example the data trustee model Microsoft offered together with the German Telekom[1784] with German data centers and a set up that would prevent that data are accessed by or shared with governmental agencies. In 2021, it was announced that the German Telekom will again provide a "Cloud Privacy Service for GDPR compliant use of Microsoft 365".[1785] Data will be

[1778] Further details are provided by EuroPrise who offer privacy seals and certifications, available at https://www.euprivacyseal.com/EPS-en/certifications-offered. Retrieved October 22, 2021.

[1779] EDPB adopts opinions on first transnational Codes of Conduct. Press release published May 20 2021, available at https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_en. Retrieved October 22, 2021.

[1780] Background information on various ISO standards is available at the German Federal Office for Information Security Bundesamt für die Sicherheit der Informationstechnik) at https://www.bsigroup.com/en-GB/ISO-IEC-27018/. Retrieved October 22, 2021.

[1781] Background information on the EU Cloud Code of Conduct including a list of adherent services (providers) is available at https://eucoc.cloud/en/home.html. Retrieved October 22, 2021.

[1782] John Garrett: EU data protection code to replace US/EU data rules. Article published September 16 2020, available at https://www.iteuropa.com/news/eu-data-protection-code-replace-useu-data-rules#:~:text=The%20EU%20Cloud%20Code%20of%20Conduct%20General%20Assembly,personal%20data%20to%20third%20countries%20around%20the%20world. Retrieved October 22, 2021.

[1783] Background information on Microsoft's decision summarized by Esat Dedezade: Microsoft to deliver cloud services from new data centers in Germany in 2019 to meet evolving customer needs. Article published August 31 2018, available at https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/. Retrieved October 22, 2021.

[1784] The project started in 2015, see https://www.webwire.com/ViewPressRel.asp?aId=200848. Retrieved October 22, 2021.

[1785] Hans Peter Schüler: Cloud Privacy Service zur DSGVO-konformen Nutzung von Microsoft 365. Article published September 6 2021, available at https://www.heise.de/hintergrund/Cloud-Privacy-Service-zur-DSGVO-konformen-Nutzung-von-Microsoft-365-6171165.html. Retrieved October 22, 2021.

encrypted, which obviously is a key measure when it comes to facilitating international data transfers: in August 2021, the Belgian Council of State said that encryption is a sufficient measure for U.S. data transfers.[1786] In this context, it is important to note that the issue of government access to personal information is neither novel nor unique to the USA. There are numerous laws that require companies to provide personal data to public authorities, e.g., for financial transactions or in the telecommunications sector. Moreover, in 2018, the European Union proposed[1787] an e-Evidence regulation[1788] that envisages that law enforcement and judicial authorities access electronic evidence for investigation purposes, and which faced criticism.[1789] Some authors claim that this proposal "continues with the disastrous development in dealing with digital platforms: the outsourcing of fundamental rights protection to providers".[1790] The obligation for service providers to cooperate with law enforcement authorities[1791] may be highly desirable from a legislator's point of view. But it must not be forgotten that private sector companies are neither responsible nor qualified for the protection of fundamental rights: How shall an average company[1792] decide whether or not the EPOC[1793] cannot be executed because based on the sole information contained in the EPOC it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive, the addressee shall also send the Form in

[1786] Tanguy van Overstraeten, Julie De Meyer: Belgium: Council of State approves U.S. data transfer. Article published September 16 2021, available at https://www.linklaters.com/th-th/insights/blogs/digilinks/2021/september/belgium-council-of-state-approves-us-data-transfer. Retrieved October 22, 2021.

[1787] Proposal for a Regulation on European production and preservation orders for electronic evidence in criminal matters, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN, and a proposal for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN. Retrieved October 22, 2021.

[1788] Council press release: Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence. Press release published January 25 2023, available at https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/?mkt_tok=MTM4LUVaTS0wNDIAAAGJiRSkCYNAmsS911gcHe_BVdKpBZhGgpe8dKAUdYtXWuEJqxAjJXG0EWuj3q1GUGF0AZkTi230AiUfO152050pU9qtbKWzsKEkJ8utxfzAa_1S. Retrieved January 29, 2023.

[1789] With an open letter, 24 civil society groups jointly called the European Parliament to revise the draft e-Evidence Regulation. Letter published November 24 2022, available at https://international.eco.de/news/eco-signs-a-letter-to-the-european-parliament-e-evidence-regulation-urgently-needs-to-be-improved/. Retrieved January 19, 2023.

[1790] Free translation of a statement within the article "E-Evidence – Outsourcing von Grundrechtsschutz" provided by Martin Schallbruch: e-Evidence: Outsourcing von Grundrechtsschutz (Teil 3). Article published May 10 2028, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/. Retrieved October 17, 2021.

[1791] Vanessa Franssen: The European Commission's E-evidence Proposal – toward an EU-wide obligation for service providers to cooperate with law enforcement? Article published October 12 2018, available at http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/. Retrieved October 17, 2021.

[1792] Any provider is affected regard of its size, meaning that SMEs are also concerned.

[1793] EPOC is the abbreviation for "European Production Order Certificate" and is, like the "European Preservation Order Certificate" (EPOC-PR) one of the cooperation instruments implementing the principle of mutual recognition. Detailed background information on the proposal on electronic evidence is available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf. Retrieved October 17, 2021.

Annex III to the competent enforcement authority in the member state of the addressee.[1794] As a consequence, providers criticize both, the effort associated with the new instruments and the planned transfer of responsibility for checking the legality of the orders.[1795] The issue is of such importance that the OECD dealt with the topic and adopted[1796] the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes, the "Declaration on Government Access to Personal Data held by Private Sector Entities."[1797]

7.2.5. Technical solutions

Various other options[1798] have been discussed at technical level to avoid (government) access to data including personal information, for example encryption or anonymization as well as data localization or the use of so-called private clouds or synthetic data – but they all come along with their own factual limitations, technical difficulties, or legal challenges: anonymization of data is difficult to achieve; many studies have shown that supposedly anonymous data can be re-identified[1799]. Similar problems have been reported for so-called synthetic, i.e., artificially manufactured, data which are currently being discussed[1800] as a privacy-friendly solution, for example in the area of healthcare.[1801] Encryption may not be appropriate for all datasets or may not work for all times due to technological progress,[1802] and the future of such a protective measure is questionable as the EU is thinking about prohibiting

[1794] See Article 9 (5) of the draft proposal.

[1795] Martin Schallbruch: E-Evidence – Outsourcing von Grundrechtsschutz. Article published May 10 2018, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/. Retrieved October 17, 2021.

[1796] Scott Ikeda: OECD nations sign privacy agreement aimed at improving transparency into government access of personal data. Article published December 26 2022, available at https://www.cpomagazine.com/data-privacy/oecd-nations-sign-privacy-agreement-aimed-at-improving-transparency-into-government-access-of-personal-data/?utm_source=ActiveCampaign&utm_medium=email&utm_content=OECD+Nations+Sign+Privacy+Agreement+Aimed+At+Improving+Transparency+Into+Government+Access+of+Personal+Data&utm_campaign=Weekly+Highlights+-+2021. Retrieved January 7, 2023.

[1797] The Declaration on Government Access to Personal Data held by Private Sector Entities adopted December 14 2022, available at https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm. Retrieved January 7, 2023.

[1798] Technical solutions are not the same as technical standards.

[1799] Researchers of the Massachusetts Institute of Technology (MIT) published a study in December 2018 explaining that anonymous data can be re-identified. The corresponding press release is available at https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized. Retrieved October 22, 2021.

[1800] Steven Bellovin, Preetam Dutta, Nathan Reiting: Privacy and synthetic datasets. Stanford Technological Law Review 2019, vol. 22, issue 1, available at https://law.stanford.edu/wp-content/uploads/2019/01/Bellovin_20190129-1.pdf. Retrieved October 22, 2021.

[1801] Bill Siwicki: Is synthetic data the key to healthcare clinical and business intelligence? Article published February 21 2020, available at https://www.healthcareitnews.com/news/synthetic-data-key-healthcare-clinical-and-business-intelligence. Retrieved October 22, 2021.

[1802] Alexander Berengaut, Jayne Ponder, Jorge Ortiz: President Biden signs Quantum Computing Cybersecurity Preparedness Act. Article published January 10 2023, available at https://www.insidetechmedia.com/2023/01/10/president-biden-signs-quantum-computing-cybersecurity-preparedness-act/. Retrieved January 10, 2023.

encryption[1803] to better fight online and / or cyber-crime. Apart from individuals' legitimate security interests, it must not be forgotten that secure communication is essential for a free press or professional secrecy, which makes the balancing of interests very hard. The use of private clouds sounds promising, but apart from access issues, private clouds could simply be less secure than public clouds: cloud service providers can spend much more on security tools than any large, but single enterprise could: the cost of security is diluted across millions of users to fractions of a cent.[1804]

7.2.6. Adequacy decisions

Adequacy decisions are the most effective mechanism for international data transfers as organizations are not required to put in place any specific measures; consequently, some "third countries" stared adapting their data protection laws to be more in line with the GDPR (for example, Brazil) in the hope to obtain the adequacy status one day.[1805] At present, only a handful of countries have been recognized as adequate by the European Commission.[1806] In this regard, the Republic of Korea was the latest addition,[1807] and conversations on EU-Japan mutual adequacy arrangements commenced.[1808] The problem with adequacy decisions is that the Commission adopts adequacy decisions at a slow pace because the European Commission is cautious and wants to ensure that adequacy decisions will prevail. In the framework of the European Parliament's annual review of data-transfer agreements, it was discussed whether California could have its own Privacy Shield arrangement separate from the rest of the U.S. given that California indeed introduced strong privacy rules.[1809] This is a truly interesting development, because many of the Big Tech players have their headquarters in California, and an arrangement with a sub-federal territory is indeed possible under GDPR, because adequacy status can be granted to regions as opposed to countries.[1810] Such a development could once more reshape the

[1803] Katarzyna Lasinska: Encryption policy issues in the EU. Article published May 25 2018, available at https://www.globalpolicywatch.com/2018/05/encryption-policy-issues-in-the-eu/. Retrieved October 22, 2021.

[1804] Jim O'Reilly: Data protection in the public cloud. Article published March 15 2018, available at https://www.networkcomputing.com/data-centers/data-protection-public-cloud-6-steps. Retrieved October 22, 2021.

[1805] Olivier Proust: What future for the transfers of personal data? Article published January 18 2022, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/what-future-for-the-transfers-of-personal-data. Retrieved October 12, 2022.

[1806] The Commission's adequacy decisions are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Retrieved October 12, 2022.

[1807] The Commission's decision on the adequate protection of personal data by the Republic of Korea is available at https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en.

[1808] The joint statement on the first review of the EU-Japan mutual adequacy arrangement dated October 26 2021 is available at https://ec.europa.eu/newsroom/just/items/724795/en. Retrieved November 12, 2021.

[1809] Jennifer Baker: EU Parliament debates: Could California be considered 'adequate' on its own? Article published January 9, 2020, available at https://iapp.org/news/a/eu-parliament-debates-could-california-be-considered-adequate-on-its-own/. Retrieved October 22, 2021.

[1810] Jennifer Baker: California Dreamin': Is a single state EU data protection deal on the cards? The article refers to a statement by Bruno Gencarelli who heads the international data flows and protection unit at the European Commission (DG Justice and Consumers). Article published January 20 2020, available at https://www.cpomagazine.com/data-protection/california-dreamin-is-a-single-state-eu-data-protection-deal-on-the-cards/. Retrieved October 22, 2021.

global landscape for data transfers. At present, it seems that a new adequacy decision for EU-US data transfers is finally underway,[1811] however, stakeholders like NYOB already raised their concerns, and announced their willingness to challenge the Commission's decision.[1812]

7.2.7. Data localization, data residency and data sovereignty

Local data storage has been discussed as an appropriate response to concerns in the framework of international data transfers and global data processing. In fact, many countries around the globe already have specific data localization requirements: some introduced rules for selected industries or certain providers such as social media companies[1813] or for public service providers or for certain types of data like government data, telecommunications (metadata), health records, payment information or geo-data.[1814] It can generally be said that various jurisdictions distinguish between data localization, data residency and data sovereignty[1815]: data residency refers to the geographic location of data storage for regulatory reasons, and data sovereignty is about data being hosted in a country to which the country's laws apply to ensure the country remains in control.[1816] Additionally, many countries restrict transfer of information which they consider relevant for national security, for example information that is relevant for military technology.[1817] However, recent developments show that local data storage might be even more difficult to achieve in the future: Microsoft is experimenting with underwater datacenters[1818] and reports that they are 'reliable, practical and use energy sustainably'. The interesting question here would be which law(s) are applicable in such scenarios. Moreover, data localization and data residency is questionable from both, a data security and a data protection perspective: common reasons for such initiatives are the fight against espionage and crime, strengthening of cyber-security and the pursuit of

[1811] European Commission press release: Commission starts process to adopt adequacy decision for safe data flows with the US. Press release published December 13 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631. Retrieved January 20, 2023.

[1812] See NYOB's open letter on the future of EU-US data transfers, published May 23 2022, available at https://noyb.eu/en/open-letter-future-eu-us-data-transfers. Retrieved January 20, 2023.

[1813] Begüm Yavuzdoğan Okumuş, Direnç Bada: Turkish data localization rules in effect for social media companies. Article published October 14 2020, available at https://gun.av.tr/insights/articles/turkish-data-localization-rules-in-effect-for-social-media-companies?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration. Retrieved October 22, 2021.

[1814] John Selby: Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology 2017, vol. 25, issue 3, pp. 213–232, available at https://academic.oup.com/ijlit/article-abstract/25/3/213/3960261?redirectedFrom=fulltext. Retrieved October 22, 2021.

[1815] Benjamin Vitaris: Data Residency: Meaning, Laws, & Requirements. Article published July 30 2020, available at https://permission.io/blog/data-residency/. Retrieved October 22, 2021.

[1816] For instance, Australia, see the Australian Privacy Principles (APPs) law, available at https://www.oaic.gov.au/privacy/australian-privacy-principles/. Retrieved October 22, 2021.

[1817] Details on export control compliance, including examples of export-controlled are available at https://exportcontrol.lbl.gov/definition/technical-data-technology/. Retrieved October 22, 2021.

[1818] John Roach: Microsoft finds underwater datacenters are reliable, practical and use energy sustainably. Article published September 14 2020 available at https://news.microsoft.com/source/features/sustainability/project-natick-underwater-datacenter/. Retrieved October 22, 2021.

resilience. But technically speaking "physical access to a server or device containing data is neither a necessary nor a sufficient condition for access to information (…). On the other hand, logical access is both necessary, and may be sufficient to provide access to data in an intelligible form, regardless of geographic location".[1819] While no general statement can be made as to whether local data storage may raise security concerns since not all local data centers may have the same (state of the art) level of safety and security, such issues may still arise when using one (single i.e. vulnerable point of failure) location which some therefore describe as the Galapagos syndrome:[1820] a comfortable short-term solution that may lead to long-term extinction. The above examples of why national legislators came up with data localization and data sovereignty should not be seen in isolation: reverse and / or social engineering may also result in loss of know-how from a company and data breach from an individual's perspective; in this regard, data localization cannot help. In many countries, an important factor to foster data localization is to help law enforcement and national security agencies' access to data – but (foreign) government access to personal information was the reason why European Court of Justice dealt with the issue of international data transfers in the framework of their EU-U.S. Privacy Shield decision. Data localization is justified by the need to protect personal information, but the above circumstances explain why there is also fear that (domestic) government access to data through data localization undermines data privacy, and that is why some claim that data localization does not solve the problem of surveillance, but introduces new troubles of its own[1821], including negative political impacts "by bringing information under governmental control".[1822] From a data privacy perspective, it should be taken into consideration that general data protection principles like data minimization, data integrity and confidentiality may not be met if companies must establish and defend multiple versions of its systems across continents with additional hardware, additional vendors and additional staff. Data localization and data residency are complicated and costly and may lead to further fragmentation. Apart from the fact that GDPR's official title explains that the regulation also is about the "free movement of data", the EU commission previously discussed to ban forced data localization,[1823] and it shall be noted that requirements to keep data in Europe would likely violate WTO rules and other global agreements.[1824]

[1819] Christopher Millard: Forced localization of cloud services: Is privacy the real driver? Paper provided for the 2015 forthcoming in IEEE Cloud Computing. Article published May 14, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605926. Retrieved October 22, 2021.

[1820] Chan-Mo Chung: Data localization: The causes, evolving international regimes and Korean practices. Journal of World Trade 2018, vol. 52, issue 2, pp. 187-208.

[1821] Anupam Chander: Is data localization a solution for Schrems II? Article published September 2020, available at https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3318&context=facpub. Retrieved October 22, 2021.

[1822] Erica Fraser: Data localization and the Balkanization of the Internet. Journal of Law, Technology & Society 2016, vol. 13, issue 3, available at https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/. Retrieved October 22, 2021.

[1823] Jennifer Baker: EU Commission aims to ban forced data localization. Article published October 24 2016, available at https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/. Retrieved October 22, 2021.

[1824] Vincent Manancourt, Melissa Heikkilä: Legal experts: EU data proposals break international law. Article published November 4 2020, available at https://www.politico.eu/article/legal-experts-eu-data-proposals-break-international-law/. Retrieved October 17, 2021.

7.3. Emerging U.S. legal landscape

U.S. legislators have been very active in recent years when it comes to regulating privacy and AI: California seems to be leading in the area of data protection as the state worked on several major initiatives: the California Consumer Privacy Act (CCPA),[1825] and the California Privacy Rights Act (CPRA)[1826] are important initiatives in this context, and the Online Privacy Protection Act (CalOPPA)[1827] was the first state law in the nation to require commercial websites and online services to post a privacy policy; it went into effect already in 2004 and was amended in 2013 to require new privacy disclosures regarding tracking of online visits.[1828] In addition, California introduced a chatbot law in 2022 that prohibits the use of undeclared bots to better identify machine generated content,[1829] and California's Privacy Protection Agency which was created under CPRA held its first meeting and is prepared for upcoming rulemaking.[1830] The U.S. privacy landscape became so dynamic that law firms started to provide weekly status information about the status of state privacy legislation.[1831] Several states introduced their own privacy bills with requirements that are somewhat similar to those set forth in the GDPR, for example Washington[1832] which grants consumers various rights such as access, portability, correction, deletion, and the right to object to the processing of their data in certain circumstances, or Virginia: the law requires opt-out for targeted advertising and profiling decisions that produce legal or similarly significant effects and mandatory data protection impact assessment for certain activities including profiling.[1833] Colorado[1834] also enacted privacy legislation that has special

[1825] The bill text of the California Consumer Privacy Act is available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Retrieved October 22, 2021.

[1826] The bill text of the California Privacy Rights Act is available at https://www.caprivacy.org/cpra-text/. Retrieved October 22, 2021.

[1827] The bill text of the Online Privacy Protection Act is available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC. Retrieved October 22, 2021.

[1828] California's Consumer Federation provides background information on various relevant laws, including the Online Privacy Protection Act, available at https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/. Retrieved October 22, 2021.

[1829] California's New Bot Law Prohibits Use of Undeclared Bots became operative on July 1, 2022: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001. Retrieved January 10, 2023.

[1830] Madeline Salinas: California Privacy Protection Agency holds first meeting. Article published June 24 2021, available at https://www.insideprivacy.com/ccpa/california-privacy-protection-agency-holds-first-meeting-preparing-for-upcoming-rulemaking/. Retrieved October 22, 2021.

[1831] David Stauss: Status of proposed CCPA-like state privacy legislation as of May 3, 2021. Article published May 2 2021, available at https://www.bytebacklaw.com/2021/05/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-may-3-2021/. Retrieved October 22, 2021.

[1832] Background information on Washington's Privacy Act (WPA) is available at https://www.consumerprivacyact.com/washington/. Retrieved October 22, 2021.

[1833] Jim Halpert, Lael Bellamy: What Virginia's Consumer Data Protection Act means for your privacy program. Article published March 8 2021, available at https://iapp.org/news/a/what-the-virginia-consumer-data-protection-act-means-for-your-privacy-program/#:~:text=Virginia%27s%20CDPA%20is%20a%20somewhat%20simplified%20version%20of,by%20overwhelming%20margin%20in%20fewer%20than%20two%20months. Retrieved October 22, 2021.

[1834] The bill text of the Colorado Privacy Act is available at https://legiscan.com/CO/drafts/SB190/2021. Retrieved October 22, 2021.

protections for sensitive data and adopted certain privacy-by-design principles,[1835] and New Jersey introduced a notable bill that reminds of GDPR by providing for a right for a consumer not to be subject to a decision based on solely automated decision making.[1836] Numerous other laws establish business obligations and consumer rights related to privacy with provisions about transparency and consent as well as data subject rights or the designation of Privacy Officers,[1837] for example, the Information Transparency & Personal Data Control Act,[1838] the Deceptive Experiences to Online Users Reduction Act,[1839] the Banning Surveillance Advertising Act,[1840] the Social Media Privacy Protection and Consumer Rights Act,[1841] or the Balancing the Rights of Web Surfers equally and responsibly Act.[1842] However, just like the American Data Privacy and Protection Act (ADPPA),[1843] a proposed federal consumer privacy bill that, if enacted into law, would have regulated how organizations keep and use consumer data, most of these laws are addressed to consumers, meaning that either definitions are different or that the scope of these laws is different in comparison to GDPR or any other data protection laws that are concerned with the individual behind the data. This shows that historically, data protection – or more appropriately: privacy – in the U.S. was about consumer protection and vice versa, whereas in continental Europe, data protection initiatives were addressed to the public sector. While the emergence of privacy laws in the U.S. is generally welcomed, some describe recent developments as a "disparate landscape in need of consolidation."[1844] Apart from basic privacy legislation, there is consensus about the need for AI-specific rules.[1845] Consequently, the White House dealt with the issue and provided guidance for the Regulation of AI applications[1846] which on the one hand, aims at promoting the development of trustworthy AI and encouraging public engagement, but on the other

[1835] Angelique Carson: Colorado Privacy Act (CPA): what is it? Article published June 11 2021, available at https://www.osano.com/articles/colorado-privacy-act-what-is-it. Retrieved October 22, 2021.

[1836] For example, the Colorado Privacy Act, Virginia's CDPA or the New Jersey Disclosure and Accountability Transparency Act.

[1837] Müge Fazlioglu: U.S. federal privacy legislation tracker. Article published April 2022, available at https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/. Retrieved July 8, 2022.

[1838] The bill text is available at https://www.congress.gov/bill/117th-congress/house-bill/1816. Retrieved July 8, 2022.

[1839] The bill text is available at https://www.congress.gov/bill/117th-congress/senate-bill/3330. Retrieved July 8, 2022.

[1840] The bill text is available at https://www.congress.gov/bill/117th-congress/house-bill/6416. Retrieved July 8, 2022.

[1841] The bill text is available at https://www.congress.gov/bill/117th-congress/senate-bill/1667. Retrieved July 8, 2022.

[1842] The bill text is available at https://www.congress.gov/bill/117th-congress/senate-bill/113. Retrieved July 8, 2022.

[1843] The text of the bill is available at https://www.congress.gov/bill/117th-congress/house-bill/8152. Retrieved

[1844] Jacob Nix, Pascal Bizarro: U.S. data privacy law: a disparate landscape in need of consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation. Retrieved October 22, 2021.

[1845] Marta Delgado Echevarría et al: European Union – Regulating Artificial Intelligence: European Commission launches proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

[1846] White House guidance for regulation of Artificial Intelligence application published November 17 2020, available at https://www.ai.gov/white-house-guidance-for-regulation-of-artificial-intelligence-applications/. Retrieved October 22, 2021.

hand also intends to promote a "light-touch AI regulatory approach."[1847] In addition, the White House launched a National AI Initiative Office for federal AI coordination,[1848] and is moreover planning for the establishment of a National Security Commission on Artificial Intelligence.[1849] The U.S. are also working on a Algorithmic Justice and Online Platform Transparency Act[1850] which sets forth specific requirements for online platforms, ranging from transparency and documentation – including annual public reports and ad libraries – over prohibition of discrimination up to the establishment of a specific task force to investigate the discriminatory algorithmic processes employed in by online platforms.[1851] The country is also making efforts towards a comprehensive federal privacy legislation,[1852] and in recent years, various AI, algorithmic as well as ADM- and accountability-specific laws have been introduced at federal and state level, for example the Algorithmic Accountability Act,[1853] the Artificial Intelligence Act[1854], the AI in Government Act,[1855] the National Artificial Intelligence Initiative Act,[1856] the Protecting Americans from Dangerous Algorithms Act,[1857] the Artificial Intelligence Reporting Act,[1858]

[1847] Katori Rameau, K.C. Halm: White House issues guidance for AI regulation and non-regulation. Article published January 22 2020, available at https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2020/01/white-house-ai-guidelines. Retrieved October 22, 2021.

[1848] Background information on the National Artificial Intelligence Initiative Office is available at https://trumpwhitehouse.archives.gov/briefings-statements/white-house-launches-national-artificial-intelligence-initiative-office/#:~:text=The%20Office%20is%20charged%20with%20overseeing%20and%20implementing,as%20with%20private%20sector%2C%20academia%2C%20and%20other%20stakeholders. Retrieved October 22, 2021.

[1849] Further details on the plans for the establishment of a National Security Commission on Artificial Intelligence are available at https://www.congress.gov/bill/115th-congress/house-bill/5356/. Retrieved October 22, 2021.

[1850] The bill text of the Algorithmic Justice and Online Platform Transparency Act is available at https://www.congress.gov/bill/117th-congress/senate-bill/1896/text. Retrieved October 22, 2021.

[1851] Pollyanna Sanderson: Automated decision systems legislation update. Presentation held on June 14 2021 during a Future of Privacy Forum meeting.

[1852] Shiva Stella: Senate Releases Principles for Comprehensive Privacy Legislation. Article published November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/. Retrieved October 22, 2021.

[1853] The bill text of the Algorithmic Accountability Act of 2019 is available at https://www.congress.gov/bill/116th-congress/senate-bill/1108. Retrieved October 22, 2021.

[1854] Benjamin Muller: The Artificial Intelligence Act – a quick explainer. Article published May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/. Retrieved October 22, 2021.

[1855] The bill text of the AI in Government Act is available at https://www.congress.gov/bill/115th-congress/senate-bill/3502. Retrieved October 22, 2021.

[1856] The bill text of the National Artificial Intelligence Initiative Act is available at https://www.congress.gov/bill/116th-congress/house-bill/6216. Retrieved October 22, 2021.

[1857] The bill text of the Protecting Americans from Dangerous Algorithms Act Act is available at https://www.congress.gov/bill/117th-congress/house-bill/2154?q=%7B%22search%22%3A%5B%22algorithmic%22%5D%7D&s=1&r=2. Retrieved October 22, 2021.

[1858] The bill text of the Artificial Intelligence Reporting Act is available at https://www.congress.gov/bill/115th-congress/house-bill/6090/. Retrieved October 22, 2021.

the Future of AI Act,[1859] the Advancing American AI Act,[1860] the Advancing AI Research Act,[1861] or the Mind Your Own Business Act.[1862] And there is further legislation aimed at addressing risks in the development and use of AI systems, in particular risks related to algorithmic bias and discrimination: the Digital Platform Commission Act of 2022 has been introduced which would empower a new federal agency, the Federal Digital Platform Commission, to develop regulations for online platforms that facilitate interactions between consumers, as well as between consumers and entities offering goods and services to ensure that algorithms "are fair, transparent, and without harmful, abusive, anticompetitive, or deceptive bias."[1863]

8. Summary and conclusions

The Thesis dealt with the examination of the existing legal framework for Big Data and Artificial Intelligence from a data protection perspective and formulated the following three hypotheses: the failure of privacy self-management, the need for further development of the transparency principle, and the necessity for new controls. To explore the legal framework for Big Data and AI, the Thesis started with an introduction to the history of privacy, the development of data protection laws and the advent of Big Data, automated decision-making and AI. It provided an overview over the characteristics, types, and benefits of Big Data and AI and examined various risks of AI. The Thesis furthermore explored on legal definitions within existing sources of law with a focus on GDPR as a role model law. The Thesis concluded with a digest on relevant legislative initiatives as well as guidance and recommendations for the future regulation of AI and algorithmic systems. The examination of the historical context showed that it is important to distinguish various terms which are used interchangeably, namely, privacy and data protection. The debate is highly valuable to understand what is protected by data protection and data privacy laws and to determine whether present definitions are future-proof. The fact that privacy and the respect for the private life are mentioned in a variety of international conventions also demonstrated that privacy is considered a fundamental right. As such, protective mechanisms have traditionally been directed against the state, and this was reflected in first-generation data protection

[1859] The bill text of the Future of AI Act is available at https://www.congress.gov/bill/115th-congress/house-bill/4625. Retrieved October 22, 2021.
[1860] The bill text of the Advancing American AI Act is available at https://www.congress.gov/bill/117th-congress/senate-bill/1353/text?q=%7B%22search%22%3A%5B%22data+OR+privacy%22%5D%7D&r=27&s=5. Retrieved October 22, 2021.
[1861] The bill text of the Advancing AI Research Act is available at https://www.congress.gov/bill/116th-congress/senate-bill/3891. Retrieved October 22, 2021.
[1862] The bill text of the Mind Your Own Business Act is available at https://www.congress.gov/bill/117th-congress/senate-bill/1444/text?q=%7B%22search%22%3A%5B%22automated+decision-making%22%5D%7D&r=3&s=3. Retrieved October 22, 2021.
[1863] Jennifer Johnson, Nicholas Xenakis, Jayne Ponder, Anna Hevia, Tyler Holbrook, Olivia Dworkin, Will Ossoff: U.S. AI, IoT, CAV, and data privacy legislative and regulatory update. Article published July 13 2022, available at https://www.insideprivacy.com/artificial-intelligence/u-s-ai-iot-cav-and-data-privacy-legislative-and-regulatory-update-second-quarter-2022/. Retrieved July 22, 2022.

laws. The Internet (of things), the growing digitalization, new technologies and new phenomena like social media platforms, together with the growing connectivity of devices, and the overall exponential growth of user, sensor, behavioral, etc. data lead to a well-known problem, the fact that the development of (appropriate) laws takes time. In this context, "cookies" are a good example: while debates are still focused on cookies, there is in fact already new technology which can do without cookies and provide for the same or at least very similar results. Another problem is that there seems to be a shift of protections of fundamental rights to the private sector: some argue that, because GDPR allows for processing based on legitimate interests as well as compatible processing and secondary use of personal information, this may lead to infinite processing or result in a self-regulatory regime. In this regard, the market power of certain companies within the so-called Industry 4.0 has to be taken into consideration: one author's situational analysis is that "Alphabet controls our search and much of our mobile experience, Apple controls the remainder of our mobile and much of our content experience, Amazon controls a large portion of our content experience and much of the Internet of Things, and Microsoft essentially sweeps up everything else."[1864] As a result, a small number of companies may have the power to control a large part of our personal information, perhaps rather based on corporate terms and conditions and less on privacy laws, and the phenomenon became so significant that it has put the antitrust authorities on notice.

As regards definitions**,** these are very significant since the scope and application of laws depend on clarity with regards to the interpretation of relevant definitions, and there are indeed challenges with definitions due to inconsistent terminology in various regulations and inconsistent use of terms within provisions, translation issues, and the introduction of new terms in new relevant laws like the draft AI regulation. It shall be noted that Big Tech players who process personal information at large scale define types of data in a way that is unknown to data protection laws. In their data processing agreements, they distinguish between data entered by users and data generated by systems or otherwise accessed, which shows that there is awareness about the de-facto predominance of indirect data collection. This shows the need for consistent and future-proof definitions. Given the fact that the GDPR has a broad definition of personal data, some speak of the GDPR as the law of everything[1865] because literally all processing seems covered as everything may be regarded as personal data. Moreover, anonymization is technically hard to achieve or cannot be applied to certain data sets where real data is needed as opposed to synthetic or dummy data. Consequently, data protection laws may indeed govern most of what happens with (customer, employee) data within a business.

[1864] Julia Black, Andrew Murray: Regulating AI and Machine Learning: setting the regulatory agenda. European Journal of Law and Technology 2019, vol. 10, issue 3, available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 24, 2021.

[1865] Nadezhda Purtova: The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology 2018, vol. 10, issue 1, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355.

Regarding the benefits, characteristics, and use cases of Big Data and AI, the Thesis explained that the exponential growth of (user, behavioral, sensor) data, the progression of computer science in recent years together with an enhanced infrastructure up to Quantum Computing and thus better speed of processing was a prerequisite for all the Big Data Vs (such as volume, variety, velocity, veracity, variability, volatility, value). It has led to the emergence of an impressive number of AI applications, ranging from Natural Language Processing, Robotics, Computer Sensing and Vision, Machine Learning and Deep Learning, Knowledge Engineering or Neural Networks to name some. While companies welcome the business intelligence that Big Data and Ai made possible by offering real-time insights, analytics, and forecasting, depending on the design and use of underlying algorithms, AI applications may collide with basic privacy principles and may have the potential for threat and harm. That is why this technology had to be evaluated from a risk perspective: the examination of AI risks showed that a common effect of algorithmic processing or automated decision-making and profiling in the context of Big Data, ADM and AI is the secondary use of personal information. Compatible re-use of personal data is admissible to the extent the conditions of GDPR Article 6 (4) are met, i.e. considering the nature of the data in question, the context in which the data were collected, the relationship between the purposes for which the data have been collected and the purposes of further processing, the impact of the envisaged data processing on the data subjects, and the safeguards applied by the controller. Since a major characteristic of many AI applications is a certain degree of autonomy with systems being able to perform in an unsupervised manner, it is questionable whether such data processing operations meet all these requirements or if that may lead to indefinite re-use of personal data which could also render purpose and storage limitation obsolete. Furthermore, data aggregation and data maximization go hand in hand with most Big Data and AI applications, simply because large (training) datasets are needed for most use cases. Big Data is about turning volume to value, but that may conflict with GDPR's principle of data minimization, and it may pose a threat to individuals insofar as there is a risk of (re-) identification: the more datasets grow, and the more data is attributed to a person, the easier it gets to identify the person behind the dataset, and various studies confirmed that actually not much information is needed to uniquely re-identify individuals. The usual practice of constant enrichment of datasets further adds to the risk of identification and profiling: if one and the same person is constantly analyzed and scored this may result in detailed profiles and (online) identities the person is not aware of. Another problem of Big Data and AI applications is that, quite often, external (collateral) data are processed; the upload of address books to social media platforms is a simple example of this risk: whenever a user uploads his individual contacts to a social media platform, the platform receives a full set of contact information of other individuals, and these individuals may not have been informed nor did they consent to such data collection. Further potential risks of AI applications are opaqueness and lack of human oversight. A challenge with Artificial Intelligence is that quite often, important factors are unknown, e.g., details of the processing operations, and the true operators behind those algorithms in the sense of who exactly is responsible for which part of the processing. In many cases, input and output are known, but the workings in between are not, which is also known as the black box effect. The ability of AI to act autonomously and in unforeseeable ways adds to the fear that certain types of AI systems may be considered a Kafkaesque system of unreviewable decision-makers,[1866] and that explains why human oversight may be at risk when algorithms are used for the processing of personal information. Closely connected to the issue of oversight are question of responsibility and liability. While accountability is established as a privacy principle and rated as an important value in literally all publications, fewer texts deal with the fact that AI has the potential to challenge the traditional notions of legal responsibility (and legal personality). In this regard, the European Parliament and the European Commission provided various publications, for example on liability issues in respect of autonomous robots, liability (and safety) implications of Artificial Intelligence and the Internet of Things, or a report on liability for other emerging technologies. In their papers, the EC and EP explain their key findings with regards to new duties of care, strict and vicarious liability, the burden of proof as well as insurance issues. From an individual's perspective, the question would probably primarily be whom to turn to: a court or a regulator or a company, and if so, which one: from a GDPR perspective, there are controllers, processors and joint controllers, but the problem is that and more laws introduce more players: e.g., the DGA, and looking at the categorization of relevant players within the draft AI regulation, the situation becomes even more complex as there are providers, manufacturers, distributors, importers – how should an average person without corresponding expertise be able to tell who is responsible for which part and under which conditions. Big Data and AI applications in many cases raise further concerns, which is a situation literature describes as the information mismatch. Companies must be transparent about the processing of personal data, but even GDPR itself sets limits to transparency obligations: Article 13 (2) lit. f limits the obligation to information about "the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". Details about the significance as well as envisaged consequences of the processing are relative insofar as dynamic processing may simply not allow to foresee all relevant consequences; details about the underlying logic are relative insofar as meaningful information is simply not the same as comprehensibility or reproducibility of decisions. Companies may moreover argue with trade and businesses secrets to avoid having to disclose underlying algorithms they use. Another factor that adds to the mismatch is the dilemma of information asymmetry between users and (Internet, online) service providers, and the situation is worsened by the fact that users in many cases are not aware that seemingly free services may not really come without a service in return, which explains the famous quote that, "if you are not paying for a service, you are the product."[1867] The problem is that individuals unlike

[1866] Daniel Solove uses the term in his book: The digital person: technology and privacy in the information age. New York University Press 2004.

[1867] Ben Kepes: Google users - You're the product, not the customer. Article published December 4 2013, available at https://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/#:~:text=The%20old%20adage%20goes%20that%20if%20you%27re%20not,up%20advertising%20to%20users%20of%20these%20free%20products.

companies do not dispose of enough information to defend themselves "against being sorted in the wrong bucket".[1868] Further risks that have been discussed in the context of Artificial Intelligence are the potential for discrimination for surveillance. The probabilistic nature of individual decision-making and profiling is highly desired from a business perspective, but their inherent opacity together with their potential for discrimination and discrimination is problematic from an individual's perspective, and that is why many believe that these two risks are probably the most important dangers from the point of view of those affected. There consequences of such risks are far-reaching. Employers may turn down job candidates based on social media information without providing candidates with an opportunity to comment on their findings, and this explains the problem of information injustice and information inequality. Some object to the use of AI applications in field of welfare, public administration, and jurisprudence as this may either pave the way or strengthen existing injustices or even restrict the legal process, and consequently, limit access to justice. Demonstrable bias in recidivism scoring systems or bias in healthcare are quite dramatic examples, and they show that AI risks affect individuals and society. The case of Cambridge Analytica demonstrated that the use of AI has a political dimension as well. Influencing voters is traditionally at the core of any campaign, but the problem is that there is little transparency and awareness of how sophisticated this technology is and how cleverly it can be used: AI could be used to create targeted propaganda or to manipulate photos (for morphing purposes) and videos (for Deep Fakes) and this way, pose a threat to democracy.

The above circumstances underline the challenges with the traditional concepts of privacy self-management and transparency: even if lack of transparency is not the problem, transparency as such is problematic since the ineffectiveness of transparency requirements seems to be proven by now. People are as badly informed as they are overtaxed with long and complex privacy notices; people routinely turn over their data for small benefits; people care much more about price-sensitive information than about data protection information; people are much more concerned about social privacy than about institutional privacy, and if people are about to decide about their privacy preferences, they tend to make their lives easy and accept all default settings instead of taking their time to really decide on relevant settings. Even worse, certain Apps take advantage of psychological (behavioral) patterns that can reinforce loss of user control, and legislation on such dark patterns is just in the process of being created. Some authors describe the afore-mentioned challenges around information obligations as the transparency paradox, which is connected to the control paradox, i.e., the problem that affording more control to users does not help them to better protect their privacy. It seems that the opposite is true, affording more control to users does not necessarily lead to a better protection of their data – this may even induce them to reveal more information. If people feel that they have control over their data, they

[1868] Omer Tene: Privacy: For the rich or for the poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html. Retrieved October 23, 2021.

tend to provide more data about themselves. Related observations are known from other fields, for example in the framework of the introduction of the safety belt legislation as people felt more secure with safety belts and drove less carefully. The control paradox is connected to another problem, the security paradox. Security measures such as access controls are principally indispensable. But any such measures require the processing of personal data such as log-in data, and the general risk is that the more data are processed, the larger the risks that data are somehow compromised. Moreover, users are often required to provide a fingerprint in the framework of the authentication process, and that may lead to further risks. The problem is that, unlike a password, there is no reset process for a unique fingerprint, and what is worse, such data can be manipulated very easily, because access to a used object is sufficient to reproduce a fingerprint, and if fingerprints are a mandatory part of official ID-documents, then the individual concerned has a serious problem. Another effect which is connected to the security paradox can be described as the trust paradox. A growing number of people are so used to relying on all kinds of Apps as their single source of truth that there does not seem to be any more room left for own decision making, and that has an impact on how they handle their data. Similar findings were made in the framework of the introduction of COVID apps. The mere fact that technology can track cases of infections does not replace other necessary measures to prevent infections. Therefore, one of the most important observations is that privacy self-management seems to have failed in practice, because the exercise of privacy self-management does not seem to afford the needed protections.

To evaluate whether traditional concepts are still viable, the existing legal framework had to be examined. Consequently, a substantial part of the Thesis is dedicated to the analysis of relevant sources of law to provide an overview over the existing legal framework for processing of personal data and the protection of individuals' rights. At international level, the Universal Declaration of Human Rights, the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, Convention 108+, OECD's Privacy Guidelines as well as further conventions and resolutions underline the human rights dimension of data protection issues. Regarding superior law, it is often overlooked that legally binding global trade agreements play a role in the context of data processing as well since they address trans-border data flows. These agreements set forth certain standards, including norms of non-discrimination that require protections against unjustified data localization requirements. From a data protection perspective, many immediately think of the General Data Protection Regulation as a major piece of legislation and because the GDPR was a milestone in the history of data protection laws and a role model law for many other countries, however, it is not the only relevant regulation. At EU-level only, a variety of other regulations and directives must be taken into consideration when processing of (personal) data, automated decision-making, profiling, Big Data or Artificial Intelligence are in question – be it from a security, database, know-how protection, compliance equal opportunity, or product safety perspective. In terms of existing rules and regulations, it is important to take note of the fact that already at present, various sector or industry specific (e.g. banking: high frequency algorithmic trading), or product specific (e.g. medical devices) as well as purpose (e.g. facial recognition, autonomous driving, autonomous weapons) and data specific (e.g. biometric data, genetic data, health information) laws exist which must be obeyed when Big Data applications and algorithmic systems are used. This is especially true when one has a look at the legal framework in the U.S.A. A federal privacy law is being discussed, and several states either already introduced or are working on laws that specifically deal with algorithm-based data processing and automated decision-making. The U.S.A. are a special case insofar as any legislative attempts de facto have a global impact since all Big Tech players have their headquarters in the U.S.A. – more concretely: California, which can be considered a pioneer of data privacy laws within the U.S. because California more than just one law dealing with data privacy, and the interesting thing is that adequacy status can not only be granted to countries.[1869] In recent years, many countries around the globe introduced their own privacy bills with requirements that are similar to those set forth in the GDPR and which grant consumers various rights such as access, portability, correction, deletion, and the right to object to the processing of their data in certain circumstances; other laws requires opt-out for targeted advertising and profiling decisions that produce legal or similarly significant effects and foresee that mandatory data protection impact assessment must be carried out for certain processing activities including profiling. Documentation requirements and data subject rights often sound familiar; however, the scope is not the same as some laws are rather concerned with consumers than individuals, and conditions for the exercise of data subject rights may vary as well. It can therefore be said that the codification and regulation of systems and applications that use Artificial Intelligence is not in their infancy as there is already a variety of laws that govern the use of AI. The same is true for technical standards, more and more standards are being developed to help with the design and implementation of AI applications. This is not surprising since such technology is already being used across the board, for example, in production (robotics), operations (forecasting), marketing (analytics), finance (scoring), healthcare (diagnostics), in smart cities, smart homes, and smart devices and as well as for (behavioral, online, location) tracking and targeting purposes. In addition, there are numerous national data protection laws and laws with specific provisions pertaining to the processing of personal data, even within the European Union as the General Data Protection Regulation has dozens of opening clauses that either provide or allow for national rules for certain areas (e.g., processing of personal data in the employment context, see GDPR Art. 88) or for certain types of data (e.g., processing of national identification numbers). Depending on the use case in question, further laws may be applicable such as consumer protection and e-commerce or competition laws for marketing activities or labor, equal opportunity and industrial constitution laws in the employment context. The same is true for products or connected devices with a particular focus on information and cyber-security provisions and rules that

[1869] Jennifer Baker: California Dreamin': Is a single state EU data protection deal on the cards? The article refers to a statement by Bruno Gencarelli who heads the international data flows and protection unit at the European Commission (DG Justice and Consumers). Article published January 20 2020, available at https://www.cpomagazine.com/data-protection/california-dreamin-is-a-single-state-eu-data-protection-deal-on-the-cards/. Retrieved October 22, 2021.

apply to the Internet of Things. It can generally be said that data protection laws are on the rise, the legal landscape became very dynamic with numerous data privacy and data security (breach provision) laws as well as specific provisions on the use of sensitive data like biometric or genetic information. Moreover, it should be considered that, for example, Brazil's LGPD has a territorial scope that extends outside of Brazil,[1870] meaning that as a result, global companies to which these laws apply must comply with a multitude of laws. This may lead to the so-called Brussels-effect which guides the way companies are doing business, because multinational organizations adjust their global operations to EU standards to be compliant. Therefore, the existing legal framework is characterized by rising complexity – and opposing legislative aspirations. A technical example is encryption which is desirable from a data protection perspective but at the same time, may be legally prohibited for reasons of crime prevention. This is both, a legislative and a provider trend as recent discussions around certain provider's filter functions show. A legal example is data localization as many countries have introduced data localization requirements, either for selected industries or for public service providers or for certain types of data (for example, government data, health records, or payment information). Another factor to consider is the different approach various legislators take. The European approach is rights-based, the U.S.A. is harm-based, and China pursues a control-based approach, and different jurisdictions focus on different things, for example the U.S. legal landscape is mostly concerned with customers, not all kinds of individuals, and often excluding employees. Probably the greatest difference between the U.S. and the EU approach to data protection is that European law is permission-based, meaning that a legal basis is always required for the processing of personal data, whereas in the US, the contrary is true, because data can generally be processed unless a law explicitly prohibits such an activity. But considering how difficult the exercise of individual rights and privacy-self management in today's Big Tech David vs. Goliath data processing environment is, a harm-based approach may be more of a future-proof concept.

As regards the GDPR, the envisaged harmonization of data protection laws was not achieved, not even within the EU. Differences in the interpretation as to the scope of data privacy laws and in particular data subject rights resulted in data protection being far less uniform than generally assumed. With regards to the question whether GDPR addresses processing with the help of Big Data, ADM, and AI, GDPR's fundamental principles, its permission- and risk-based approach together with a dedicated set of individual rights form a sound foundation for data protection. The General Data Protection Regulation focuses on principles such as lawfulness, fairness, and transparency, data minimization and accuracy, purpose, and storage limitation; existing controller and processor duties include accountability and joint liability, and obligatory vendor contracts and screenings. Documentation and evaluation requirements range from records of processing activities to impact assessments and notices; mandatory consultations

[1870] Caitlin Fennessy: Top five operational impacts of Brazil's LGPD. Part 3: international transfers. Article published November 5 2020, available at https://iapp.org/news/a/top-5-operational-impacts-of-brazils-lgpd-part-3-international-transfers/. Retrieved October 17, 2021.

with data protection supervisory authorities whenever impact assessment indicates that the processing would result in a high risk are also foreseen by law (GDPR Art. 36), and supervisory authorities do not only have the competency to issue fines, they may also impose a temporary or definitive limitation including a ban on processing (GDPR Art. 58 II lit. f). From a data security standpoint, technical and organizational measures, anonymization and pseudonymization, or certifications are required by law, and further measures like codes of conduct are conceivable to achieve an appropriate level of data protection. Therefore, the GDPR does provide a variety of means to deal with (high-risk) processing of personal information. The GDPR is also not silent on various topics that are highly relevant for Big Data, ADM, and AI, for example, consent, profiling, automated decision-making, data subject rights, admissible re-use of personal information, international data transfers, transparency, data security or special categories of personal information. Moreover, GDPR has numerous ambiguities. While data subject rights are strengthened, legitimate interests are an acknowledged legal basis, and compatible processing is admissible under the conditions set forth in GDPR Art 6 IV, which is why some fear this may lead to unlimited processing. There is also controversy about whether profiling under GDPR Art 22 shall be interpreted as a prohibition or a data subject right, and there is not much (consistent) case law to explain GDPR Art 21, the right to object, on grounds relating to his or her particular situation. The fact that the standard of GDPR Art. 22 is only applicable if the decision is based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her sounds like a guarantee, but it also shows that there is a limit to this right, because fully automated means that there is no human intervention at all, which could be circumvented by implementing spot checks. It is also not always clear what has the quality of a decision (or similar legal effect): does that only apply to a final (job candidate selection, loan, or housing application, etc.) decision or should this rather be regarded as a constant criterion for the design of Big Data and AI applications, and thus be applicable to every relevant processing phase? GDPR is perhaps not as far-reaching or future-proof in terms of data subject rights, and GDPR enforcement seems to be a challenge as well. While we have seen several multi-million dollars fines, there has also been a series of fine failures with drastic reductions of penalties of up to 90 % which showed that imposing administrative fines under GDPR might not be easy, because administrative, procedural as well as commercial criminal laws must be taken into consideration as well. With respect to individual rights, GDPR indeed introduced new rights such as the right to data portability, however, some argue that the right to be forgotten or the right to restriction of processing shall be enhanced by adding a right to have data replaced as this may help with preventing identification, and a right to participation and human intervention as that may be useful with the needed social debate at societal and to avoid undesired results at individual level. Moreover, some U.S. laws introduced “Do Not Sell” as an individual right, and that may be more efficient than GDPR’s transparency, information and onwards notification obligation. This approach underlines the awareness for the value of data, the importance of data sovereignty and the significance of today's data-driven businesses which some describe as surveillance capitalism.[1871]

With respect to a possible (future) framework for Big Data and AI, numerous guidelines and recommendations have been issued by public bodies and private sector initiatives as a reaction to the emergence of Big Data and AI as an economic and societal given. At international level, OECD's AI principles as well as the G20, G7 and World Economic Forum recommendations on AI are noteworthy initiatives, ditto for various declarations that have been provided by the United Nations, for example, by UNESCO, UNICRI, UNICEF or UN's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. As for guidance and recommendations at European level, the European Commission was very active by issuing a White Paper on Artificial Intelligence, an Ethical Charter on the Use of AI in Judicial Systems, or the Resolution on Civil Law Rules on Robotics. The Council of Europe also issued recommendations as well as ethics guidelines for trustworthy AI, which is a good example of the fact that the most of these initiatives focus on AI ethics. The same is true for various expert guidelines, civil society and multistakeholder recommendations such as the Toronto and the Montreal Declaration or papers published by the Future of Life Institute and the Centre for Information Policy Leadership. There is also considerable intergovernmental cooperation with regards to Artificial Intelligence, e.g., OECD's Network of Experts on AI, UNESCO's Ad Hoc Expert Group, EU's High-level Expert Group on Artificial Intelligence, or the Global Partnership on AI. As regards to expert / multistakeholder / NGO guidelines, it can be said that these initiatives have in common that they intend to provide useful recommendations for the use of Artificial Intelligence, however, they vary insofar that some guidelines focus on the ethics and responsible use of AI including the future of work, whereas other recommendations are concerned with the classification of AI systems. Most of these papers underline the importance of awareness raising and emphasize the relevance of a human-centered approach to AI and the need for the protection of privacy and intimacy, as well as human control and oversight. Notwithstanding their differences, these initiatives show certain parallels, and a common feature of many international, intergovernmental, multistakeholder, civil society initiatives and expert guidelines is that they stress the relevance, application, and enforcement of existing principles like fairness, accountability, transparency, purpose specification, collection and use limitation data quality, accuracy, Privacy by Design and by Default, and technical and organizational measures. An analysis of propositions relating to AI applications shows that many proposals suggest that any future AI regulations or AI principles shall also take privacy, responsibility, non-discrimination as well as human control of technology and the promotion of human values into consideration.[1872] Some of these initiatives also

[1871] Shoshanna Zuboff: The age of surveillance capitalism – the fight for human future at the new frontier of power. Profile Books, 2019.

[1872] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar: Principled Artificial Intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center Research Publication no. 2020-1 published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. Retrieved October 17, 2021.

address judicial and societal implications of AI applications and examine how to best ensure fair trial and access to justice and welfare how to best protect the freedom of expression, assembly and association, and the right to work in an era of growing automatization and digitalization. Other initiatives elaborated on the question how privacy bills should (not) be written, and they question the concept of rights-based governance where individual rights function as the primary mechanism for governing the collection and processing of personal data since that puts the burden of privacy controls on the individual rather than the controller as such a conventional approach might not be appropriate in the AI era. To that end, some papers propose the strict prohibition of certain AI uses, for example secret profiling and unitary scoring, or facial recognition. Others stress that existing legal framework shall be exploited, for example, by focusing on the principle of accountability. But the question is whether accountability as set forth in existing data privacy laws goes far enough to guarantee responsibility, liability, contestability, safety, and fairness together with an approach to data processing that includes sound risk assessment and human oversight and human intervention if need be. One problem with the application of existing legal principles of data protection is that, even if privacy principles are applied, there is a risk of trade-offs between different data protection principles. Such tensions may arise between the principles of accuracy, fairness and privacy, for example, more data may lead to more accuracy, but at the expense of individual's privacy; if AI is tailored to avoid discrimination, i.e., if certain indicators are removed to that AI is fair, this may have an impact on accuracy; if AI is tested to see if it may be discriminatory, it needs to be tested by using data that is labeled by protected characteristics, but that may be restricted under privacy laws that govern the processing of special category data. The concepts of privacy self-management and transparency are closely connected, and if privacy self-management as a rights-based concept no longer fits the era of AI because it does not seem to afford the needed protections, then the concept of transparency needs to be changed as well given the information mismatch and the inconsistency between peoples' opinions on the relevance of privacy and their actual behavior which tells a different story. Transparency could be further developed by moving away from lengthy one-time notices that address individuals in processing scenarios and which are written by lawyers for lawyers in the direction of comprehensive and meaningful (ad hoc and repetitive, see GDPR Art. 13 III) information including making true operators known: various service providers may be involved in processing operations, but this is not what the average app user gets to know. Publicity could be added on top of transparency, meaning that not only individuals need to be informed, but a wider audience, for example, by establishing public registries allowing any interested party to access relevant information such as details on risk evaluations, mitigation measures and information on sub-processors, and general labeling obligations when humans interact with AI irrespective of legal or other significant effects, and if the AI application makes decisions: mandatory information about the legal and factual scope of the decision, as well as explainability and replicability of decisions. Ideas like mandatory labelling of AI applications and failure transparency, i.e., the obligation to inform the public about mis-developments and errors as well as public registries for (audited) AI apps that establish improved access to information that is not limited to one's own personal information, could help establish a new kind of transparency that exceeds existing standards, moving in the direction of general publicity instead of individual information. This may increase the chances for the needed social debate for this important technology that has the potential to shape our lives, and it could also allow to better exercise individual's rights and foster individual engagement, which is a factor that should not be underestimated as a single data subject's activity has repeatedly brought down an entire framework for international data transfers. The success of such initiatives can be compared to the functioning of the fourth pillar of the state which, in addition to the executive, legislative and judicial branches, can influence developments through reporting and public discussion. And public debate is an important instrument as it allows for better insight into how algorithmic apps can be used like the case on leaks on Meta's practices such as design decisions that may influence the spread of misinformation or have a negative impact on users' mental health[1873] has proven. From an individual's perspective, some underline the need for the establishment of new data subject rights such as the right to participation or the right to human intervention or examine the idea of having personal information replaced rather than having the processing restricted, because that might be a more effective way to avoid re-identification and help with non-linkability. They moreover demand enhanced redress mechanisms and broaden the right of action for consumer protection and competition authorities or advocate to foster the use of anonymized and synthetic data whenever possible. There are also debates about data ownership to fight data monetization, but it is questionable how that may work in practice, however, contractual limitations of the use of personal data are not unimaginable given that service-for-data is a well-established business model, but at present, it is strictly unilateral. Given AI's capability for surveillance and its potential impact on human rights and democracy, some recommendations dealt with new requirements such as mandatory human rights impact assessments and termination obligations in the event a system gets out of control. Others recommend the introduction of further principles such as non-discrimination and inclusion, equality and diversity that should be applied whenever algorithmic processing is in question. Some of the guidelines emphasize the need for a new kind of accountability which shall include "all players" in the data value chain; GDPR sets forth controller and processor responsibilities, but it does not necessarily address manufacturers: the law is concerned with the processing of data, not products. Digital workforce aspects show that there is an important intersection between individuals rights and societal values, and some therefore claim that new controls shall also include new values which are not only judged from an individual's perspective but consider the societal perspective and include public safety obligations. The mass application of Big Data, AI and automated decision-making not only affects individuals, but society so that many initiatives focused on a human-centric approach that serves society and explored on embedding ethics into Big Data, ADM, and AI, and. But embedding ethics may be problematic as

[1873] Ryan Browne: Facebook whistleblower behind major leak is going to testify in Europe. Article published October 12 2021, available at https://www.cnbc.com/2021/10/12/facebook-whistleblower-behind-major-leak-is-going-to-testify-in-europe.html. Retrieved January 22 2022.

the interpretation of ethical standards may vary; what might not be acceptable to some, may be acceptable to others, and this approach was also criticized as some consider that ethics may be an escape from regulation.[1874] It is comprehensible that industry may prefer a deregulated landscape for novel technology claiming that regulation stifles innovation, but self-regulation has not proven to work,[1875] and therefore, many voices explore on new algorithmic accountability codes instead of voluntary codes of conduct, and call for the establishment of mandatory auditing and monitoring of AI systems. Ditto for standardization of testing procedures, because poor data quality and errors in the design of AI apps may lead to bias and discrimination. Many also recommended the formation of specialist independent oversight bodies with simplified coherence mechanisms, including the right to issue orders against any processor or manufacturer to capture all players, and many initiatives insist on the prohibitions of certain AI applications, for example, for secret profiling, or the right not to be subject to a discriminatory decision, which shall be interpreted as an interdiction. AI can be used in novel ways, for example, by exploiting human vulnerabilities (e.g., by using speech synthesis for impersonation), by utilizing existing software vulnerabilities (e.g., through automated hacking) or the vulnerabilities of AI systems (e.g., through data poisoning or by introducing training data that causes a learning system to make mistakes or by inputs designed to be misclassified by Machine Learning systems). The potential for malicious use is one thing, AI's dual use character another: already today, AI is incorporated in "slaughter-bots," and that is why the United Nations discussed a ban[1876] on such technology; algorithmic errors in this context do not cause IT bugs that need fixing, but could lead to humans being killed,[1877] and the fact that the European Parliament,[1878] the Commission,[1879] and the Council[1880] address this gives

[1874] Ben Wagner: Ethics as an escape from regulation. From ethics-washing to ethics-shopping? In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds,): Being profiled – cogitas ergo sum. 10 years of profiling the European citizen. Amsterdam University Press 2018, pp. 84-88.

[1875] MEP Christel Schaldemose is quoted by Euronews in their October 5 2021 news entry: Frances Haugen whistleblower leaks show Facebook cannot regulate itself, MEPs say. Article available at https://www.euronews.com/next/2021/10/05/frances-haugen-whistleblower-leaks-show-facebook-cannot-regulate-itself-meps-say. Retrieved January 22, 2022.

[1876] Sam Shead: UN talks to ban 'slaughter-bots' collapsed – here's why that matters. Article published December 22 2021, available at https://www.cnbc.com/2021/12/22/un-talks-to-ban-slaughterbots-collapsed-heres-why-that-matters.html. Retrieved January 22, 2022.

[1877] James Dawes: An autonomous robot may have already killed people – here's how the weapons could be more destabilizing than nukes. Article published September 29 2021, available at https://theconversation.com/an-autonomous-robot-may-have-already-killed-people-heres-how-the-weapons-could-be-more-destabilizing-than-nukes-168049. Retrieved October 22, 2021.

[1878] Background information on the European Parliament's civil law rules on robotics is provided by the European Parliament, available at https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-civil-law-rules-on-robotics#:~:text=On%2017%20February%202017%20the%20Parliament%20called%20upon,a%20European%20agency%20for%20robotics%20and%20artificial%20intelligence. Retrieved October 22, 2021.

[1879] Details on the Commission's work are provided by Samuel Stolton: Commission reveals details on future EU robotics policy. Article published February 4 2021, available at https://www.euractiv.com/section/digital/news/commission-reveals-details-on-future-eu-robotics-policy/. Retrieved October 22, 2021.

[1880] The Council's Ad hoc Committee on Artificial Intelligence (CAHAI) has been succeeded by CAI and continues to work on AI issues. Details on CAI's work and initiatives are provided on the Council's website, available at https://www.coe.int/en/web/artificial-intelligence/cai. Retrieved January 20, 2023.

cause to hope. It is incomprehensible why this technology should be treated in a different manner than other technology for which imminent high risks have been identified; nuclear power, drugs or weapons and autonomous vehicles are typical examples where nobody would seriously argue against the need for a legal framework that addresses these risks. An important conclusion therefore is that new controls are needed, including a specific liability regime in accordance with product liability regulations which should cover all involved providers. Further recommendations for the future regulation of AI stress the importance of technical standardization or certifications, the need for external control mechanisms including the establishment of specific AI supervisory bodies or compulsory public archives and the introduction of termination obligations. There is a need for clear statements on and limits of certain use cases such as social scoring to rate citizens' behavior, because such uses of Big Data and AI may have an impact on fundamental rights such as freedom of expression,[1881] freedom of assembly and association,[1882] liberty, security[1883] and fair trial,[1884] physical, psychological, and moral integrity,[1885] as well as prohibition of discrimination.[1886] In this context, the proposals for the AI Act and for AI liability immediately attracted a lot of attention and received numerous comments: positive ones due documentation and evaluation requirements and owing to the establishment of a European AI board and a public database; negative ones for unclear definitions, the missing right to compensation, numerous exceptions, and the "missed opportunity to draw red lines for certain technologies."[1887] Unsolicitous codices, optional self-regulation, or ethics rules may not be sufficient to mitigate the risks posed by Big Data, automated decision-making, and Artificial Intelligence because AI applications may have an impact on human rights, and most importantly, not the private sector, but the state and the legislature are called to protect individual's fundamental rights. Consequently, new controls are needed such as external audits, specialist oversight bodes, technical standards, and public registries – steps which are already foreseen in some legislative drafts for the future regulation of Artificial Intelligence. This shall be welcomed since "legislative history in the course of industrial revolutions and across various sectors, be it transportation, chemical engineering, communications, aviation or biotechnology and digitization has shown that voluntary codes or self-regulation may simply not work, and that regulatory discussions should not primarily focus on specific harms or individual risks but also take the systemic and structural risk of Artificial Intelligence into consideration.[1888] Given the potential risks of AI, it is time to treat this technology like any other potentially hazardous technology, that is, enforce and enhance comprehensive

[1881] See UDHR Art. 19 and ECHR Art. 10.
[1882] See UDHR Art. 20 and ECHR Art. 11.
[1883] See UDHR Art. 3 and ECHR Art. 6.
[1884] See UDHR Art. 10 and ECHR Art. 47.
[1885] See UDHR Art. 3 and ECHR Art. 3.
[1886] See UDHR Art. 19 and ECHR Art. 21.
[1887] Friederike Reinhold, Angela Müller: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – a major step with major gaps. Article published April 22 2021, available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/. Retrieved October 22, 2021.
[1888] Julia Black, Andrew Murray: Regulating AI and Machine Learning: setting the regulatory agenda, European Journal of Law and Technology 2019, vol. 10, issue 3, available at https://ejlt.org/index.php/ejlt/article/view/722/980. Retrieved October 22, 2021.

regulation and risk mitigation, taking into consideration existing privacy, security, product, liability, machinery, consumer, e-commerce, employment, anti-discrimination as well as any other applicable data-, purpose-, or sector specific laws and corresponding legal initiatives around the use of Big Data, ADM and AI into consideration. There are also interesting alternative approaches to issues that arise with the use of Algorithms and Artificial Intelligence such as the call for a Hippocratic oath for data scientists, and that may perhaps be truly needed as algorithms may promote depression and self-harm or even suicide: some authors raised their voice to underline that AI regulation shall address critical manipulative methods as there have already been cases in which it was reported that algorithms enforced teenager's depression with fatal consequences.[1889] One of the greatest challenges from a legislative and regulatory point of view is the failure to recognize[1890] that many of the new technologies not only pose challenges to individuals, but society, meaning that legal initiatives and approaches shall be adjusted accordingly, which is confirmed by the fact that Recital 4 says that "the processing of personal data should be designed to serve mankind.".

[1889] Matija Franklin, Hal Ashton, Rebecca Gorman, Stuart Armstrong: The EU's AI Act needs to address critical manipulation methods. Article published March 21 2023, available at https://oecd.ai/en/wonk/ai-act-manipulation-methods. Retrieved March 23, 2023.

[1890] Alexander Roßnagel, Christian Geminn: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. Report published November 26 2019, available at https://www.heise.de/downloads/18/2/8/0/2/5/0/7/vzbv.pdf. Retrieved October 20, 2021.

Bibliography

This section consists of two parts: the bibliography reflects the literature review. The second part provides an overview of relevant resources: conventions, regulations, directives, resolutions, trade agreements as well as non-binding initiatives, recommendations, and guidance at international, EU and non-governmental level, as well as various technical standards.

ABRAMS Martin: 50 year heritage of the Fair and Open Use Act. Article published June 24 2021, available at https://informationaccountability.org/2021/06/50-year-heritage-of-the-fair-and-open-use-act/.

ABRAMS Martin: Time to break the privacy legislative paradigm – IAF Model Legislation. Article published June 3 2021, available at https://informationaccountability.org/2021/06/time-to-break-the-privacy-legislative-paradigm-iaf-model-legislation/.

ACCESSNOW: Europe's approach to artificial intelligence: How AI strategy is evolving. Report published December 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf.

ACCESSNOW: EU AI Act must protect all people, regardless of migration status. Article published December 6 2022, available at https://www.accessnow.org/eu-ai-act-migration-status/.

ADAMEK, Max, RÄDER, Julian: DSGVO-Verstöße und das OWiG. Article published August 20 2021, available at https://haerting.de/wissen/dsgvo-verstoesse-und-das-owig/#:~:text=Gem.%20%C2%A7%2030%20Abs.%201%20Nr.%205%20OWiG,handelt%20und%20eine%20Straftat%20oder%20Ordnungswidrigkeit%20begangen%20hat.

AGOMUOH Fionna: ChatGPT has a new way to detect its own plagiarism. Article published February 1 2023, available at https://www.digitaltrends.com/computing/chatgpt-new-way-to-detect-plagiarism/.

ALAN TURING INSTITUTE: AI, ethics, and the law: what challenges and what opportunities. Article published January 18 2018, available at https://aticdn.s3-eu-west-1.amazonaws.com/2018/03/140318-Ai-ethics-and-the-law-public-panel-report.pdf.

Van ALSENOY Brendan: Liability under EU Data Protection Law - from Directive 95/46 to the General Data Protection Regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2016.

AMNESTY INTERNATIONAL, PRIVACY INTERNATIONAL and the CENTRE FOR RESEARCH ON MULITINATIONAL CORPORATIONS: "Operating from the shadows." Report published 2021, available at https://www.privacyinternational.org/sites/default/files/2021-06/DOC1041822021EN.pdf.

ANDERSON Kenneth, WAXMAN Matthew: Law and ethics for Autonomous Weapon Systems: Why a ban won't work and how the laws of war can, American University Washington College of Law Research Paper no. 2013-11. The article is available at http://ssrn.com/abstract=2250126.

ANDREI Mihai: Japanese phenomenon of extreme social isolation – and why it seems to be spreading. Article published January 22 2021, available at https://www.zmescience.com/science/hikikomori-loneliness/.

ANGWIN Julia, LARSON Jeff, MATTU Surya, KIRCHNER Lauren: Machine Bias: There's software used across the country to predict future criminals. Article for ProPublica published May 23 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

AUSSENAC-GILLES Nathalie, CHARLET Jean, REYNAUD Chantal: Knowledge Engineering. A Guided Tour of Artificial Intelligence Research. Springer Publishing 2020.

AYLETT-BULLOCK Caragh: Automating insecurity – decision making in recruitment. Article published March 13 2022, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment.

BADA Adebusola: UK tribunal rejects application for £ 2.3 billion class action suit against Meta. Article published February 21 2023, available at https://www.jurist.org/news/2023/02/uk-tribunal-rejects-application-for-2-3-billion-class-action-suit-against-meta/#:~:text=The%20UK%E2%80%99s%20competition%20tribunal%20Monday%20rejected%20an%20application,required%20for%20the%20class%20action%20to%20move%20forward.

BADER Sebastian, HITZLER Pascal: Dimensions of neural-symbolic integration – a structured survey. Article published November 10 2005, available at https://arxiv.org/pdf/cs/0511042.pdf.

BAKER Jennifer: California Dreamin': Is a single state EU data protection deal on the cards? Article published published January 20 2020, available at https://www.cpomagazine.com/data-protection/california-dreamin-is-a-single-state-eu-data-protection-deal-on-the-cards/.

BAKER Jennifer: EU Parliament debates: Could California be considered 'adequate' on its own? Article published January 9 2020, available at https://iapp.org/news/a/eu-parliament-debates-could-california-be-considered-adequate-on-its-own/.

BAKER Jennifer: What does the newly signed 'Convention 108+' mean for UK adequacy? Article published October 30, 2018, available at https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/.

BAKER Jennifer: EU Commission aims to ban forced data localization. Article published October 24 2016, available at https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/.

BARHAM Husam: Achieving competitive advantage through Big Data – a literature review. Conference paper for the 2017 International Conference on Management of Engineering and Technology (PICMET) at Portland, Oregon, USA. Conference paper available at https://www.researchgate.net/publication/318351614_Achieving_Competitive_Advantage_Through_Big_Data_A_Literature_Review.

BARNES Neil: Data – a new direction: what is it & what is being proposed? Article published July 19 2022, available at https://www.bulletproof.co.uk/blog/data-a-new-direction#:~:text=UK%20government%27s%20new%20proposals%20are%20designed%20to%20reform,need%20for%20DPOs%2C%20DPIAs%2C%20LIAs%2C%20ROPAs%20and%20DSARs.

BARNETT John: Will AI revolution lead to mass unemployment? What Artificial Intelligence might mean for your job and industry. Article published April 25 2017, available at https://www.business.com/articles/john-barnett-artificial-intelligence-job-market/#:~:text=Well%2C%20the%20real%20answer%20lies%20somewhere%20in%20between.,will%20result%20in%20huge%20losses%20and%20then%20layoffs.

BARROS VALE Sebastiao, ZANFIR-FORTUNA Gabriela for the Future of Privacy Forum: Automated decision-making under the GDPR: practical cases from courts and data protection authorities. Report published May 17 2022, available at https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/.

BARTH Susanne, De JONG Menno: The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior: a systematic literature review. Journal of Telematics and Informatics 2017, vol. 34, issue 7, pp. 1038-1058.

BASHIR Masooda, HAYES Carol, LAMBERT April, KESAN, Jay: Online privacy and informed consent: The dilemma of information asymmetry. Proceedings of the Association for Information Science and Technology 2015, vol. 52, issue 1, pp. 1-10.

BAYERN May: Autonomous vehicles: How seven countries are handling the regulatory landscape. Article published February 5 2020, available at https://www.techrepublic.com/article/autonomous-vehicles-how-7-countries-are-handling-the-regulatory-landscape/.

BÄUMLER Helmut, von MUTIUS Albert: Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts. Luchterhand Publishing 1999.

BEAUMONT Samantha: The data protection directive versus the GDPR: understanding key changes. Article published March 6 2018, available at https://www.grcworldforums.com/gdpr/the-data-protection-directive-versus-the-gdpr/26.article#:~:text=%20The%20data%20protection%20directive%20versus%20the%20GDPR%3A,vs.%20Data%20Processors.%20A%20key%20difference...%20More%20.

BEEDHAM Matthew: Why Tesla’s in-car monitoring camera is a major privacy risk. Article published March 24 2021, available at https://thenextweb.com/news/teslas-driver-monitoring-cameras-privacy-risk.

BEIOLEY Kate: Metaverse vs employment law: the reality of the virtual workplace. Article published February 21 2022, available at https://www.ft.com/content/9463ed05-c847-425d-9051-482bd3a1e4b1.

BEKKER Alexander: Twenty Big Data use cases. Article published March 6 2018, available at https://www.experfy.com/blog/twenty-big-data-use-cases.

BELL Lee: Machine Learning versus AI: what's the difference? Article published December 1 2016, available at https://www.wired.co.uk/article/machine-learning-ai-explained.

BELLOVIN Steven, DUTTA, Preetam, REITING, Nathan: Privacy and synthetic datasets. Stanford Technological Law Review 2019, vol. 22, issue 1.

BENDER David: GDPR harmonization: Reality or myth? Article published June 7, 2018 on IAPP’s website, available at https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/.

BENICHOU Brahim, De BRUYNE Jan, GILS Thomas, WAUTERS Ellen: Regulating AI in the European Union: seven key takeaways. Article published February 25 2020, available at https://ai-laws.org/2020/02/regulating-ai-in-the-european-union-seven-key-takeaways/.

BERENDT Bettina, PREIBUSCH Sören: Toward accountable discrimination-aware data mining- the importance of keeping the human in the loop. Big Data. 2017, vol. 5, Nr. 2, pp. 135-152.

BERENGAUT Alexander, PONDER Jayne, ORTIZ Jorge: President Biden signs Quantum Computing Cybersecurity Preparedness Act. Article published January 10 2023, available at https://www.insidetechmedia.com/2023/01/10/president-biden-signs-quantum-computing-cybersecurity-preparedness-act/.

BERTUZZI Luca: AI standards set for joint drafting among European standardization bodies. Article published May 30 2022, updated June 2 2022, available at https://www.euractiv.com/section/digital/news/ai-standards-set-for-joint-drafting-among-european-standardisation-bodies/.

BHASKAR Rohith: 5G: Why is it the next big thing? Article published February 22 2021, available at https://www.moneycontrol.com/news/technology/5g-why-is-it-the-next-big-thing-6555881.html.

BHUNIA Priyankar: Plans for cloud-first strategy and national AI framework revealed at 29th MSC Malaysia Implementation Council Meeting. Article published October 28 2017, available at https://opengovasia.com/plans-for-cloud-first-strategy-and-national-ai-framework-revealed-at-29th-msc-malaysia-implementation-council-meeting/.

BINDI Tas: Amazon, Google, Facebook, IBM, and Microsoft form AI non-profit. Article published September 29 2016, available at https://www.zdnet.com/article/amazon-google-facebook-ibm-and-microsoft-form-ai-non-profit/.

BINNS Reuben, GALLO Valeria: Trade-offs. Article published published July 25 2019, available at https://ico.org.uk/about-the-ico/news-and-events/ai-blog-trade-offs/.

BLACK Julia, MURRAY Andrew: Regulating AI and Machine Learning: setting the regulatory agenda. European Journal of Law and Technology 2019, vol. 10, issue 3.

BLACKMAN James: Operational intelligence, three ways – descriptive, predictive, and prescriptive. Article published December 11 2018, available at https://enterpriseiotinsights.com/20181211/channels/fundamentals/descriptive-predictive-prescriptive-analytics.

BLAIR Keily, HALL James, SCHRÖDER Christian, SUSSMAN Heather, YAROVSKY Shannon: The new EU approach to the regulation of Artificial Intelligence. Article published May 10 2021, available at https://www.jdsupra.com/legalnews/the-new-eu-approach-to-the-regulation-4438826/.

BOARDMAN Ruth, HUTT Louise, BOYCE Antonia: Article 49 derogations – summary table with examples. Article published May 12 2021, available at https://iapp.org/media/pdf/resource_center/article_49_derogations_summary_table_with_examples_iapp.pdf.

BOBRIAKOV Igor: Top 10 data science use cases in retail. Article published July 22 2018, available at https://medium.com/activewizards-machine-learning-company/top-10-data-science-use-cases-in-retail-6483accc6042.

BOGLE Ariel: Australian Federal Police officers trialed controversial facial recognition tool Clearview AI. Article published April 15 2020, available at https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894.

BOLTON Doug: The rise of artificial intelligence could put millions of human workers out of jobs - could a basic income be a solution? Article published February 19 2016, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/basic-income-artificial-intelligence-ai-robots-automation-moshe-vardi-a6884086.html.

BORGESIUS Frederik, POORT Joost: Online price discrimination and EU data privacy law. Journal of Consumer Policy 2017, vol. 40, issue 3, pp. 347-366.

BORSA Diana, PIOT Bilal, MUNOS Rémi, PIETQUIN Olivier: Observational learning by reinforcement learning. Article published June 20, 2017, available at https://arxiv.org/abs/1706.06617.

BRADFORD Anu: The Brussels Effect - How the European Union rules the world. Oxford University Press 2020.

BRANDIMARTE Laura, ACQUISTI Alessandro, LOEWENSTEIN George: Misplaced confidences – Privacy and the control paradox. Article published August 9 2012, available at http://www.futureofprivacy.org/wpcontent/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf.

BRANDOM Russell: New Toronto Declaration calls on algorithms to respect human rights. Article published May 16 2018, available at https://www.theverge.com/2018/5/16/17361356/toronto-declaration-machine-learning-algorithmic-discrimination-rightscon.

BRETTHAUER Sebastian in: Louisa Specht/Reto Manz: Handbuch europäisches und deutsches Datenschutzrecht. C.H. Beck Publishing 2019.

BREUER Marten: The Council of Europe as an AI standard setter. Article published April 4 2022, available at https://verfassungsblog.de/the-council-of-europe-as-an-ai-standard-setter/.

BRIGGS Alan: Government guidance –10 core principles for stewardship of AI apps. Article published January 15 2020, available at https://pubsonline.informs.org/do/10.1287/LYTX.2020.01.18n/full/.

BROWNE Ryan: Facebook whistleblower behind major leak is going to testify in Europe. Article published October 12 2021, available at https://www.cnbc.com/2021/10/12/facebook-whistleblower-behind-major-leak-is-going-to-testify-in-europe.html.

BRUNDAGE Miles et al: The Malicious use of Artificial Intelligence: forecasting, prevention, and mitigation. Article published February 2018, available at https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217.

BRÜHL Jannis, HURTZ Simon: Eine Software schockiert Amerika. Article published January 20 2020, available at https://www.sueddeutsche.de/digital/gesichtserkennung-clearview-app-polizei-gesicht-1.4764389.

BRYANT Jennifer: Irish DPC fines Meta 390M euros over legal basis for personalized ads. Article published January 4 2023, available at https://iapp.org/news/a/irish-dpc-fines-meta-390m-euros-over-legal-basis-for-personalized-ads/.

BUCHHOLTZ Gabriele, STENTZEL Rainer in: Gierschmann, Schlender, Stentzel, Veil: Kommentar zur Datenschutzgrundverordnung. Bundesanzeiger Publishing 2017.

BUCHNER Benedikt, KÜHLING Jürgen in Kühling/Buchner: Kommentar zur DSGVO. C.H. Beck Publishing 2016.

BUCKWELL Matthew: EU Commission proposes to update the NIS/Cybersecurity Directive only two years after implementation. Article published January 2021, available at https://www.twobirds.com/en/news/articles/2021/global/eu-commission-proposes-to-update-the-nis-cybersecurity-directive-only-two-years-after-implementation.

BÜCKING Jens: Datenschutzgrundverordnung, NIS-Richtlinie der EU und das IT-Sicherheitsgesetz – ein neues, einheitliches Datensicherheits-/Datenschutzrecht für Europa. Working Paper published January 10 2018, available at https://www.sep.de/fileadmin/user_upload/Compliance/SEPsesam_Compliance_de_web.pdf.

BUNYAN Tony: The “point of no return” - Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases.

Paper published July 2018, available at https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf.

BUSCH Danny: MiFID II - Regulating high frequency trading, other forms of algorithmic trading and direct electronic market access. Law and Financial Markets Review 2016/2, available at https://ssrn.com/abstract=3068104 or http://dx.doi.org/10.2139/ssrn.3068104.

CADWALLADR Carole: AggregateIQ – the obscure Canadian tech firm and the Brexit data riddle. Article published March 21 2018, available at https://www.theguardian.com/uk-news/2018/mar/31/aggregateiq-canadian-tech-brexit-data-riddle-cambridge-analytica.

CADWALLADR Carole, TOWNSEND Mark: Revealed – the ties that bound Vote Leave's data firm to controversial Cambridge Analytica. Article published March 24 2018, available at https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions.

CALDAROLA Maria Cristina, SCHREY Joachim: Big Data und Recht. C.H. Beck Publishing 2019.

CALO Ryan: The boundaries of privacy harm. Indiana Law Journal 2011, vol. 86, no. 3.

CANTER Libbi, YERGIN Rebecca: Newly effective Florida law imposing criminal sanctions adds to developing nationwide patchwork of state genetic privacy laws. Article published October 6 2021, available at https://www.insideprivacy.com/health-privacy/newly-effective-florida-law-imposing-criminal-sanctions-adds-to-developing-nationwide-patchwork-of-state-genetic-privacy-laws/.

CAPONE Bruno: Intrusion detection based on Deep Learning. Article published October 16 2020, available at https://www.aitech.vision/en/2020/10/16/intrusion-detection-based-on-deep-learning/.

CARSON Angelique: Colorado Privacy Act (CPA): What is it? Article published June 11 2021, available at https://www.osano.com/articles/colorado-privacy-act-what-is-it.

CATE Fred, MAYER-SCHÖNBERGER Viktor: Notice and consent in a world of Big Data. International Data Privacy Law 2013, vol. 3, no. 2.

CAVOUKIAN Ann, JONAS Jeff: Privacy by Design in the age of Big Data. Article published June 8 2012, available at https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf.
Center for Information Policy Leadership: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. Paper published December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

CENTRE FOR INFORMATION POLICY LEADERSHIP: Essential legislative approaches for enabling cross-border data transfers in a global economy. White Paper publishesd September 25 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf.

CEMPER Christoph: 13 AI content detection tools tested and AI watermarks. Article published December 29 2022, available at https://www.linkresearchtools.com/blog/ai-content-detector-tools/.

CERULUS Laurens: Europe to crack down on surveillance software exports. Article published October 15 2020, available at https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/.

CHANDER Anupam: Is data localization a solution for Schrems II? Article published September 2020, available at https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3318&context=facpub.

CHAUHAN Nagesh Singh: Introduction to artificial neural networks. Article published October 13, 2019, available at https://towardsdatascience.com/introduction-to-artificial-neural-networks-ann-1aea15775ef9.

CHEEVER Nancy, ROSENBLATT Larry, CARRIER Mark, CHAVEZ Amber: Out of sight is not out of mind: The impact of restricting wireless mobile device use on anxiety levels among low, moderate and high users. Computers in Human Behavior 2014, vol. 37, pp. 290-297.

CHOI Jay, JEON Doh-Shin, KIM Byung-Cheol: Privacy and personal data collection with information externalities. Journal of Public Economics 2019, vol. 173, pp. 113-124, available at https://www.sciencedirect.com/science/article/abs/pii/S0047272719300131.

CHOUDHURY Saheli: Malicious use of A.I. could turn self-driving cars and drones into weapons, top researchers warn. Article published February 21 2018, available at https://www.cnbc.com/2018/02/21/malicious-use-of-ai-by-hackers-could-pose-security-risks-threats.html.

CHOUHBI Kamal: Hippocratic Oath for data scientists – the ethical checklist that every data scientist must follow. Article published October 6 2020, available at https://towardsdatascience.com/hippocratic-oath-for-data-scientists-407d2db15a78.

CHRISTAKIS Theodore, BECUYWE Mathis: Pre-market requirements, prior authorisation and lex specialis – novelties and logic in the facial recognition-related provisions of the draft AI Regulation. Article published May 4 2021, available at https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/.

CHUNG Chan-Mo: Data localization: The causes, evolving international regimes and Korean practices. Journal of World Trade 2018, vol. 52, issue 2, pp. 187-208.

De CICCO Diletta, HELLEPUTTE Charles-Albert: The EU Artificial Intelligence Act. Article published May 2021, available at https://www.steptoeinternationalcomplianceblog.com/files/2021/05/AI_Infographic-1.pdf.

CIMPANU Catalin: Chinese company leaves Muslim-tracking facial recognition database exposed online: Researcher finds one of the databases used to track Uyghur Muslim population in Xinjiang. Article published February 14 2019, available at https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/.

CITRON KEATS Danielle, SOLOVE Daniel: Privacy harms, published February 2021 at George Washington Law School Public Law and Legal Theory Paper no. 2021-11.

CLARK Sam: Draft SCC clash with Irish law reaches European Commission. Article published February 25 2021, available at https://globaldatareview.com/data-privacy/draft-scc-clash-irish-law-reaches-european-commission.

COFONE Ignacio: Google v. Spain: a right to be forgotten? Chicago-Kent Journal of International and Comparative Law 2015, vol. 15, no. 1, 2015, pp. 1-11.

COHEN Julie: How (not) to write a privacy law – disrupting surveillance-based business models requires government innovation. Article published March 23 2021, available at https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

COOK Diane, AUGUSTO Juan, JAKKULA Vikramaditya: Ambient intelligence: Technologies, applications, and opportunities. Article published in Pervasive and Mobile Computing 2009, vol. 5, issue 4, pp. 277-298, available at https://www.sciencedirect.com/science/article/abs/pii/S157411920900025X#:~:text=Ambient%20intelligence%20is%20an%20emerging%20discipline%20that%20brings,and%20sensor%20networks%2C%20pervasive%20computing%2C%20and%20artificial%20intelligence.

COOPER Dan, BERTRAND Alix, VALAT Diane: French CNIL finds GDPR not applicable to a US company providing a browser extension. Article published January 5, 2023, available at https://www.insideprivacy.com/eu-data-protection/french-cnil-finds-gdpr-not-applicable-to-a-us-company-providing-a-browser-extension/.

COOPER Dan, PEETS Lisa, SHEPHERD Nicholas, OBERSCHELP de MENESES Anna: European Commission publishes directive on the liability of Artificial Intelligence systems. Article published October 12 2022, available at https://www.insideprivacy.com/artificial-intelligence/european-commission-publishes-directive-on-the-liability-of-artificial-intelligence-systems/.

COOPER Dan, SOMAINI Laura, JUNGYUN CHOI Sam: European Parliament adopts DSA. Article published July 6 2022, available at https://www.insideprivacy.com/european-union-2/european-parliament-adopts-dsa/.

COST Edward: What is the Digital Operational Resilience Act. Article published June 7 2022, available at https://www.upguard.com/blog/what-is-the-digital-operational-resilience-act.

COX Joseph: Data broker is selling location data of people who visit abortion clinics. Article published May 3 2022, available https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

CRITCHEY Liam: Storing information and data with DNA. Article published August 11 2020, available at https://www.electropages.com/blog/2020/08/storing-information-and-data-dna.

CWALINA Chris, SERRATO Jeewon Kim, ROSS Susan, COUGHLIN Tristan:The European Parliament asks for the suspension of the privacy shield. Article published July 17 2018, available at https://www.dataprotectionreport.com/2018/07/european-parliament-asks-for-suspension-privacy-shield/.

CYPHERS Bennett: Google’s FLoC is a terrible idea. Article published March 3 2021, available at https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea.

DACHWITZ Ingo, FANTA Alexander: EU-Staaten wollen Verlagen einen Blankoscheck für Online-Tracking gewähren. The article provides background information on the draft ePrivacy regulation. Article published November 18 2019, available at https://netzpolitik.org/2019/eu-staaten-wollen-verlagen-einen-blankoscheck-fuer-online-tracking-gewaehren/.

DASTIN Jeffrey: Amazon scraps secret AI recruiting tool that showed bias against women. Article published October 11 2018, available at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

DATAMEER: Top five high-impact use cases for Big Data analytics. E-book published 2016, available at http://orcp.hustoj.com/wp-content/uploads/2016/01/eBook-Top-Five-High-Impact-UseCases-for-Big-Data-Analytics.pdf.

DAVIS Ben: 13 examples of dark patterns in ecommerce checkouts. Article published on April 6 2017, available at https://econsultancy.com/13-examples-of-dark-patterns-in-ecommerce-checkouts/.

DAWES James: An autonomous robot may have already killed people – here's how the weapons could be more destabilizing than nukes. Article published September 29 2021, available at https://theconversation.com/an-autonomous-robot-may-have-already-killed-people-heres-how-the-weapons-could-be-more-destabilizing-than-nukes-168049.

DAY Anthony, DONOVAN Nichola, OSSACK David: Operational Resilience: Update EU – publication of DORA. Article published January 16 2023, available at https://www.technologyslegaledge.com/2023/01/operational-resilience-update/?utm_source=DLA+Piper+-+Technology%27s+Legal+Edge&utm_campaign=29e7915ae6-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_451d831b6d-29e7915ae6-92373648.

DECLERCK, Thomas: New EU Cybersecurity Strategy: European Commission accelerates push for EU to lead in cybersecurity regulation. Article published December 24 2020, available at https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/.

DEMISHEV Konstantin: Internet of Things technology for connected cars: the future of automobiles is here. Article published August 6 2020, available at https://www.topdevelopers.co/blog/iot-technology-for-connected-cars-the-future-of-automobiles/.

DESAI Deven, MAKRIDIS Christos: We should have known SolarWinds would be a target. Article published January 6 2021, available at https://www.cfr.org/blog/we-should-have-known-solarwinds-would-be-target.

DETERMANN Lothar: California data broker registrations: Who made the list on Jan. 31? Article published February 11 2020, available at https://iapp.org/news/a/california-data-broker-registrations-who-made-the-list-on-jan-31/.

DHONT Jan, CUYVERS Lauren: National variations further fragment GDPR. Article published June 26 2018, available at https://www.alstonprivacy.com/gdpr-fragmentation-may-appear-more-significant-than-intended/.

DICKSON Ben: Why the difference between AI and Machine Learning matters. Article published October 8 2018, available at https://bdtechtalks.com/2018/10/08/artificial-intelligence-vs-machine-learning/.

DLA Piper: Netherlands – highest court side-steps determining whether legitimate interests may be purely commercial. Article published 28 July 2022, available at https://blogs.dlapiper.com/privacymatters/netherlands-highest-court-side-steps-determining-whether-legitimate-interests-may-be-purely-commercial/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter.

DOCTER-LOEB Hannah: Scientists now want to create AI using real human brain cells. Article published February 28 2023, available at https://www.vice.com/en/article/qjkgap/scientists-now-want-to-create-ai-using-real-human-brain-cells.

DONATH Andreas: ChatGPT in der Robotik soll Sprachsteuerung ermöglichen. Article published February 22 2023, available at https://www.golem.de/news/kuenstliche-intelligenz-chatgpt-in-der-robotik-soll-sprachsteuerung-ermoeglichen-2302-172080.html?utm_source=nl.2023-02-22.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter.

DOPPLICK Renee: New Statement on Algorithmic Transparency and Accountability by ACM U.S. Public Policy Council. Article published January 14 2017, available at https://techpolicy.acm.org/2017/01/new-statement-on-algorithmic-transparency-and-accountability-by-acm-u-s-public-policy-council/.

DRAKE Emma, BOARDMAN Ruth: UK data protection reform: What is in the government's proposals? Article published June 23 2022, available at https://iapp.org/news/a/uk-data-protection-reform-what-is-in-the-governments-proposals/.

DRESP-LANGLEY Birgitta, HUTT Axel: Digital addiction and sleep. Article published June 5 2022, available at https://pubmed.ncbi.nlm.nih.gov/35682491/#:~:text=In%202020%2C%20the%20World%20Health%20Organization%20formally%20recognized,produce%20disturbed%20sleep%20patterns%20or%20insomnia%20during%20nighttime.

DREYER Stephan, SCHULZ Wolfgang: Was bringt die Datenschutzgrundverordnung für automatisierte Entscheidungssysteme? Bertelsmann Stiftung Publishing 2018.

DUTCH Mike: A data protection taxonomy. Paper published June 2010, available at https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf.

ECHEVARIA DELGADO Marta et al: European Union – Regulating Artificial Intelligence: European Commission launches proposals. Article published April 30 2021, available at https://www.jonesday.com/en/insights/2021/04/regulating-artificial-intelligence-european-commission-launches-proposals?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

EGETOFT Karsten: Data-driven analytics: practical use cases for financial services. Article published January 29 2019, available at https://www.digitalistmag.com/customer-experience/2019/01/29/data-driven-analytics-practical-use-cases-for-financial-services-06195123/.

ESCHHOLZ Stefanie, DJABBARPOUR Jonathan: Big Data und Scoring in der Finanzbranche. Dossier published January 2015, available at http://www.abida.de/sites/default/files/06%20Scoring.pdf.

European Center for Non-For-Profit-Law: Recommendations for assessing AI impacts to human rights, democracy, and the rule of law. Paper published November 2021, available at https://ecnl.org/publications/recommendations-incorporating-human-rights-ai-impact-assessments.

EVANS Marcus, MERCHANT Anj: UK AI – UK consults on non-statutory cross-sectoral guidance principles for regulating AI – final approach still some way off. Article published July 27 2022, available at https://www.insidetechlaw.com/blog/uk-consults-on-non-statutory-cross-sectoral-guidance-principles-for-regulating-ai.

EVANS Marcus, BUNDY-CLARKE Fiona, DADDAR Shiv: UK GDPR Reform: government publishes response to consultation – likely to form basis of forthcoming UK Data Reform Bill. Article published June 22 2022, available at https://www.dataprotectionreport.com/2022/06/uk-gdpr-reform-government-publishes-response-to-consultation-likely-to-form-basis-of-forthcoming-uk-data-reform-bill/.

EVANS Marcus, McBURNEY Peter, SINCLAIR Michael: The UK national AI strategy: regulation, data protection and IPR in the mix. Article published September 27 2021, available at https://www.insidetechlaw.com/blog/the-uk-national-ai-strategy-regulation-data-protection-and-ipr-in-the-mix.

FAGELLA Daniel: Will there be another Artificial Intelligence winter? Article published January 2 2019, available at https://emerj.com/ai-executive-guides/will-there-be-another-artificial-intelligence-winter-probably-not/.

FAIR Lesley: Health app broke its privacy promises by disclosing intimate details about users. Article published for FTC's Business Blog, posted on January 13 2021, available at https://www.ftc.gov/business-guidance/blog/2021/01/health-app-broke-its-privacy-promises-disclosing-intimate-details-about-users.

FANTA Alexander: France, Spain push for new EU data retention law. Article published March 5, 2021, available at https://netzpolitik.org/2021/urgently-needed-france-spain-push-for-new-eu-data-retention-law/.

FARGO Nikolaus, HÄNOLD Stefanie, SCHÜTZE Benjamin: The principle of purpose limitation in Big Data in: Marcelo Corales, Mark Fernwick, Nikolaus Fargo (eds.): New Technology, Big Data and the Law. Springer Publishing 2017.

FAY Joe: Vatican signs up IBM and Microsoft as AI ethics apostles. Article published March 2 2020, available at https://devclass.com/2020/03/02/vatican-signs-up-ibm-and-microsoft-as-ai-ethics-apostles/.

FAZLIOGLU Müge: U.S. federal privacy legislation tracker. Article published April 2022, available at https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/.

FAZLIOGLU Müzge; Transparency and the GDPR: Practical guidance and interpretive assistance from the Article 29 Working Party. Article published December 14 2017, available at https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/.

FEDERAL TRADE COMMISSION: Big Data: a tool for inclusion or exclusion? Report published January 2016, available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report.

FEILER Lukas, SEINEN Wouter: BCRs as a robust alternative to Privacy Shield and SCCs. Article published July 23 2020, available at https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/.

FEILER Lukas: Die 69 Öffnungsklauseln der DSGVO - Regelungsspielräume der nationalen Gesetzgeber. Presentation held on June 1 2017, available at http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf.

FEKETE Michael: ISO/IEC 27018 – new code of practice promotes privacy protection in the cloud, 2014. Article published October 20 2014, available at https://www.lexology.com/library/detail.aspx?g=ff6d5e13-1f3e-4539-887e-20dfc12eb8fd.

FENNESSY Caitlin: Top five operational impacts of Brazil’s LGPD. Part 3: international transfers. Article published November 5 2020, available at https://iapp.org/news/a/top-5-operational-impacts-of-brazils-lgpd-part-3-international-transfers/.

FERENSTEIN Greg: The birth and death of privacy: 3000 years of history told in 46 images. Article published November 25 2015, available at https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e#.8tcuzmf86.

FERRARIS Valeria, BOSCO, Francesca Bosco, D’ANGELO, Elena: The impact on profiling on fundamental rights. Article published December 22 2013, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753.

FIELD Jessica et al: Principled Artificial Intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center Research Publication no. 2020-1. Article published February 14 2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482.

FOLGER Jean: What is the Metaverse? Article published July 6 2022, available at https://www.investopedia.com/metaverse-definition-5206578.

FOOTE Keith: A brief history of Big Data. Article published December 14 2017, available at https://www.dataversity.net/brief-history-big-data/.

FOURNERETIS Eric: The dangers of Musk's Neuralink. Article published April 1 2022, available at https://iai.tv/articles/the-dangers-of-musks-neuralink-auid-2092.

FRANKLIN Matija, ASHTON Hal, GORMAN Rebecca, ARMSTRONG Stuart: The EU's AI Act needs to address critical manipulation methods. Article published March 21 2023, available at https://oecd.ai/en/wonk/ai-act-manipulation-methods.

FRANSSEN Vanessa: The European Commission's E-evidence proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement? Article published October 2018, available at http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

FRANTZMAN Seth: Israel and UAE defense companies partner on Artificial Intelligence. Article published April 21 2021, available at https://nationalinterest.org/blog/buzz/israel-and-uae-defense-companies-partner-artificial-intelligence-183274.

FRASER Erica: Data localisation and the Balkanisation of the Internet. Journal of Law, Technology & Society 2016, vol. 13, issue 3.

FRENZEL Eike in Paal/Pauly: Kommentar zur Datenschutzgrundverordnung, Bundesdatenschutzgesetz. C.H. Beck Publishing 2018.

GABEL Detlev, HICKMAN Tim: Chapter 8: Consent – unlocking the EU General Data Protection Regulation. Article published April 5 2019, available at https://www.whitecase.com/publications/article/chapter-7-legal-basis-processing-unlocking-eu-general-data-protection.

GALLAGHER James, GRAN Amy: The proposal for a revised EU Product Liability Directive. Article published October 12 2022, available at https://www.mhc.ie/latest/insights/the-proposal-for-a-revised-eu-product-liability-directive#:~:text=The%20Proposal%20has%20several%20stated%20aims%3A%201%20To,on%20making%20claims%20where%20appropriate%2C%20and%20Weitere%20Elemente.

GALLAGHER Catherine: 25 stunning advances in Artificial Intelligence. Article published June 23 2019, available at https://stacker.com/stories/3336/25-stunning-advances-artificial-intelligence.

GARRETT Paul et al: Privacy and health: the lesson of COVID-19. Article published February 4 2021, available at https://pursuit.unimelb.edu.au/articles/privacy-and-health-the-lessons-of-covid-19.

GARRETT John: EU data protection code to replace US/EU data rules. Article published September 16 2020, available at https://www.iteuropa.com/news/eu-data-protection-code-replace-useu-data-rules#:~:text=The%20EU%20Cloud%20Code%20of%20Conduct%20General%20Assembly,personal%20data%20to%20third%20countries%20around%20the%20world.

GAUDINO Francesca: International data transfer solutions under GDPR. Article published April 19 2020, available at https://globalcompliancenews.com/international-data-transfer-solutions-under-gdpr-23032020/.

GELLERT Raphael: Understanding data protection as risk regulation, Journal of Internet Law 2015, pp. 3-15.

GERTZ Bill: Social credit score: China set to roll out “Orwellian” mass surveillance tool. Article published December 9 2019, available at https://www.washingtontimes.com/news/2019/dec/9/social-credit-system-china-mass-surveillance-tool/.

GESSER Avi, MADDOX Robert, GRESSEL Anna, COLLELURI Frank Colleluori, PIZZI Michael: Debevoise & Plimpton discusses the EU AI Liability Directive’s impact on Artificial Intelligence legal risks. Article published November 21 2022, available at https://clsbluesky.law.columbia.edu/2022/11/21/debevoise-plimpton-discusses-eu-ai-liability-directives-impact-on-artificial-intelligence-legal-risks/.

GEWIRTZ David: Volume, velocity, and variety - understanding the three V's of Big Data. Article published March 21 2018, available at https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/.

GILLIARD Chris: The rise of luxury surveillance. Article published October 18 2022, available at https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/.

GRESLEY Jenny: European Commission proposes new cybersecurity rules for products with digital elements. Article published December 2 2022, available https://www.loc.gov/item/global-legal-monitor/2022-12-01/european-union-commission-proposes-new-cybersecurity-rules-for-products-with-digital-elements/.

GIERSCHMANN Sibylle: Was bringt deutschen Unternehmen die DSGVO – mehr Pflichten, aber die Rechtsunsicherheit bleibt. Zeitschrift für Datenschutz 2016, pp. 51-54.

GILES Ralph: The AI Liability Directive. Key points to be aware of for businesses that use AI. Article published November 17 2022, available at https://www.bristows.com/news/the-ai-liability-directive/.

GLOBAL PARTNERS DIGITAL: National Artificial Intelligence strategies and human rights: a review. Paper published April 15 2020, available at https://www.gp-digital.org/publication/national-artificial-intelligence-strategies-and-human-rights-a-review/.

GLOBAL LEGAL GROUP: The international comparative legal guide to data protection, 5th edition 2018, available at https://iapp.org/media/pdf/resource_center/Legal_Guide_To_Data_Protection_2018.pdf.

GOEBEL Nicole: All EU ID cards to include fingerprints. Article published April 16 2018, available at https://www.dw.com/en/all-eu-id-cards-to-include-fingerprints-eu-commissioner/a-43401789.

GOLA Peter: Bundesdatenschutzgesetz. C.H. Beck Publishing 2012.

GONZALEZ FUSTER Gloria, GUTWIRTH Serge, ELLYNE Eriak: Profiling in the European Union – a high-risk practice, Inex Policy Brief no. 10, published June 2010, available at https://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf.

GOODFELLOW Ian et al.: Generative Adversarial Networks. Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), pp. 2672-2680, available at https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf.

GORLICK Adam: Researchers say voters swayed by candidates who share their looks, Stanford University report published October 22 2008, available at https://news.stanford.edu/news/2008/october22/morph-102208.html.

GOUBET Jean-Etienne: AI Ethics – beware of AI ethics washing. Article published September 24 2019, available at https://www.genesys.com/blog/post/ai-ethics-beware-of-ai-ethics-washing.

GOW Glenn: The AI Bill Of Rights: protecting Americans from the dangers of Artificial Intelligence. Article published January 9 2022, available at https://www.forbes.com/sites/glenngow/2022/01/09/the-ai-bill-of-rights-protecting-americans-from-the-dangers-of-artificial-intelligence/.

GUPTA Rachana: China making big strides in Artificial Intelligence. Article published September 6 2019, available at http://www.china.org.cn/opinion/2019-09/06/content_75178964.htm.

GUTWIRTH Serge, LEENES, Ronald, De HERT, Paul: Data Protection on the move – current developments in ICT and privacy / data protection. Springer Science + Media Publishing 2016.

HALPERT Jim, BELLAMY Lael: What Virginia's Consumer Data Protection Act means for your privacy program. Article published March 8 2021, available at https://iapp.org/news/a/what-the-virginia-consumer-data-protection-act-means-for-your-privacy-program/#:~:text=Virginia%27s%20CDPA%20is%20a%20somewhat%20simplified%20version%20of,by%20overwhelming%20margin%20in%20fewer%20than%20two%20months.

HAMILTON Isobel: The FTC can move forward with its bid to make Meta sell Instagram and WhatsApp, judge rules. Article published January 12 2022, available at https://www.businessinsider.com/ruling-ftc-meta-facebook-lawsuit-instagram-whatsapp-can-proceed-2022-1#:~:text=Judge%20James%20Boasberg%20ruled%20on%20Tuesday%20that%20the,lawsuit%2C%20which%20was%20rejected%20by%20Boasberg%20in%20June.

HAMILTON Ernest: The future Of Neuralink: does it affect our private lives? Article published December 8 2020, available at https://www.sciencetimes.com/articles/28562/20201208/the-future-of-neuralink-does-it-affect-our-private-lives.htm.

HAN Meghan: China aims to get the jump on AI standardization. Article published January 25 2018, available at https://syncedreview.com/2018/01/25/china-aims-to-get-the-jump-on-ai-standardization/.

HAO Karen: A horrifying new AI app swaps women into porn videos with a click. Article published September 13 2021, available at https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/.

HAWKINS Andrew: Two new fatal Tesla crashes are being examined by US investigators. Article published July 7 2022, available at https://www.theverge.com/2022/7/7/23198997/tesla-fatal-crashes-california-florida-autopilot-nhtsa.

HÄRTING Niko: Kopplungsverbot nach der DSGVO – erste Sichtung der Literatur. itrb-Rechtsberater 2019, Sonderheft zur DSGVO.

HÄRTING Niko: Mit der DSGVO zum "Golden Handshake" – von der Sprengkraft des "Rechts auf Kopie". Article published March 29 2019, available at https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/.

HÄRTING Niko: Wann ist eine Datenverarbeitung eigentlich „erforderlich"? Article published February 1 2019, available at https://www.cr-online.de/blog/2019/02/01/wann-ist-eine-datenverarbeitung-eigentlich-erforderlich/.

HÄRTING Niko: Post von der Datenschutzbehörde – Risiken des Wohlverhaltens: Was ist zu beachten, wenn eine Datenschutzbehörde Auskünfte verlangt? Article published November 8 2018, available at https://www.cr-online.de/blog/2018/11/08/post-von-der-datenschutzbehoerde-risiken-des-wohlverhaltens/.

HÄRTING Niko: DSGVO – gibt es Regelungen für anonyme Daten? Article published May 3 2016, available at https://www.cr-online.de/blog/2016/05/03/dsgvo-gibt-es-regelungen-fuer-anonyme-daten/.

HÄRTING Niko: Datenschutzgrundverordnung. Dr. Otto Schmidt Publishing 2016.

HÄRTING Niko: Internetrecht. Dr. Otto Schmidt Publishing 2014.

HEADDON Toby, CROWTHER Hannah: Two worlds collide: the Data Act proposal v. GDPR. Article published June 14 2022, available at https://www.bristows.com/news/two-worlds-collide-the-data-act-proposal-v-gdpr/.

HEIDRICH Jörg: Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig. Article published October 23 2020, available at https://www.heise.de/news/Datenschutzbehoerden-erklaeren-den-Einsatz-von-Microsoft-365-fuer-rechtswidrig-4931745.html.

HEIKKILA Melissa: AI: Decoded: U.S. states move to ban facial recognition - AI and structural racism. Article published May 12 2021, available at https://www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-ai-gov-us-states-move-to-ban-facial-recognition-ai-and-structural-racism/.

HEIKKILÄ Melissa: The rise of AI surveillance. Article published May 26 2021, available at https://www.politico.eu/article/the-rise-of-ai-surveillance-coronavirus-data-collection-tracking-facial-recognition-monitoring/.

HELBING Thomas: Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung. Kunst und Recht 2015, vol. 3, pp. 145-150.

HELLER Brittan: Watching androids dream of electric sheep: Immersive technology, biometric psychography, and the law. Vanderbilt Journal of Entertainment and Technology Law 2021, vol. 23, issue 1, pp. 1-51, available at https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1.

HELLER Brittan: Reimagining Reality: Human rights and immersive technology. Article published June 12 2020, available at https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology.

HENGESBAUGH Brian et al.: US state laws. Article published May 2 2022, available at https://www.connectontech.com/tag/us-state-laws/.

HENLEY John, BOOTH, Robert: Welfare surveillance system violates human rights, Dutch court rules. Article published February 5 2020, available at https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules.

De HERT Paul, PAPAKONSTANINOU Vagelis: The new police and criminal justice data protection directive: A first analysis. New Journal of European Criminal Law 2016, vol. 7, issue 1, pp. 7-19.

De HERT Paul, GUTWIRTH Serge: Regulating profiling in a democratic constitutional state, in: Profiling the European citizen, Springer Publishing 2008.

HEYMANN Daniel: DSGVO und UWG – Wettbewerbsrecht und Datenschutz. Article published July 26 2019, available at https://www.petersenhardrahtpruggmayer.de/de/news/dsgvo-und-uwg-wettbewerbsrecht-und-datenschutz/.

HEYWOOD Debbie: The EC draft Data Governance Act – an altruistic approach to data. Article published January 29 2021, available at https://www.taylorwessing.com/en/insights-and-events/insights/2021/01/the-ec-draft-data-governance-act---an-altruistic-approach-to-data#:~:text=The%20DGA%20applies%20to%20a%20very%20broad%20range,the%20form%20of%20sound%2C%20visual%20or%20audiovisual%20recording%22.

HIDAKA Seiko: EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? Article published July 5 2021, available at https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/.

HILDEBRANDT Mireille: Slaves to Big Data. Or are we? Keynote during the 9th Annual Conference on Internet, Law & Politics on June 25, 2013 in Barcelona, available at http://works.bepress.com/mireille_hildebrandt/52.

HLADJK Jörg, von DIEMAR Undine, HAAS Olivier, LITTLE Jonathon Little: European Union: New regulation favors free flow of non-personal data in the EU. Article published17 December 2018, available at http://www.mondaq.com/x/762982/data+protection/New+Regulation+Favors+Free+Flow+Of+NonPersonal+Data+In+The+EU.

HOEREN Thomas, MÜNKE, Reiner: Die EU-Richtlinie für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung unter besonderer Berücksichtigung der Produzentenhaftung. Wettbewerb in Recht und Praxis 2018, vol. 2, pp. 150-155, available at https://www.itm.nrw/wp-content/uploads/Die-EU-Richtlinie.pdf.

HOEREN Thomas: Big Data und Recht, C.H. Beck Publishing 2014.

HORNUNG Gerrit: A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25 January 2012. Article published March 6 2018, available at https://script-ed.org/article/general-data-protection-regulation-europe-light-shade-commissions-draft-25-january-2012/.

House of Lords Select Committee on Artificial Intelligence: HL Paper 100 - AI in the UK: ready, willing, and able? Report of Session 2017–19, published April 2018, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

HUDDLESTON Tom Jr.: This 29-year-old book predicted the 'Metaverse' – and some of Facebook's plans are eerily similar. Article published November 3 2021, available at https://www.cnbc.com/2021/11/03/how-the-1992-sci-fi-novel-snow-crash-predicted-facebooks-metaverse.html.

HUMAN RIGHTS WATCH and HARVARD LAW SCHOOL INTERNATIONAL HUMAN RIGHTS CLINIC: Agenda for action – alternative processes for negotiating a killer robots treaty. Report published November 10 2022, available at https://www.hrw.org/report/2022/11/10/agenda-action/alternative-processes-negotiating-killer-robots-treaty.

HUMPHREYS Jamie, TURTLE Edward: European Parliament publishes its proposals for new AI laws. Article published October 28 2020, available at https://products.cooley.com/2020/10/28/regulating-ai-eu-proposes-legal-framework-for-artificial-intelligence/.

IAPP and FTI Consulting joint report on Privacy and AI Governance. Report published January 2023, available at https://iapp.org/resources/article/ai-governance-report-summary/?mkt_tok=MTM4LUVaTS0wNDIAAAGJg-8GK3cP-hfHi0yz1s63YttbFgDBnovCnlsyOUnEB_zUcoykvCDEfx57nVN5ye6zeM2saf2pII4Kot0-eahTGgIkN5FfAJS1RdCct8yoY4zQ.

IKEDA Scott: OECD nations sign privacy agreement aimed at improving transparency into government access of personal data. Article published December 26 2022, available at https://www.cpomagazine.com/data-privacy/oecd-nations-sign-privacy-agreement-aimed-at-improving-transparency-into-government-access-of-personal-data/?utm_source=ActiveCampaign&utm_medium=email&utm_content=OECD+Nations+Sign+Privacy+Agreement+Aimed+At+Improving+Transparency+Into+Government+Access+of+Personal+Data&utm_campaign=Weekly+Highlights+-+2021.

IKEDA Scott: Big Tech companies may face blizzard of new probes in EU as CJEU ruling clears path for data protection authorities. Article published June 28 2021, available at https://www.cpomagazine.com/data-protection/big-tech-companies-may-face-blizzard-of-new-probes-in-eu-as-cjeu-ruling-clears-path-for-data-protection-authorities/#:~:text=The%20new%20CJEU%20ruling%20gives%20the%20data%20protection,protection%20authorities%20will%20need%20to%20meet%20certain%20conditions.

ILKOUNA Eleni, KOUTRAKIA Maria: Symbolic vs. sub-symbolic AI methods: friends or enemies? Proceedings of the CIKM 2020 Workshops, October 19-20, Galway, Ireland, available at http://ceur-ws.org/Vol-2699/paper06.pdf.

INTERNATIONAL NETWORK OF PRIVACY PROFESSIONALS: A brief history of data protection: how did it all start? Aarticle published June 1 2018, available at https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/.

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS: Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics. Paper published May 2014, available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf.

IZDEBSKI, Krzysztof: Comment on AI regulation proposal. EU database on high-risk AI systems. Article publishedApril 28 2021, available at https://epf.org.pl/en/2021/04/28/comment-on-ai-regulation-proposal-eu-database-on-high-risk-ai-systems/.

JALAN Trisha: European Commission proposes Data Act 2021 to increase data sharing between businesses and governments. Article published February 21 2020, available at https://www.medianama.com/2020/02/223-european-commission-data-sharing/.

JAMES Rebecca: When using the Tor browser becomes illegal? Article published March 24 2023, available at https://beencrypted.com/privacy/anonymous-browsing/is-tor-illegal/.

JANSSEN Jan-Keno, TREMMEL Sylvester: Die Psycho-Tricks der App-Entwickler. Article published October 15 2019, available at https://www.heise.de/ct/artikel/Die-Psycho-Tricks-der-App-Entwickler-4547123.html?seite=all.

JANSSEN Wiel: Seat-belt wearing and driving behavior – an instrumented-vehicle study. Accident Analysis and Prevention 1994, vol. 26, no. 2, pp. 261-268. A summary of the study is available at https://www.ncbi.nlm.nih.gov/pubmed/8198694?dopt=Abstract.

JEFFERY Christopher: Dutch data protection guidance on the use of cookie walls. Article published May 1 2019, available at https://www.taylorwessing.com/en/global-data-hub/2019/may---adtech/dutch-data-protection-authority-guidance-on-the-use-of-cookie-walls.

JHA Manu Siddhartha: Want to win an election? Use AI and Machine Learning. Article published April 23 2020, available at https://www.mygreatlearning.com/blog/how-ai-and-machine-learning-can-winelections/#:~:text=Artificial%20Intelligence%20for%20the%20Benefit%20of%20the%20Voter,help%20them%20make%20up%20their%20minds%20about%20candidates.

JOHNSON Khari: Iran says face recognition will ID women breaking hijab laws. Article published January 10 2023, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment.

JOHNSON Jennifer, XENAKIS Nicholas, PONDER Jayne, HEVIA Anna, HOLBROOK Tyler Holbrook, DWORKIN Dworkin, OSSOFF Ossoff: U.S. AI, IoT, CAV, and data privacy legislative and regulatory update. Article published July 13 2022, available at https://www.insideprivacy.com/artificial-intelligence/u-s-ai-iot-cav-and-data-privacy-legislative-and-regulatory-update-second-quarter-2022/.

JONAS Jeff: Master data management vs. sensemaking. Article published November 11 2011, available at http://jeffjonas.typepad.com/jeff_jonas/2011/11/master-data-management-mdm-vs-sensemaking.html.

KAGAN Odia: Latin American and Spanish DPAs Issue Joint Statement on Data Processing and Artificial Intelligence. Article published October 24 2019, available at https://dataprivacy.foxrothschild.com/2019/10/articles/general-privacy-data-security-news-developments/latin-american-and-spanish-dpas-issue-joint-statement-on-data-processing-and-ai/

KAGAN Odia: FTC filling role of de facto U.S. privacy regulator. Article published March 7 2019, available at https://dataprivacy.foxrothschild.com/2019/03/articles/general-privacy-data-security-news-developments/ftc-filling-role-of-de-facto-u-s-privacy-regulator/.

KALMAN Lawrence: The GDPR and NIS Directive – a new age of accountability, security and trust?, presentation held during the 2017 OWASP summit, available at https://www.owasp.org/images/b/b9/Olswang_slides_-_GDPR_and_NIS_Directive_-_accountability_security_and_trust_-_25_Jan_2017.pdf.

KAUFMANN Julia, SCHMIDL Michael, LUTZ Holger (editors) for Baker McKenzie: GDPR national legislation survey. Report published January 2018, available at https://www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en.

KE Xu, LIU Vicky, LUO Yan, YU Zhijing: Analyzing China's PIPL and how it compares to the EU's GDPR. Article published August 24 2021, available at https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/.

KEIZER Gregg: WWII's Colossus computer cracks codes once again. Article published November 15 2007, available at https://www.computerworld.com/article/2540136/wwii-s-colossus-computer-cracks-codes-once-again.html.

KELLY Éanna: Israel sets out to become the next major artificial intelligence player. Article published July 2 2019, available at https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligence-player.

KEPES Ben: Google Users - You're the product, not the customer. Article published December 4 2013, available at https://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/#:~:text=The%20old%20adage%20goes%20that%20if%20you%27re%20not,up%20advertising%20to%20users%20of%20these%20free%20products.

KHAN Shmyla: Surveillance as a feminist issue. Article published November 21 2017, available at https://www.privacyinternational.org/news-analysis/3376/surveillance-feminist-issue.

KHARPAL Arjun: China is about to get tougher on deepfakes in an unprecedented way. Here’s what the rules mean. Article published December 22 2022, available at https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html#:~:text=In%20January%2C%20China%20will%20introduce,the%20dissemination%20of%20fake%20news.

KHARPAL Arjun: China is building a giant $2.1 billion research park dedicated to developing A.I. Article published January 3 2018, available at https://www.cnbc.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html.

KIM Laura, GRAUBERT John: Dark Patterns: what they are and what you should know about them. Article published July 9, 2019, available at https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/.

KLEIN Daniel: Mighty mouse. Article published December 19 2018, available at https://web.archive.org/web/20220125004420/https://www.technologyreview.com/2018/12/19/138508/mighty-mouse/.

KLEINMAN Zoe, VALLANCE Chris: AI 'godfather' Geoffrey Hinton warns of dangers as he quits Google. Article published May 3 2023, available at https://www.bbc.com/news/world-us-canada-65452940.

KLEKOVIC Ivan: EU GDPR vs. European data protection directive. Article published October 30 2017, available at https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/.

KLÜMPER Donald, ROSEN Peter, MOSSHOLDER Kevin: Social networking websites, personality ratings and the organizational context – more than meets the eye? Journal of Applied Social Psychology 2012, vol. 42, issue 5, pp.1143-1172.

KNIGHT Will: Clearview AI has new tools to identify you in photos. Article published April 10 2021, available at https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.

KNIGHT Daniel: Personal computer history from 1975 to 1984. Article published June 26 2014, available at https://lowendmac.com/2014/personal-computer-history-the-first-25-years/.

KOBIE Nicole: The complicated truth about China's social credit system. Article published June 7, 2019, available at https://www.wired.co.uk/article/china-social-credit-system-explained.

KOBIELUS James: The enterprise data warehouse – defined, refined, evolving with the times. Article published April 8 2008, available at https://go.forrester.com/blogs/08-04-08-the_enterprise_data_warehouse_edw_defined_refined_evolving_with_the_times/.

KÖHLER Helmut: Die Umsetzung der Richtlinie über unlautere Geschäftspraktiken in Deutschland – eine kritische Analyse. Gewerblicher Rechtsschutz und Urheberrecht 2012, pp. 1073-1079.

KOKOTT Juliane, SOBOTTA Christoph: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law 2013, vol. 3, issue 4, pp. 222-228, available at https://academic.oup.com/idpl/article/3/4/222/727206.

KONING Merel: EU companies selling surveillance tools to China’s human rights abusers. Article published September 21 2020, available at https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/.

KORNMEIER Udo, BARANOWSKI Anne: Eigentum an Daten – Zugang statt Zuordnung. Der Betriebsberater 2019, pp. 1219-1225.

KRANIG Thomas, SACHS Andreas, GIERSCHMANN Markus: Datenschutz-Compliance nach der DSGVO – Handlungshilfe für Verantwortliche inclusive Prüffragen für Aufsichtsbehörden. Bundesanzeiger Publishing 2017.

KRASADAKISD George: Artificial Intelligence: The impact on employment and the workforce. How is AI replacing jobs? Which roles and industries will be most impacted? How can societies get prepared? Article published January 2018, available at https://medium.com/innovation-machine/artificial-intelligence-3c6d80072416.

KRAUL Torsten, von SCHÖFELD Max, BARTELS Marvin: Europäische Datenstrategie: EU-Kommission veröffentlicht Folgenabschätzung zum Data Act. Article published June 24 2021, available at https://www.noerr.com/en/insights/european-data-strategy-eu-commission-publishes-impact-assessment-on-the-data-act.

KREMPL Stefan: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck. Article published December 28, 2014, available at https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html.

KRITIKOS Mihalis: Artificial Intelligence ante portas: legal and ethical reflections, EPRS briefing. Paper published March 2019, available at https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf.

KUNAR Varun: 22 Most Interesting Facts About Quantum Computers. Article published January 2 2023, available at https://www.rankred.com/interesting-facts-about-quantum-computers/.

KUNE, Christopher, CATE Fred, MILLARD Christopher, SVANTESSON Dan: The challenge of Big Data for data protection. International Data Privacy Law 2012, vol. 2, no. 2, pp. 48-52.

KUNER Christopher: The European Union and the search for an international data protection framework. Groningen Journal of International Law 2014, vol. 2, pp. 55-71.

KUSNER Matt, LOFTUS Joshua, RUSSELL Chris, SILVA Ricardo: Counterfactual fairness, presented and published at the 31st Conference on Neural Information Processing Systems, available at https://papers.nips.cc/paper/6995-counterfactual-fairness.pdf.

KÜHLING Jürgen: Die Europäisierung des Datenschutzrechts – Gefährdung deutscher Grundrechtsstandards? C.H. Beck Publishing 2014.

LANEY Doug: 3D Data Management – controlling data volume, velocity, and variety. Article published February 2001, available at http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

LANXON Nate, SHANKLEMAN Jess: The terms and conditions reckoning is coming. The authors report that PayPal’s terms and conditions are almost 50,000 words spread across 21 separate web pages: Article published April 20 2018, available at https://www.bloomberg.com/news/articles/2018-04-20/uber-paypal-face-reckoning-over-opaque-terms-and-conditions.

LARSEN Benjamin: Harmonizing Artificial Intelligence: The role of standards in the EU AI Regulation. Article published January 18, 2022, available at https://montrealethics.ai/harmonizing-artificial-intelligence-the-role-of-standards-in-the-eu-ai-regulation/.

LASINSKA Katarzyna: Encryption policy issues in the EU. Article published May 25 2018, available at https://www.globalpolicywatch.com/2018/05/encryption-policy-issues-in-the-eu/.

LATONERO Mike: Governing Artificial Intelligence: upholding human rights & dignity. Paper for Data & Society issued 2018, available at https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

LEDFORD Heidi: Millions of black people affected by racial bias in health-care algorithms. Article published October 24 2019 (updated October 26 2019), available at https://www.nature.com/articles/d41586-019-03228-6.

LEE Phil: Why Apple's "Consent for IDFA" announcement is a game changer for online and mobile privacy. Article published on June 24, 2020, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/why-apples-consent-idfa-announcement-is-a-game-changer.

LENSDORF Lars, HENRICI Robert, HÜSCH Moritz, SHEPHERD Nicholas: A new day for GDPR damages claims in Germany? Article published February 25 2021, available at https://www.insideprivacy.com/data-privacy/a-new-day-for-gdpr-damages-claims-in-germany/.

LESLIE David, BURR Christopher, AITKEN Mhairi, KATELL Michael, BRIGGS Morgan, RINCON Cami: Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal prepared for the Council of Europe’s Ad hoc Committee on Artificial Intelligence. Paper published June 2022, available at https://doi.org/10.5281/zenodo.5981676.

LI Abner: Google names external advisory council to guide artificial intelligence usage. Article published March 26 2019, available at https://9to5google.com/guides/google-ai-principles/#:~:text=Google%20AI%20Google%20AI%20Principles.%20Back%20in%20June%2C,implemented%20to%20ensure%20that%20all%20guidelines%20are%20enforced.

LIAO Todd, WANG Judy, HU Sylvia: China releases Standard Contractual Clauses for cross-border data transfers. Article published July 11 2022, available at https://www.morganlewis.com/pubs/2022/07/china-releases-standard-contractual-clauses-for-crossborder-data-transfers.

Van LIESHOUT Marc: The value of personal data. In: Jan Camenisch, Simone Fischer-Hubner, Marit Hansen (eds). Privacy and Identity Management for the Future Internet in the Age of Globalisation. Springer Publishing 2015.

LINKEDIN 2018 Report on global trends in recruiting. Report published January 2018, available at https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment.

LINVILL Darren, WARREN Patrick: Troll factories – manufacturing specialized disinformation on Twitter. Article published February 5 2020, available at https://www.tandfonline.com/doi/abs/10.1080/10584609.2020.1718257?journalCode=upcp20.

LOMAS Natasha: European parliament found to have broken EU rules on data transfers and cookie consents. Article published January 11 2022, , available at https://techcrunch.com/2022/01/10/edps-decision-european-parliament-covid-19-test-website/.

LOMAS Natasha: Sweden’s data watchdog slaps police for unlawful use of Clearview AI. Article published February 12 2021, available at https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAA

Lgmrj2j7lIqtPjUw9cgbbjI_LwuKoMDVdLqwxaBB4vNzCgFK7Pbz7Ez_PA0oQOMd7Csz70S7acDJmzPURaBLxCvcCrHG9kAiK1112tsVuo1yTd_vtJ3XMiwQYkT2_yofnTUP6pgIpte0masI6OagPfoQ91ZjZA16T2v7bBqJRwp.

LONG William, BLYTHE Francesca, CUYVERS Lauren, ZDZIEBORSKA Monika: EU Commission issues draft AI regulation. Article published April 23 2021, available at https://datamatters.sidley.com/eu-commission-issues-draft-ai-regulation.

LOPES Stephanie: Key insights from the leaked EU Data Governance Act. Article published November 6 2020, available at https://digitalbusiness.law/2020/11/key-insights-from-the-leaked-eu-data-governance-act/.

LUO Yan, DAN Xuezi, LIU Vicky, SHEPHERD Nicholas: China proposes draft measures to regulate generative AI. Article published April 12 2023, available at https://www.insideprivacy.com/artificial-intelligence/china-proposes-draft-measures-to-regulate-generative-ai/.

LOUVEN Sebastian: Digital Markets Act – Verbot der Datenzusammenführung. Article published July 20 2022, available at https://www.cr-online.de/blog/2022/07/20/digital-markets-act-verbot-der-datenzusammenfuehrung/.

LOUVEN Sebastian, ENGELER, Malte: Copyright Directive – does the best effort principle comply with GDPR? Article published March 23 2019, available at https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html%EF%BB%BF.

LUKIANETS Nikita: A (more) visual guide to the proposed EU Artificial Intelligence Act. Article published May 3 2021, available https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act.

LUSARDI Giacomo, DARLING Coran: The AI liability directive: EU improves liability protections for those impacted by AI. Article published December 6 2022, available at https://www.technologyslegaledge.com/2022/12/the-ai-liability-directive-eu-improves-liability-protections-for-those-impacted-by-ai/.

LYNSKEY Orla: Criminal justice profiling and EU data protection law: precarious protection from predictive policing. International Journal of Law in Context 2019, vol. 15, issue 2, pp. 162-176.

LYONS Kim: Google Pixel 6 leak teases magic eraser feature, plus five years of Android security updates. Article published October 9 2021, available at https://www.theverge.com/2021/10/9/22718007/google-pixel-6-leak-teases-magic-eraser-camera-five-years-android-security-updates.

MacCARTHY Mark, PROPP Kenneth: The EU's White Paper on AI: A thoughtful and balanced way forward. Article published March 5 2020, available at https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward.

MALDOFF Gabe: NIS + GDPR = A New Breach Regime in the EU. Article published December 22 2015, available at https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/.

MANANCOURT Vincent: Have a GDPR complaint? Skip the regulator and take it to court. Article published August 30 2020, available at https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/.

MAO Mark et al: Data privacy – the current legal landscape. Article published February 2016, available at https://iapp.org/media/pdf/resource_center/TS_CurrentLegalLandscape_February_2016.pdf.

MARR Bernard: How much data do we create every day? The Mind-Blowing Stats Everyone Should Read. Article published May 21, 2018, available at https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2152235f60ba.

MARTINI Mario: Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz in: Hill/Martini/Wagner: Die digitale Lebenswelt gestalten. Nomos Publishing Baden Baden 2015, pp. 99-169.

MARTINHO-TRUSWELL Emma, GOMEZ MONT Constanza: Mexico leads Latin America as one of the first ten countries in the world to launch an artificial intelligence strategy. Article published May 24 2018, available at https://www.oxfordinsights.com/insights/2018/5/24/mexico-leads-latin-america-as-one-of-the-first-ten-countries-in-the-world-to-launch-an-artificial-intelligence-strategy.

MARTINSON Molly: Work in progress – substantial revisions recommended to the European Commission's draft new Standard Contractual Clauses. Article published January 28 2021, available at https://practicalprivacy.wyrick.com/blog/work-in-progress-substantial-revisions-recommended-to-the-european-commissions-draft-new-standard-contractual-clauses.

MATHEWS Kristen, BOWMAN Courtney: The California Consumer Privacy Act of 2018. Article published July 13, 2018, available at https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

MAYER-SCHÖNBERGER Viktor, BRANDL, Ernst, KRISTOFERITSCH, Hans: Datenschutzgesetz. Linde Publishing 2014.

MAYER-SCHÖNBERGER Viktor: Generational development of data protection in Europe, in: Philip Agre, Marc Rotenberg (eds.): Technology and privacy – the new landscape. Massachusetts Institute of Technology Press 1998, pp. 219-241.

McCULLAGH Karen: Protecting privacy through control of personal data processing – a flawed approach. International Review of Law, Computers and Technology 2009, vol. 23, no. 1, pp. 23-29.

McNEILL Cassandra: Veracity – the most important "V" of Big Data. Article published August 29 2019, available at https://www.gutcheckit.com/blog/veracity-big-data-v/.

MEDEIROS Maya, BEATSON: Canada's Artificial Intelligence legislation is here. Article published June 28 2022, available at https://www.dataprotectionreport.com/2022/06/canadas-artificial-intelligence-legislation-is-here/.

MEDEIROS Maya: A legal framework for Artificial Intelligence. Article published November 20 2019, available at https://www.socialmedialawbulletin.com/2019/11/a-legal-framework-for-artificial-intelligence/.

MENDOZA Isak, BYGRAVE Lee: The right not to be subject to automated decisions based on profiling, University of Oslo, Legal Studies, Research Paper Series no. 2017-20, available at https://ssrn.com/abstract=2964855.

METZ Rachel: Researchers can now use AI and a photo to make fake videos of anyone. Article published May 24 2019, available at https://edition.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html.

MILLARD Christopher: Forced localization of cloud services: is privacy the real driver? Paper provided for the 2015 forthcoming in IEEE Cloud Computing. Article published May 14, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605926.

MILLER Oliver: A conversation with ELIZA, the electronic therapist. Article published August 1 2012, available at https://thoughtcatalog.com/oliver-miller/2012/08/a-conversation-with-eliza/.

MODRALL Jay: For connected cars, an evolving EU regulatory landscape – the EU's regulatory landscape for connected cars is evolving, with new functionalities appearing almost daily. Article published April 26 2022, available at https://europe.autonews.com/guest-columnist/connected-cars-evolving-eu-regulatory-landscape.

MODRALL Jay: EU proposes new Artificial Intelligence regulation. Article published April 16 2021, available at https://www.nortonrosefulbright.com/en/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation.

MOEREL Lokke, PRINS Corien: On the death of purpose limitation. Article published June 2 2015, available at https://iapp.org/news/a/on-the-death-of-purpose-limitation/.

MOEREL Lokke: Big Data protection – how to make the draft EU regulation on data protection future proof. Tilburg University Press 2014, available at https://pure.uvt.nl/ws/portalfiles/portal/2837675/oratie_Lokke_Moerel.pdf.

MOLTZAU Alex: The French national strategy on Artificial Intelligence. Article published January 15 2020, available at https://towardsdatascience.com/the-french-national-strategy-on-artificial-intelligence-c8c8fcfdace1.

MONTEIRO LEITE Renato: GDPR matchup – Brazil's general data protection law. Article published October 4 2018, available at https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

MONTEIRO LEITE Renato: The new Brazilian General Data Protection Law — a detailed analysis. Article published August 15 2018, available at https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/.

MORGENSTERN Ulf: Fünfte MaRisk-Novelle in Kraft getreten – deutliche Herausforderungen für Kreditinstitute. Article published December 20 2017, available at https://bankinghub.de/banking/steuerung/5-marisk-novelle-kraft-getreten.

MOSCUFO Michela, PARKS Mary Alice, TAUDTE Jeca: Period-tracking apps may help prosecute users, advocates fear. Article published July 2 2022, available at https://abcnews.go.com/Health/abortion-advocates-fear-period-tracking-apps-prosecute-abortion/story?id=85925714.

MULLER Benjamin: The Artificial Intelligence Act – a quick explainer. Article published on May 4 2021, available at https://datainnovation.org/2021/05/the-artificial-intelligence-act-a-quick-explainer/.

MULLER Catelijne: The impact of Artificial Intelligence on human rights, democracy and the rule of law. Report for the Council of Europe Ad Hoc Committee on Artificial Intelligence. Report published June 24 2020, available at https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da.

MÜLLER Claudio: Leben im Metaverse: Was, wenn Zuckerberg gewinnt? Article published November 19 2021, available at https://www.giga.de/news/leben-im-metaverse-was-wenn-zuckerberg-gewinnt/.

NATI Michele, AHLIN Cert: Data Portability 2.0 is yet to come. Article published September 17, 2018, available at https://medium.com/mydata/data-portability-2-0-is-yet-to-come-1c438c2a96c1.

NAUDS Laurens: The right not to be subject to automated decision-making: the role of explicit consent. Article published in 2016 available at https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/.

NELSON Alondra, FIEDLER Sorelle, FIELDS-MEYER Ami: vision for protecting our civil rights in the algorithmic age. Published October 4 2022, available at https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/.

NG Alfred: Facebook's Mark Zuckerberg to appear before Senate and House committees to answer questions about privacy and user data. Article published April 4 2018, available at https://www.cnet.com/news/politics/mark-zuckerberg-will-testify-to-congress-on-april-11/.

NIRWAN Debby: Using forward-search algorithms to solve AI Planning Problems. Article published September 19 2020, available at https://ai.plainenglish.io/using-forward-search-algorithms-to-solve-ai-planning-problems-361ad4910239.

NIX Jacob, BIZARRO Pascal: U.S. data privacy law: a disparate landscape in need of consolidation. Article published September 9 2020, available at https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/us-data-privacy-law-a-disparate-landscape-in-need-of-consolidation.

NONE OF YOUR BUSINESS: Open letter on the future of EU-US data transfers. Blog entry published May 23 2022, available at https://noyb.eu/en/open-letter-future-eu-us-data-transfers.

NONE OF YOUR BUSINESS: NYOB files 422 formal GDPR complaints over nerve-wrecking cookie banners. Blog entry published August 10 2021, available at https://noyb.eu/en/noyb-files-422-formal-gdpr-complaints-nerve-wrecking-cookie-banners.

O'DONOGHUE Cynthia, SPLITTGERBER Andreas, IBRAIMOVA Asel: European Commission issues New Standard Clauses for data transfers outside the EEA: Act within 18 months. Article published June 4 2021, available at https://www.technologylawdispatch.com/2021/06/global-data-transfers/european-commission-issues-new-standard-clauses-for-data-transfers-outside-the-eea-act-within-18-months/.

O'DONOGHUE Cynthia, IBRAIMOVA Asel: ICO announces it is working on bespoke UK set of Standard Contractual Clauses. Article published 5 May 2021, available at https://www.technologylawdispatch.com/2021/05/privacy-data-protection/ico-announces-it-is-working-on-bespoke-uk-set-of-standard-contractual-clauses/.

OEHLENSCHLAGER Mie: First European ethical charter on AI in judicial systems. Article published on January 16, 2019, available at https://dataethics.eu/first-european-ethical-charter-on-ai-in-judicial-systems/.

OLIVEIRA Arlindo: Biotechnology, Big Data and Artificial Intelligence. Biotechnology Journal 2019, vol. 14, issue 8, also also available at https://doi.org/10.1002/biot.201800613.

OLUKOYA Samed: Think20 says Artificial Intelligence (AI) based learning technologies can overcome current educational challenges. Article published August 25 2020, available at https://investorsking.com/2020/08/25/think20-says-artificial-intelligence-ai-based-learning-technologies-can-overcome-current-educational-challenges/.

ORBACH Meir: Israel launches national AI program, but lack of budget threatens its implementation. Article published December 22 2020, available at https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html.

O'REILLY Jim: Data protection in the public cloud. Article published March 15 2018, available at https://www.networkcomputing.com/data-centers/data-protection-public-cloud-6-steps.

OSBORNE Cailean: The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem. Article for the Centre for Data Ethics and Innovation. Article published May 11 2021, available at https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/.

Van OVERSTRATEN Tanguy, De MEYER Julie: Belgium: Council of State approves U.S. data transfer. Article published September 16 2021, available at https://www.linklaters.com/th-th/insights/blogs/digilinks/2021/september/belgium-council-of-state-approves-us-data-transfer.

PAKALSKI Ingo: OpenAI veröffentlicht Tool zur Erkennung von KI-Texten. Article published February 1 2023, available at https://www.golem.de/news/ai-classifier-chatgpt-erfinder-wollen-texte-von-maschinen-erkennen-2302-171582.html?utm_source=nl.2023-02-01.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter,

PANDYA Jayshree: The dual-use dilemma of Artificial Intelligence. Article published January 7 2019, available at https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/.

PANIMALAER Arockia, SHREE Varnekha, VENESHIA Kathrine: The 17 V's of Big Data, International Research Journal of Engineering and Technology 2017, vol. 4, Issue 9, pp. 329-333, available at https://www.irjet.net/archives/V4/i9/IRJET-V4I957.pdf.

PAPAKONSTANTINOU Vagelis, De HERT Paul: Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA, and the EU regulation of AI. Article published April 1 2021, available at https://lsts.research.vub.be/en/20210401.

PARISE Salvatore, IYER Bela, VESSET Dan: Four strategies to capture and create value from big data. Article published in Ivey Business Journal, July/August issue 2012, available at http://www.iveybusinessjournal.com/topics/strategy/four-strategies-to-capture-and-create-value-from-big-data#.Uwm-L4XHjWh.

PATEL Oliver, NATHAN Lea: EU-U.S. Privacy Shield, Brexit, and the future of transatlantic data flows, published in May 2020 by the UCL European Institute. Article published May 2020, available at https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf.

PAULICK James: The California Invasion of Privacy Act. Article published September 20 2022, available at https://www.leechtishman.com/insights/blog/the-california-invasion-of-privacy-act-californias-wiretap-act/.

PEART Andy: Homage to John McCarthy, the father of Artificial Intelligence. Article published October 29 2020, available at https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence.

PEETS Lisa, HANSEN Mart, CHOI Sam, SHEPHERD Nicholas, OBERSCHELP de MENESES: European Commission presents strategies for data and AI. Article published February 20, 2020, available at https://www.covingtondigitalhealth.com/2020/02/european-commissions-white-paper-on-artificial-intelligence-part-2-of-4/.

PEHLIVAN Ceyhun, CHURCH Peter: The ePrivacy Regulation - let the trilogue begin! Article published February 12 2021, available at https://www.linklaters.com/en/insights/blogs/digilinks/2021/february/eu---the-eprivacy-regulation---let-the-trilogue-begin.

PEPER Erik, HARVEY Richard: Digital Addiction – increased loneliness, anxiety, and depression. Article published March 30 2018, available at https://www.neuroregulation.org/article/view/18189.

PETEREIT Dieter: Google wird seine Tracking-Alternative FLoC zunächst nicht in Europa einführen. Der Suchmaschinenriese will erst die rechtliche Basis klären. DSGVO-Verstöße können schließlich sehr teuer werden. Article published March 24 2021, available at https://t3n.de/news/huch-dsgvo-googles-floc-scheitert-1369031/.

PETERSON Jason, De La TORRE Lydia: Is California on its way to going for 'adequacy'? Article published April 6, 2018, available at https://iapp.org/news/a/is-california-on-its-way-to-going-for-adequacy/#:~:text=A%20California%20adequacy%20decision%20could%20allow%20California-based%20organizations,as%20standard%20contractual%20clauses%2C%20or%20binding%20corporate%20rules%29.

PETRANYI Dora, DOMOKOS Marton: EU adopts NIS2 directive to enhance cybersecurity and resilience. Article published January 4 2023, available at https://www.cms-lawnow.com/ealerts/2023/01/eu-adopts-nis2-directive-to-enhance-cybersecurity-and-resilience.

PETRANYI Dora, HORVATH Katalin, DOMOKOS Marton, BERTOK, Gabor: Hungary adopts new AI strategy. Article published September 18, 2020, available at https://www.cms-lawnow.com/ealerts/2020/09/hungary-adopts-new-ai-strategy.

PIEPER Fritz-Ulli, SCHMALENBERGER Alexander: AI Liability Directive – Welche Haftungsregeln erwarten uns zukünftig für KI? Article published October 4 2022, available at https://www.taylorwessing.com/de/insights-and-events/insights/2022/10/ai-liability-directive-haftungsregeln.

PILTZ Carlo, QUIEL Philipp: The role of „Convention No. 108" and "Convention No. 108+" as part of the examination of the level of protection in third countries under the GDPR. Article published September 1, 2020, available at https://www.delegedata.de/2020/09/the-role-of-convention-no-108-and-convention-no-108-as-part-of-the-examination-of-the-level-of-protection-in-third-countries-under-the-gdpr/.

PILTZ Carlo: Bundeskartellamt erlasst Untersagungsverfügung gegen Facebook – Warum das Vorgehen der Behörde datenschutzrechtlich kritisch betrachtet werden muss. Article published February 7 2019, available at https://www.delegedata.de/2019/02/bundeskartellamt-erlasst-untersagungsverfuegung-gegen-facebook-warum-das-vorgehen-der-behoerde-datenschutzrechtlich-kritisch-betrachtet-werden-muss/.

PILTZ Carlo: Oberster Gerichtshof in Österreich zur Kopplung der Einwilligung nach der DSGVO – grundsätzlich unzulässig? Article published November 13 2018, available at https://www.delegedata.de/2018/11/oberster-gerichtshof-in-oesterreich-zur-kopplung-der-einwilligung-nach-der-dsgvo-grundsaetzlich-unzulaessig/.

PILTZ Carlo: How German data protection authorities interpret the GDPR. Article published July 5 2017, available at https://www.delegedata.de/2017/07/how-german-data-protection-authorities-interpret-the-gdpr/.

PLATH Kai-Uwe: Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Publishing 2016.

POCKLINGTON Robert: The General Data Protection Act (LGPD) in Brazil: "the Brazilian GDPR". Article published September 30 2021, available at https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/general-data-protection-act-lgpd-brazil-brazilian-gdpr-2021-09-30_en.

POWELL Meaghan, SUTTON Lesley: AI regulation: the push for Australian standards. Article published July 29 2019, available at https://www.gtlaw.com.au/insights/ai-regulation-push-australian-standards.

POZZA Duane, RUFF Jacquelyn: The next phase of AI regulation in the U.S. and abroad. Article published July 19, 2019, available at https://www.wileyconnect.com/home/2019/7/19/the-next-phase-of-ai-regulation-in-the-us-and-abroad.

PRAWITZ Dag: Tacit knowledge - an impediment for AI? in: Göranzon et al.: Artifical Intelligence, culture and language: on education and work. Springer Publishing 1990, available at https://doi.org/10.1007/978-1-4471-1729-2_7.

Du PREEZ Derek: UK unveils new 'AI rulebook' that takes different regulatory approach to the EU. Article published July 18 2022, available at https://diginomica.com/uk-unveils-new-ai-rulebook-takes-different-regulatory-approach-eu.

PRESS Gil: A very short history of Artificial Intelligence. Article published December 30 2016, available https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/.

PRICE WATERHOUSE COOPERS: Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Report published August 2019, available at https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

PROUST Olivier: What future for the transfers of personal data? Article published January 18 2022, available at https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/what-future-for-the-transfers-of-personal-data.

PURKAYASTHA Kanan: Challenges from malicious use of AI. Article published May 18 2020, available at https://www.observerbd.com/news.php?id=257035.

PURTOVA Nadezhda: The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology 2018, vol. 10, issue 1, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355.

PURTOVA Nadezhda: Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships. International Data Privacy Law 2018, vol. 8, issue 1, pp. 52-68, available at https://doi.org/10.1093/idpl/ipx021.

Van QUATHEM Kristof: New draft ePrivacy regulation released. Article published on October 14, 2019, available at https://www.insideprivacy.com/international/european-union/new-draft-eprivacy-regulation-released/.

RAJPUKAR Pranav, CHEN Emma, BANERJEE Oishi Banerjee, TOPOL Eric: AI in health and medicine. Article published January 20 2022, available at https://www.nature.com/articles/s41591-021-01614-0.

RAMEAU Katori, HALM K.C.: White House issues guidance for AI regulation and "non-regulation". Article published January 22 2020, available at https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2020/01/white-house-ai-guidelines.

RAMMO Katrin: E-Mail-Werbung künftig auch ohne Einwilligung möglich? Article published March 30 2017, available at https://www.datenschutzbeauftragter-info.de/e-mail-werbung-kuenftig-auch-ohne-einwilligung-moeglich/.

RAMOS Gabriela, MAZZUCATO Mariana: AI in the common interest. Article published December 22 2022, available at https://www.project-syndicate.org/commentary/ethical-ai-requires-state-regulatory-frameworks-capacity-building-by-gabriela-ramos-and-mariana-mazzucato-2022-12.

RAY Tiernan: The public perceives OpenAI's ChatGPT as revolutionary. Article published January 23 2023, available at https://www.zdnet.com/article/chatgpt-is-not-particularly-innovative-and-nothing-revolutionary-says-metas-chief-ai-scientist/.

RAYMOND Nate: Facebook parent Meta to settle Cambridge Analytica scandal case for $725 million. Article published December 23 2022, available at https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/.

REGULATORY INSTITUTE: Report on Artificial Intelligence part I: the existing regulatory landscape. Report published May 14 2018, available at https://www.howtoregulate.org/artificial_intelligence/.

REINHOLD Friederike, MÜLLER Angela: AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – a major step with major gaps. Article published April 22 2021. AlgorithmWatch's response is available at https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/.

REN Daniel: AI, Machine Learning tech promises US$600 billion annually for China economy as it pervades industries, says McKinsey. Article published July 25 2022, available at https://www.scmp.com/business/banking-finance/article/3186409/ai-machine-learning-tech-promises-us600-billion-annually?utm_source=Twitter&utm_medium=share_widget&utm_campaign=3186409.

RICHARDS Neil, KING Jonathan: Three paradoxes of Big Data, Stanford Law Review Online 2013, vol. 66:41, available at http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data.

RIPPY Sarah: Virginia passes the Consumer Data Protection Act. Article published March 3 2021, available at https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

ROACH John: Microsoft finds underwater datacenters are reliable, practical and use energy sustainably. Article published September 14 2020 available at https://news.microsoft.com/source/features/sustainability/project-natick-underwater-datacenter/.

RODRIGUEZ Salvador: Facebook changes company name to Meta. Article published October 28 2021, available at https://www.cnbc.com/2021/10/28/facebook-changes-company-name-to-meta.html.

ROOS Gina: 5G – the next big thing is here. Article published September 25 2020, available at https://www.electronicproducts.com/5g-the-next-big-thing-is-here/.

ROOSA Steven, ROSENZWEIG Daniel: iOS 15: New privacy features industry should note. Article published October 7 2021, available at https://www.ntanalyzer.com/blog/ios-15-new-privacy-features-industry-should-note/.

ROSER Max: The brief history of Artificial Intelligence: The world has changed fast – what might be next? Article published December 6 2022, available at https://ourworldindata.org/brief-history-of-ai**.**

ROßNAGEL Alexander, GEMINN Christian: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. (vzbv) Report published November 2019, available at https://www.heise.de/downloads/18/2/8/0/2/5/0/7/vzbv.pdf.

RUBINSTEIN Ira: Big Data: The end of privacy or a new beginning? International Data Privacy Law 2013, vol. 3, no. 2, pp. 77-81.

SAENKO Kate: It takes a lot of energy for machines to learn – here's why AI is so power-hungry. Article published December 14 2020, available at https://theconversation.com/it-takes-a-lot-of-energy-for-machines-to-learn-heres-why-ai-is-so-power-hungry-151825.

SAIKALI Ali: Federal Data Breach Notification Laws. Article published May 6 2012, available at https://www.datasecuritylawjournal.com/2012/05/06/federal-data-breach-notification-laws/.

SALINAS Madeline: California Privacy Protection Agency holds first meeting. Article published June 24 2021 for Covington & Burling LLP, available at https://www.insideprivacy.com/ccpa/california-privacy-protection-agency-holds-first-meeting-preparing-for-upcoming-rulemaking/.

SANATHKUMAR Sairam: Artificial Intelligence, autonomous vehicles, and Canadian law. Article published December 16 2022, available at https://www.lexpert.ca/legal-insights/artificial-intelligence-autonomous-vehicles-and-canadian-law/372144.

SANDALIZ Kate, TSIRKIN Julie: AI wrote a bill to regulate AI. Now Rep. Ted Lieu wants Congress to pass it. Article published January 26 2023, available at https://www.nbcnews.com/politics/congress/ted-lieu-artificial-intelligence-bill-congress-chatgpt-rcna67752.

SANDERSON Pollyanna: Automated decision systems legislation update. Presentation held on June 14 2021 during a Future of Privacy Forum meeting.

Delli SANTI Marianno: ePrivacy Regulation – an open letter from 30 civil society organizations: our letter to the European Parliament asking them to stand up against online tracking. Article published April 14 2021, available at https://www.openrightsgroup.org/publications/eprivacy-regulation-an-open-letter-from-30-civil-society-organisations/.

SAYER Peter: German court upholds WhatsApp-Facebook data transfer ban. Article published April 26 2017, available at https://www.computerworld.com/article/3192613/german-court-upholds-whatsapp-facebook-data-transfer-ban.html.

Van SCHALK Richard, POLE Francesca: Netherlands – highest court side-steps determining whether legitimate interests may be purely commercial. Article published 28 July 2022, available at https://blogs.dlapiper.com/privacymatters/netherlands-highest-court-side-steps-determining-whether-legitimate-interests-may-be-purely-commercial/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter.

SCHALLBRUCH Martin: E-Evidence – Outsourcing von Grundrechtsschutz. Article published in the CR- blog in May 2018, available at https://www.cr-online.de/blog/2018/05/10/e-evidence-outsourcing-von-grundrechtsschutz-teil-3/.

SCHÄFER Michael: EU-Urheberrechtsreform – Kelber bekräftigt Ablehnung von Upload-Filtern. Article published March 16 2019, available at https://www.computerbase.de/2019-03/eu-urheberrechtsreform-kelber-ablehnung-upload-filtern/.

SCHIRMBACHER Martin: Österreich: Grundrecht auf Datenschutz für juristische Personen. Article published September 1 2020, available at https://haerting.de/wissen/oesterreich-grundrecht-auf-datenschutz-fuer-juristische-personen/#:~:text=F%C3%BCr%20die%20Praxis%20ist%20bedeutend%2C%20dass%20sich%20juristische,Auf%20die%20grundlegenden%20Rechte%20f%C3%BCr%20Betroffene%20k%C3%B6nnen%20.

SCHIFF Allison: Google Will not run FLoC origin tests in Europe due to GDPR concerns. Article published March 23 2021, available at https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/.

SCHMIDT Jens Peter: European Commission proposes world's first ever regulatory framework on Artificial Intelligence. Article published March 23 2021, available at https://www.noerr.com/en/newsroom/news/european-commission-proposes-worlds-first-ever-regulatory-framework-on-artificial-intelligence-ai.

SCHMIDT-ERFURTH Ursula, SEFEGHIPOUR Amir, GERENDASBianca, WALDSTEIN Sebastian, BEGUNOVIC, Hrvoje: Artificial Intelligence in retina. Article published August 1 2018, available at https://pubmed.ncbi.nlm.nih.gov/30076935/.

SCHMON Christoph, GULLO Karen: Euopean's Commission proposed Digital Services Act, got several things right, but improvements are necessary to put users in control. Article published December 15 2020, available https://www.eff.org/deeplinks/2020/12/european-commissions-proposed-regulations-require-platforms-let-users-appeal.

SCHMON Christoph: Our EU policy principles: platform liability. Article published July 9 2020, available at https://www.eff.org/deeplinks/2020/07/effs-eu-policy-principles-platform-liability-and-monitoring.

SCHNEIDER Andreas: Datenschutzgrundverordnung. Presentation held at the KISA forum on February 18 2018, available at https://www.kisa.it/de/datei/anzeigen/id/19667,3/datenschutzgrundverordnung.pdf.

SCHROEDER Calli: When the world's DPAs get together: Resolutions of the ICDPPC. Article published November 28 2017, available at https://iapp.org/news/a/when-the-worlds-dpas-get-together-resolutions-of-the-icdppc/.

SCHÜLER Hans Peter: Cloud Privacy Service zur DSGVO-konformen Nutzung von Microsoft 365. Article published September 6 2021, available at https://www.heise.de/hintergrund/Cloud-Privacy-Service-zur-DSGVO-konformen-Nutzung-von-Microsoft-365-6171165.html.

SCHULZKI-HADDOUTI Christiane: Wenn der stochastische Papagei sich verplappert. Article published February 28 2023, available at https://www.golem.de/news/chatgpt-und-datenschutz-wenn-der-stochastische-papagei-sich-verplappert-2302-172227.html?utm_source=nl.2023-02-28.html&utm_medium=e-mail&utm_campaign=golem.de-newsletter.

SCHULZKI-HADDOUTI Christiane: Scharfe E-Privacy-Verordnung verabschiedet: Mehr Datenschutz, klares Nein zu Hintertüre. Article published October 26 2017, available at https://www.heise.de/newsticker/meldung/Analyse-EU-Kommission-verschlimmbessert-Entwurf-zur-E-Privacy-Verordnung-3594716.html.

SCHULZKI-HADDOUTI Christiane: Datenschutz-Verstöße werden sehr selten sanktioniert. Article published April 4 2016, available at https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/.

SEDOVA Katerina, McNEILL Christine, JOHNSON Aurora, JOSHI Aditi Joshi, WULKAN Ido: AI and the future of disinformation campaign. Center for Security and Emerging Technology Policy brief published December 2021, available at https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/.

SELBY John: Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology 2017, vol. 25, issue 3, pp. 213-232, available at https://academic.oup.com/ijlit/article-abstract/25/3/213/3960261?redirectedFrom=fulltext.

SHAFER Tom: The 42 V's of Big Data and data science. Article published April 1 2017, available at https://www.elderresearch.com/blog/42-v-of-big-data.

SHAPIRO Ivor, MacLEOD Brian: How the "Right to be Forgotten" challenges journalistic principles. Article published 18 November 18 2016, available at https://www.tandfonline.com/doi/abs/10.1080/21670811.2016.1239545?journalCode=rdij20.

SHERER Lori: Data scientists, take a Hippocratic Oath: While the ethics of analytical tools can be tricky to parse, five basic principles can help data scientists address the challenge. Article published June 13 2018, available at https://www.bain.com/insights/data-scientists-take-a-hippocratic-oath-forbes/#.

SHERMAN Justin: Examining state bills on data brokers. Article published May 31 2022, available at https://www.lawfareblog.com/examining-state-bills-data-brokers.

SHIVA Stella: Senate releases principles for comprehensive privacy legislation. Article published on November 18 2019, available at https://www.publicknowledge.org/press-release/senate-releases-principles-for-comprehensive-privacy-legislation/.

SHORTEN Connor: Machine Learning vs. Deep Learning. Article published on September 7, 2018, available at https://towardsdatascience.com/machine-learning-vs-deep-learning-62137a1c9842.

SIMITIS Spiros: Bundesdatenschutzgesetz. Nomos Publishing Baden Baden 2014.

SIMPSON Meagan: Canada, France governments announce declaration of the International Panel on AI. Article published May 16 2019, available at http://canada.ai/posts/canada-france-governments-announce-declaration-of-the-international-panel-on-ai.

SIMONITE Tom: Should data scientists adhere to a Hippocratic Oath? Article published on August 2 2018, available at https://www.wired.com/story/should-data-scientists-adhere-to-a-hippocratic-oath/.

SINGH Ranjeet: The rise and fall of symbolic AI. Article published September 14 2019, available at https://towardsdatascience.com/rise-and-fall-of-symbolic-ai-6b7abd2420f2.

SIWICKI Bill: Is synthetic data the key to healthcare clinical and business intelligence? Article published February 21 2020, available at https://www.healthcareitnews.com/news/synthetic-data-key-healthcare-clinical-and-business-intelligence.

SJOUWERMAN Stu: Seven reasons for cybercrime's meteoric growth. Article published December 23 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/#:~:text=Cybercrime%20has%20been%20on%20the%20rise%20for%20years.,more%20criminals%20are%20leveraging%20the%20internet%20to%20steal.

SLATER Felicity: The future of manipulative design regulation. Article published January 19 2022, available at https://fpf.org/blog/the-future-of-manipulative-design-regulation/.

De SMEDT Stephanie: Free flow of non-personal data and GDPR. Article published June 19 2019, available at https://www.lexology.com/library/detail.aspx?g=240c3d71-f818-4233-a7f3-01b32f17b3b3.

SOLOVE Daniel: Introduction: privacy self-management and the consent dilemma. Harward Law Review 2013, vol. 126:1880, pp. 1886-1903.

SOLOVE Daniel: Understanding Privacy. Harvard University Press 2008.

SOLOVE Daniel: Conceptualizing privacy. California Law Review 2005, vol. 90, no. 4, pp. 1132-1140, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.

SOLOMON Howard: Privacy by Design to become an ISO standard next month. Article published January 11 2023, available at https://www.itworldcanada.com/article/privacy-by-design-to-become-an-iso-standard-next-month/521415?mkt_tok=MTM4LUVaTS0wNDIAAAGJS0q3vTc2wGOv97CzHvWrfuVuy0g03NHESUYs9hBY2VJUZx2kRq7P8-PHtd90alDmo9rCjwp7I7WYC4fteM6-Dfx4qV5xattmN-4oeH16JcM7**.**

SPÄTH Dennis: Artificial Intelligence is transforming the workforce as we know it. Article published March 18, 2019, available at https://workplaceinsight.net/artificial-intelligence-is-transforming-the-workforce-as-we-know-it/.

SPIES Axel: Germany and the EU Artificial Intelligence Act. Article published July 29 2022, available at https://www.aicgs.org/2022/07/germany-and-the-eu-artificial-intelligence-act/.

SPLITTGERBER Andy: German cookie law enters into force on December 1, 2021. Article published May 21 2021, available at https://viewpoints.reedsmith.com/post/102gyp8/german-cookie-law-enters-into-force-on-dec-1-2021.

STATEWATCH: Building the biometric state – police powers and discrimination. Report published February 28 2022, available at https://www.statewatch.org/news/2022/february/eu-ongoing-rollout-of-biometric-identification-systems-likely-to-exacerbate-ethnic-profiling/.

STAUSS David: Status of proposed CCPA-like state privacy legislation as of May 3, 2021. Article published May 2 2021, available at https://www.bytebacklaw.com/2021/05/status-of-proposed-ccpa-like-state-privacy-legislation-as-of-may-3-2021/.

STEINMÜLLER Wilhelm: Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann. Recht der Datenverarbeitung 2007, pp. 158-161.

STENTZEL Rainer: Das Grundrecht auf ...? Auf der Suche nach dem Schutzgut des Datenschutzes in der Europäischen Union, PingG (Privacy in Germany), issue 5, pp. 185-191, available at https://www.pingdigital.de/ce/das-grundrecht-auf/detail.html.

STENTZEL Rainer: Das Grundrecht auf ...? Auf der Suche nach dem Schutzgut des Datenschutzes in der Europäischen Union, Privacy in Germany, issue 5, pp. 185-191, available at https://www.pingdigital.de/ce/das-grundrecht-auf/detail.html.

STEPPE Richard: Online price discrimination and personal data: A General Data Protection Regulation perspective, Computer Law & Security Review 2017, vol. 33, issue 6, pp. 768-785, available at https://www.sciencedirect.com/science/article/abs/pii/S0267364917301656.

STEPHENSON Sean, LALONDE Paul: The limits of data localization laws. Article published August 9 2019, available at http://www.dentonsdata.com/the-limits-of-data-localization-laws-trade-investment-and-data/.

STIRLING Richard, MILLER Hannah, MARTINHO-TRUSWELL Emma: Oxford Institute government AI readiness index, Article published in 2017, available at https://www.oxfordinsights.com/government-ai-readiness-index?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BeJ%2FPpiq8RzyLuLPtyf%2FYoA%3D%3D.

STOKEL-WALKER Chris: The most data-invasive health and fitness apps. Article published May 13 2022, available at https://cybernews.com/privacy/the-most-data-invasive-health-and-fitness-apps/.

STOLTON Samuel: After Clearview AI scandal, Commission 'in close contact' with EU data authorities. Article published February 12 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/.

SYSIAK Pawel: Exponential growth of computing. Article published March 21 2016, available at https://medium.com/ai-revolution/exponential-growth-of-computing-a836fce8b907.
TAI Nancy: Dimensions of Big Data. Article published July 27 2018, available at http://www.klarity-analytics.com/2015/07/27/dimensions-of-big-data/.

TAKASE Kensaku: GDPR matchup – Japan's act on the protection of personal information. Article published August 29 2017, available at https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/.

TANIMOTO Steven: The elements of Artificial Intelligence. Computer Science Press 2010.

TAYLOR Josh, HERN Alex: 'Godfather of AI' Geoffrey Hinton quits Google and warns over dangers of misinformation. Article published May 2 2023, available at https://www.theguardian.com/technology/2023/may/02/geoffrey-hinton-godfather-of-ai-quits-google-warns-dangers-of-machine-learning.

TENE Omer, POLONETSKY Jules: Big Data for all – privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property 2013, vol. 11, issue 5, pp. 239-273, available at https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip.

TENE Omer, POLONETSKY Jules: Privacy in the age of Big Data – a time for big decisions, Stanford Law Review 2012, vol. 64:63.

TENE Omer: Privacy for the rich or for the poor? Concurring Opinions. Article published July 26 2012, available at http://www.concurringopinions.com/archives/2012/07/privacy-for-the-rich-or-for-the-poor.html.

TIELEMANS Jetty: EU data initiatives in context. Infographic published (last updated) March 22, available at https://iapp.org/resources/article/infographic-recent-eu-data-initiatives-in-context/?mkt_tok=MTM4LUVaTS0wNDIAAAGFbmT22pIZgQLYKokUEfduUMWT7bFxo5xvWxumwh--7YEQwlsG4QbKMQD-kqpMdUBMkR8dCpMAoXQzsLORoDI7IY507c26mwLwi8YYxQBk-B24.

TIELEMANS Jetty, FAZLIOGLU Müzge: ePrivacy Regulation - Q&A on select topics. Article published May 25 2021, available at https://iapp.org/news/a/eprivacy-regulation-qa-on-select-topics/.

TIELEMANS Jetty: A look at what's in the EU's newly proposed regulation on AI. Article published April 21 2021, available at https://iapp.org/news/a/a-look-at-whats-in-the-eus-newly-proposed-regulation-on-ai/.

TIMON Victor, HART Helen: EU plans changes to e-commerce and competition law. Article published June 10 2020, available at https://www.lewissilkin.com/en/insights/eu-plans-changes-to-e-commerce-and-competition-law.

De La TORRE Lydia: GDPR matchup – the California Consumer Privacy Act. Article published July 31 2018, available at https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.

TOTH Anne: New EU data protection law is a milestone in privacy regulation. Article published May 23 2018, available at https://www.thenationalnews.com/business/technology/new-eu-data-protection-law-a-milestone-in-privacy-regulation-

1.733347#:~:text=New%20EU%20data%20protection%20law%20a%20milestone%20in,half%20a%20billion%20European%20A%20European%20Union%20flag.

UNIVERSITY OF STANFORD: One-hundred-year study on Artificial Intelligence (AI100). Report published 2015, available at https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.

VALE Sebastião Barros, ZANFIR-FORTUNA Gabriela for Future of Privacy Forum: Automated decision-making under the GDPR – practical cases from courts and data protection authorities. Paper published May 2022.

VALE Marshall: Privacy, sustainability and the importance of "and". Article published March 30 2021, available at https://blog.google/products/chrome/privacy-sustainability-and-the-importance-of-and/.

VANIAN Jonathan: Why tech insiders are so excited about ChatGPT, a chatbot that answers questions and writes essays. Article published December 13 2022, available at https://www.cnbc.com/2022/12/13/chatgpt-is-a-new-ai-chatbot-that-can-answer-questions-and-write-essays.html.

VEALE Michael, ZUIDERVEEN BORGESIUS Frederik: Demystifying the draft EU Artificial Intelligence Act. Article published July 31 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852.

VEIL Winfried: Zum Schutzgut der DSGVO – eine naive Wortlautanalyse. Article published April 22 2021, available at https://www.cr-online.de/blog/2021/04/22/zum-schutzgut-der-ds-gvo-eine-naive-wortlautanalyse/.

VEIL Winfried: Die Schutzgutmisere des Datenschutzrechts (Teil I). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/.

VEIL Winfried: Die Schutzgutmisere des Datenschutzrechts (Teil II). Article published February 6 2019, available at https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/.

VEIL Winfried: 21 Thesen zum Irrweg der DSGVO. Article published May 23 2018, available at https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker4.

VEIL Winfried: Accountability – wie weit reicht die Rechenschaftspflicht der DSGVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs. Zeitschrift für Datenschutz 2018, vol. 1, pp. 9-16.

VILLANI Cedric: For a meaningful Artificial Intelligence – towards a French and European strategy. Article published March 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.

VILLASENOR John: Products liability law as a way to address AI harms. Article published October 31, 2019, available at https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/.

VITARIS Benjamin: Data Residency: Meaning, Laws, & Requirements. Article published July 30 2020, available at https://permission.io/blog/data-residency/.

VOISKUNSKY Alexander, SOLDATOVA Galina: The loneliness epidemic in the digital society: Hikikomori as a cultural and psychological phenomenon. Article published in the Journal for

Consultative Psychology and Psychotherapy 2019, vol. 27, no. 3, pp. 22-43. An English translation of the article is available at https://translated.turbopages.org/proxy_u/ru-en.ru.01322d87-62e6acea-b532bfdd-74722d776562/https/psyjournals.ru/files/108495/cpp_2019_n3_Voiskunskii_Soldatova.pdf.

VOLLMER Timothy: Copyright filtering mechanisms don't (and can't) respect fair use. Article published February 22 2017, available at https://creativecommons.org/2017/02/22/copyright-filtering-mechanisms-dont-cant-respect-fair-use/.

WACHTER Sandra, MITTELSTADT Brent, FLORIDI Luciano: Why a right to explanation of automated decision-making does not exist in the GDPR. International Data Privacy Law 2017, vol. 7, issue 2, pp. 76-99.

WAEM Heidi, VERSCHAEVE, Simon: What's left of the GDPR's one-stop-shop? CJEU clarifies the competences of non-lead data protection authorities. Article published July 5 2021, available at https://blogs.dlapiper.com/privacymatters/eu-whats-left-of-the-gdprs-one-stop-shop-cjeu-clarifies-the-competences-of-non-lead-data-protection-authorities/?utm_source=mailpoet&utm_medium=email&utm_campaign=privacy-matters-newsletter.

WAGNER Ben: Ethics as an escape from regulation. From ethics-washing to ethics-shopping? In: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds): BEING PROFILED: COGITAS ERGO SUM. 10 Years of Profiling the European Citizen, 2018: Amsterdam University Press, 84-88.

WANG Gang: Tech Talk: Intuit's AI-powered tax knowledge engine boosts filers' confidence. Article published March 6 2019, available at https://www.intuit.com/blog/social-responsibility/tech-talk-intuits-ai-powered-tax-knowledge-engine-boosts-filers-confidence/?q=knowledge+engineering++taxation&qs=n&form=QBRE&sp=-1&pq=knowledge+engineering+taxation&sc=0-30&sk=&cvid=C86F17EA921A4662B0AEE8187B558298.

WAREHAM Mary: Statement on lethal autonomous weapons systems to the CCW Annual Meeting. Article published November 16, 2022 https://www.hrw.org/news/2022/11/16/statement-lethal-autonomous-weapons-systems-ccw-annual-meeting-0.

WARREN Samuel, BRANDEIS Louis: The right to privacy. Harvard Law Review, vol. 4, no. 5. 1890, pp. 193-220.

WEIZENBAUM INSTITUT: Statement on the proposed Digital Content Directive. The statement was published July 4 2018, available at https://www.weizenbaum-institut.de/index.php?id=107&tx_news_pi1%5Baction%5D=&tx_news_pi1%5Bcontroller%5D=&tx_news_pi1%5Bnews%5D=36&L=5&cHash=416e3183f5ac501a1777c33e947ff6ae.

WENTING Zhou: Shanghai unveils 10-year AI plan. Article published July 12 2021, available at https://english.www.gov.cn/news/topnews/202107/12/content_WS60eb9428c6d0df57f98dcbbb.html.

WERRY Susanne: New German model for the calculation of GDPR fines - a blueprint for Europe? Article published October 21 2019, available at https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2019/10/new-german-model-for-the-calculation-of-gdpr-fines.html.

WESTIN Alan: Social and political dimensions of privacy. Journal of Social Issues 2003, vol. 59, no. 2, pp. 431-434, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.4866&rep=rep1&type=pdf.

WHITE Lara, BUNDY-CLARKE, Fiona: Tentative further steps towards an agreed ePrivacy Regulation. Article published February 15 2021, available at https://www.dataprotectionreport.com/2021/02/tentative-further-steps-towards-an-agreed-eprivacy-regulation/.

WILSON James, DAUGHERTY Paul, DAVENPOR, Chase: The future of AI will be about less data, not more. Article published January 14 2019, available at https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more.

WITZLEB Eva, SCHUHMACHER Pascal: Datenschutz vs. Kartellrecht - Die nächste Runde. Article published May 6 2021, available at https://www.noerr.com/de/newsroom/news/datenschutz-vs-kartellrecht.

WOMEN LEADING IN AI: 10 principles for responsible AI. White Paper published in 2019, available at https://womenleadinginai.org/report2019.

WORLD ECONOMIC FORUM: Research shows AI is often biased. Here's how to make algorithms work for all of us. Article published July 19 2021, available at https://www.weforum.org/agenda/2021/07/ai-machine-learning-bias-discrimination/.

WRIGHT David, De HERT Paul, GUTWIRTH Serge: Are the OECD guidelines at 30 showing their age? Communications of the ACM 2011, vol. 54, issue 2, pp. 119-127.

WRIGHT Connor: The ethical need for watermarks in machine-generated language. Article published November 27 2022, available at https://montrealethics.ai/the-ethical-need-for-watermarks-in-machine-generated-language/?utm_source=substack&utm_medium=email.

WU Wenjun, KEGONG Tiejun Huang: Ethical principles and governance technology development of AI in China, Engineering vol. 6, issue 3, March 2020, pp. 302-309.

YAVUZDOGAN OKUMUS Begüm, BADA Direnç: Turkish data localization rules in effect for social media companies. Article published October 14 2020, available at https://gun.av.tr/insights/articles/turkish-data-localization-rules-in-effect-for-social-media-companies?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

YOU Joanna, BERNEY Louis: Guangzhou International Institute of AI launched in Nansha. Article published December 15 2017, available at https://www.lifeofguangzhou.com/whatsNew/content.do?contextId=6987&frontParentCatalogId=199&frontCatalogId=200.

YOUNG Mark, CHOI Sam Jungyun, ONG Jiayen: Global CBPR Forum – a new international data transfer mechanism. Article published May 2 2023, available at https://www.insideprivacy.com/cross-border-transfers/global-cbpr-forum-a-new-international-data-transfer-mechanism/.

YOUNG Mark, MAYNARD Paul, OBERSCHELP de MENESES Anna: Three interesting features of the proposed EU Cyber Solidarity Act. Article published April 29 2023, available at https://www.insideprivacy.com/cybersecurity-2/stronger-cybersecurity-reducing-cyber-incidents-greater-eu-strategic-autonomy-three-interesting-features-of-the-proposed-eu-cyber-solidarity-act/.

ZARSKY Tal: The Trouble with algorithmic decisions: An analytic roadmap to examine efficiency and fairness in automated and opaque decision making, Science, Technology, & Human Values 2016, vol. 41 (1), pp. 118-132.

ZUBIK Marek, PODKOWIK Jan, RYBSKI Robert: European constitutional courts towards data retention laws. Springer Nature Switzerland AG 2021.

ZUBOFF Shoshanna: The age of surveillance capitalism – the fight for human future at the new frontier of power. Profile Books, 2019.

ZWEIG Katharina, FISCHER Sarah, LISCHKA Konrad: Wo Maschinen irren können – Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung, Bertelsmann Stiftung Publishing 2018.

Resources

This part of the Thesis provides an overview of relevant resources: conventions, regulations, directives, resolutions, trade agreements as well as non-binding initiatives, recommendations, and guidance at international, EU and non-governmental level, as well as various technical standards.

Conventions, declarations, and resolutions[1891]

Convention on Human Rights, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.

Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data (Council of Europe Data Protection Convention – Convention 108) 1981 version available at https://rm.coe.int/16808ade9d.

Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data (Council of Europe Data Protection Convention – Convention 108+). Modernized version available at https://rm.coe.int/16808accf8.

Charter of Fundamental Rights of the European Union, available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), available at https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.

European Parliament Resolution with recommendations to the Commission on a civil liability regime for Artificial Intelligence (2020/2014(INL), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

European Parliament Resolution on intellectual property rights for the development of Artificial Intelligence technologies (2020/2015(INI), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html.

European Parliament Resolution with recommendations to the Commission on a framework of ethical aspects of Artificial Intelligence, robotics and related technologies (2020/2012(INL), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html#:~:text=European%20Parliament%20resolution%20of%2020%20October%202020%20with,artificial%20intelligence%2C%20robotics%20and%20related%20technologies%20%282020%2F2012%20%28INL%29%29.

International Covenant on Civil and Political Rights, available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf.

Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data: 1980 version available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines.

[1891] This refers to conventions, declarations, and resolutions at international level.

Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data: 2013 version available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

United Nations Convention on Certain Conventional Weapons, available at https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/.

United Nations Convention on Migrant Workers, available at http://www.un.org/documents/ga/res/45/a45r158.htm.

United Nations Convention on Rights of the Child, available at http://www.un.org/documents/ga/res/44/a44r025.htm.

United Nations Guidelines on Consumer Protection, available at https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf.

United Nations Regulation on Automated Lane Keeping Systems (ALKS) available at https://unece.org/sustainable-development/press/un-regulation-automated-lane-keeping-systems-alks-extended-trucks.

United Nations Resolution on the Right to Privacy in the Digital Age, available at https://digitallibrary.un.org/record/848969/files/A_C-3_71_L-39_Rev-1-EN.pdf.

United Nations Universal Declaration of Human Rights, available at http://www.un.org/en/universal-declaration-human-rights/index.html.

Vienna Convention on Road Traffic, available at https://globalautoregs.com/rules/157-1968-vienna-convention-on-road-traffic?show=agreements.

Global trade agreements

Comprehensive Economic and Trade Agreement (CETA) between Canada and the European Union, available at https://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), available at https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents/Pages/official-documents.

World Trade Organization’s General Agreement on Trade and Services (GATS), available at https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm.

Directives and regulations[1892]

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31996L0009.

Directive 98/44/EC on the legal protection of biotechnological inventions is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31998L0044.

[1892] This refers to directives and regulations at EU level.

Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation. available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078.

Directive 2000/43/EC on equal treatment and against discrimination and Directive 2004/113/EC on equality in the access to and supply of goods and services, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML.

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

Directive 2006/54/EC of the European Parliament and of the Council on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054.

Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0022.

Directive 2009/43/EC on intra-EU transfers of defense-related products, available at https://ec.europa.eu/growth/sectors/defence/transfers-products_en#:~:text=The%20transfer%20directive%20Directive%202009%2F43%2FEC%20on%20intra-EU%20transfers,for%20transfers%20of%20defence-related%20products%20within%20the%20EU.

Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0065.

Directive 2016/680 of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG.

Directive 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

Directive 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0770.

Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374.

Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.409.01.0001.01.ENG.

Regulation 536/2014 of the European Parliament and of the Council on clinical trials on medicinal products for human use, available at https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf.

Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

Regulation 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725.

Regulation 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.303.01.0059.01.ENG.

Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber-security Agency", and repealing Regulation 526/2013, and on Information and Communication Technology Cyber-Security Certification ("Cybersecurity Act"), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0151+0+DOC+PDF+V0//EN.

Recommendations and guidelines[1893]

Association for Computing Machinery (ACM) statement on Algorithmic Transparency and Accountability, available at https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf.

CNIL report on ethical issues of Algorithms and Artificial Intelligence published May 25 2018, available at https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues.

Council of Europe Commissioner for Human Rights recommendation, available at https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.

Council of Europe Recommendations on Human Rights Impacts of Algorithmic Systems, available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

Datenschutzkonferenz: Auskunftsrecht der betroffenen Person nach Art. 15 DSGVO published 2017, available at https://www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf.

European Commission Ethics Guidelines for trustworthy AI, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[1893] This section is non-exhaustive and lists a selection of important recommendations and guidelines regardless of whether they have been issued by the EU or a public body, or if they are the result of a private sector / multistakeholder or NGO initiative.

European Commission White Paper on Artificial Intelligence, available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Ethical Charter on the Use of AI in Judicial Systems (CEPEJ), available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

European Center for Non-For-Profit-Law: Recommendations for assessing AI impacts to human rights, democracy, and the rule of law. Paper published November 2021, available at https://ecnl.org/publications/recommendations-incorporating-human-rights-ai-impact-assessments.

Fairness, Accountability, and Transparency in Machine Learning (FAT / ML) Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, available at https://www.fatml.org/resources/principles-for-accountable-algorithms.

Future of Life Institute Asilomar AI Principles, available at https://futureoflife.org/ai-principles/.

G7 statement on Artificial Intelligence and society, available at https://www.leopoldina.org/en/publications/detailview/publication/g7-statement-artificial-intelligence-and-society-2019/.

G20 AI principles, available at https://www.mofa.go.jp/files/000486596.pdf.

ICO GDPR guidance – contracts and liabilities between controllers and processors published 2018, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf.

ICO guidance on AI and data protection last updated March 25 2013, available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/.

ICO guide to the General Data Protection Regulation published 2018, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

Information Accountability Foundation Fair and Open Use Act, available at https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2021/05/FAIR-and-OPEN-USE-Act-May-26-2021-1.pdf?time=1623678345.

Information Accountability Foundation Fair Processing Principles, available at https://informationaccountability.org/publications/.

International Conference of Data Protection and Privacy Commissioners (ICDPPC) Declaration on Ethics and Data Protection in Artificial Intelligence, available at https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

IEEE Ethically Aligned Design, available at https://engagestandards.ieee.org/rs/211-FYL-955/images/EAD1e.pdf?mkt_tok=eyJpIjoiWkRVME1UVm1OREE1TVRSbSIsInQiOiIxY3RONFl6YXh0cWxSRUpLNE9taUtwQllpaXNkYktmd3FDM2lOQ1ZNXC9YUURKV3Z4b2dJc3d3ekNDREdTd24zMHNcL0xUTEFqeFFoYTN4NWNqQUZRclY0amMyTzhXeU9VXC9yNjhneWlIeHFHV3lSMU1rRGxmeUJSTU9cL3dDeXZmN1AifQ%3D%3D.

International Working Group on Data Protection in Telecommunications (IWGDPT) working paper on Privacy and Artificial Intelligence, available at https://www.datenschutz-

berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf.

Japan's AI R&D Guidelines, available at http://www.soumu.go.jp/main_content/000507517.pdf.

Madrid Resolution, available at https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf.

Montreal declaration for a responsible development of Artificial Intelligence, available at https://www.montrealdeclaration-responsibleai.com/the-declaration.

Organization for Economic Co-operation and Development (OECD) AI principles, available at http://www.oecd.org/going-digital/ai/principles/.

The Toronto Declaration: Protecting the right to equality and non-discrimination in Machine Learning systems, available at https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf.

UNESCO Beijing Consensus on Artificial Intelligence and Education, available at http://en.moe.gov.cn/news/press_releases/201909/t20190902_396913.html#:~:text=UNESCO%20has%20just%20published%20the%20Beijing%20Consensus%20on,objectives%20set%20out%20in%20the%20Education%202030%20Agenda.

UNESCO Recommendation on the Ethics of Artificial Intelligence, available at https://ircai.org/wp-content/uploads/2020/07/Recommendation_first_draft_ENG.pdf.

UNICEF Policy Guidance AI for Children, available at https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf.

UNI Global Union top 10 Principles for Ethical Artificial Intelligence, available at http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf.

Universal Guidelines for Artificial Intelligence (UGAI) available at https://blog.epic.org/2018/10/23/universal-guidelines-artificial-intelligence-announced-brussels/.

WOMEN LEADING IN AI White Paper:10 Principles for Responsible AI available at https://womenleadinginai.org/report2019.

World Economic Forum White Paper on AI, available at http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discriminatory_Outcomes_in_Machine_Learning.pdf.

AI and ADM specific laws[1894]

Advancing American Artificial Intelligence Act, available at https://www.congress.gov/bill/117th-congress/senate-bill/1353/text?q=%7B%22search%22%3A%5B%22data+OR+privacy%22%5D%7D&r=27&s=5.

Advancing Artificial Intelligence Research Act, available at https://www.congress.gov/bill/116th-congress/senate-bill/3891.

[1894] These are at the same time U.S. laws. Given the dynamics, the list is not exhaustive.

Algorithmic Accountability Act, available at https://www.congress.gov/bill/116th-congress/senate-bill/1108.

Artificial Intelligence in Government Act, available at https://www.congress.gov/bill/115th-congress/senate-bill/3502.

Artificial Intelligence Reporting Act, available at https://www.congress.gov/bill/115th-congress/house-bill/6090/.

Future of Artificial Intelligence Act, available at https://www.congress.gov/bill/115th-congress/house-bill/4625.

Growing Artificial Intelligence Through Research Act, available at https://www.congress.gov/bill/116th-congress/house-bill/2202.

Mind Your Own Business Act, available at https://www.congress.gov/bill/117th-congress/senate-bill/1444/text?q=%7B%22search%22%3A%5B%22automated+decision-making%22%5D%7D&r=3&s=3.

National Artificial Intelligence Initiative Act, available at https://www.congress.gov/bill/116th-congress/house-bill/6216.

Protecting Americans from Dangerous Algorithms Act, available at https://www.congress.gov/bill/117th-congress/house-bill/2154?q=%7B%22search%22%3A%5B%22algorithmic%22%5D%7D&s=1&r=2.

Washington, D.C.'s Stop Discrimination by Algorithms Act of 2021, available at https://oag.dc.gov/release/ag-racine-introduces-legislation-stop.

U.S. legislation[1895]

Age Discrimination in Employment Act (ADEA), available at https://www.ecfr.gov/current/title-29/subtitle-B/chapter-XIV/part-1625#:~:text=%C2%A7%201625.2%20Discrimination%20prohibited%20by%20the%20Act.%20It,older%2C%20unless%20one%20of%20the%20statutory%20exceptions%20applies.

American Data Privacy and Protection Act (ADPPA), available at https://www.congress.gov/bill/117th-congress/house-bill/8152.

Balancing the Rights of Web Surfers equally and responsibly Act, available at https://www.congress.gov/bill/117th-congress/senate-bill/113.

Banning Surveillance Advertising Act, available at http://eshoo.house.gov/sites/evo-subsites/eshoo-evo.house.gov/files/BanningSurveillanceAdvertisingAct.pdf.

California Consumer Privacy Act (CCPA), available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

California Genetic Information Privacy Act, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB41.

[1895] U.S. bills may not have specific titles, and abbreviations may furthermore not be final Given the dynamics in this field of law, the list is not exhaustive.

California Online Privacy Protection Act (CalOPPA), available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC.

California Privacy Rights Act (CPRA), available at https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/.

Children's Online Privacy Protection Act (COPPA), available at https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

Colorado Privacy Act, available at https://leg.colorado.gov/bills/sb21-190.

Connecticut Privacy Act, available at https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN SPAM Act), available at https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf.

Deceptive Experiences to Online Users Reduction Act (DETOUR Act), available at https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

Facial Recognition and Biometric Technology Moratorium Act, available at https://www.congress.gov/bill/117th-congress/senate-bill/2052/text.

Fair Credit Reporting Act (FCRA), available at https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F.

Fair Housing Act (FFHA), available at https://www.justice.gov/crt/fair-housing-act-2.

Florida Protecting DNA Privacy Act, available at https://flsenate.gov/Session/Bill/2021/833.

Freedom of Information Act (FOIA), available at https://www.govtrack.us/congress/bills/89/s1160.

Genetic Information Nondiscrimination Act (GINA), available at https://www.govtrack.us/congress/bills/110/hr493/text.

Gramm-Leach-Bliley-Act (GLBA), available at https://www.sec.gov/about/laws/glba.pdf.

Hawaii Consumer Data Protection Act, available at https://www.capitol.hawaii.gov/session/measure_indiv.aspx?billtype=SB&billnumber=974&year=2023.

Health Insurance Portability and Accountability Act (HIPAA), available at https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

Illinois Biometric Information Privacy Act (BIPA), available at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

Indiana Data Protection Act, available at https://iga.in.gov/legislative/2023/bills/senate/5#document-b95da0f8.

Internet of Things Cybersecurity Improvement Act (IoT Security Bill), available at https://www.congress.gov/bill/116th-congress/house-bill/1668.

Iowa Consumer Data Protection Act, available at
https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=HSB12.

Kentucky Consumer Data PrivacyAct, available at
https://apps.legislature.ky.gov/record/23rs/sb15.html

Maryland Consumer Protection Act (Online and Biometric Data Privacy), available at
https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0698?ys=2023RS.

Massachusetts Data Privacy Protection Act (MDPPA), available at
https://malegislature.gov/Bills/193/SD745.

Massachusetts Information Privacy and Security Act (MIPSA), available at
https://malegislature.gov/Bills/193/SD1971.

Minnesota Privacy Act, available at
https://www.revisor.mn.gov/bills/bill.php?b=Senate&f=SF0950&ssn=0&y=2023&keyword_type=all&keyword=privacy.

Mississippi Consumer Data Privacy Act, available at
http://billstatus.ls.state.ms.us/2023/pdf/history/SB/SB2080.xml.

Montana Privacy Act, available at
https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231.

New Hampshire Data Privacy Act, available at
https://www.gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1.

New Jersey Disclosure and Accountability Transparency Act, available at
https://legiscan.com/NJ/bill/A505/2022.

New York privacy act, available at
https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S00365&term=2023&Summary=Y&Actions=Y&Text=Y.

New York Employee Monitoring Law, available at
https://www.nysenate.gov/legislation/bills/2019/s4586.

Oklahoma Computer Data Privacy Act, available at
http://www.oklegislature.gov/BillInfo.aspx?Bill=HB1602&session=2100.

Quantum Computing Cybersecurity Preparedness Act, available at https://www.congress.gov/bill/117th-congress/house-bill/7535/text.

Rhode Island Data Transparency and Privacy Protection Act, available at
http://webserver.rilegislature.gov/BillText/BillText23/HouseText23/H5354.pdf.

Social Media Privacy Protection and Consumer Rights Act, available at
https://www.congress.gov/bill/116th-congress/senate-bill/189/text.

Texas privacy bill (Act Relating to the Regulation of the Collection, Use, Processing, and Treatment of Consumers' Personal Data by Certain Business Entities) available at
https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB1844.

Transparency and Personal Data Control Act (ITPDCA), available at https://www.congress.gov/bill/117th-congress/house-bill/1816/text.

Telemarketing Sales Rule (TSR), available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr310_main_02.tpl.

Telephone Consumer Protection Act (TCPA), available at https://www.govinfo.gov/content/pkg/FR-2012-06-11/pdf/2012-13862.pdf.

Tennessee Information Protection Act. available at https://www.capitol.tn.gov/Bills/113/Bill/SB0073.pdf.

Utah Consumer Privacy Act (UCPA), available at https://le.utah.gov/~2022/bills/static/SB0227.html.

Utah Genetic Information Privacy Act, available at https://le.utah.gov/~2021/bills/static/SB0227.html.

Vermont Consumer Data Privacy Act, available at https://legislature.vermont.gov/bill/status/2024/H.121.

Virginia Consumer Data Protection Act (VCDPA), available at https://law.lis.virginia.gov/vacode/title59.1/chapter53/.

West Virginia Consumer Data Protection Act, available at http://www.wvlegislature.gov/Bill_Status/Bills_history.cfm?input=3498&year=2023&sessiontype=RS&btype=bill.

Technical standards[1896]

ISO standards

ISO/IEC JTC 1/SC 41: Internet of Things and digital twin, available at https://www.iso.org/committee/6483279.html.

ISO/IEC JTC 1/SC 38: Cloud Computing and distributed platforms, available at https://www.iso.org/committee/601355.html.

ISO/IEC JTC 1/SC 37: Biometrics, available at https://www.iso.org/committee/313770.html.

ISO/IEC 23894: AI Risk Management, available at https://www.iso.org/standard/77304.html

ISO/IEC WD 42001: AI Management systems, available at https://www.iso.org/standard/81230.html.

ISO/IEC WD 5338 73: AI system life cycle processes, available at https://www.iso.org/standard/81118.html.

ISO/IEC AWI TR 5469: Functional safety and AI systems, available at https://www.iso.org/standard/81283.html.

ISO/IEC AWI TR 24368: Overview of ethical and societal concerns, available at https://www.iso.org/standard/78507.html.

ISO/IEC TR 24027: Bias in AI systems and AI-aided decision making, available at https://www.iso.org/standard/77607.html?browse=tc.

[1896] Some of the listed standards may not yet be finalized.

ISO/IEC CD 24668: Process management framework for Big Data analytics. available at https://www.iso.org/standard/78368.html.

ISO/IEC CD 38507: Governance implications of the use of AI by organizations, available at https://www.iso.org/standard/56641.html.

ISO/IEC TR 24028:2020: Overview of trustworthiness in Artificial Intelligence, available at https://www.iso.org/standard/77608.html.

ISO/IEC DTR 24029-1: Robustness of neural networks, available at https://www.iso.org/standard/77609.html.

ISO/IEC AWI 24029-2: Robustness of neural networks, available at https://www.iso.org/standard/79804.html.

ISO/IEC AWI TR 24372: Overview of computational approaches for AI systems, available at https://www.iso.org/standard/78508.html.

ISO/IEC WD TS 4213 76: Assessment of Machine Learning classification performance, available at https://www.iso.org/standard/79799.html.

ISO/IEC AWI 25059: Quality model for AI-based systems (Systems and software Quality Requirements and Evaluation: SQuaRE), available at https://www.iso.org/standard/80655.html.

ETSI standards

DGR SAI-001: Securing Artificial Intelligence: AI Threat Ontology, available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856.

DGR SAI-002: Securing Artificial Intelligence: Data Supply Chain Report, available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857.

DGS SAI-003: Securing Artificial Intelligence: Security Testing of AI, available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58860.

DGR SAI-005: Securing Artificial Intelligence: Mitigation Strategy Report, available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59214

TR 103 674 SmartM2M – Artificial Intelligence and the oneM2M architecture, available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57866.

TR 103 675 SmartM2M: AI for IoT: A Proof of Concept, available at https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57867.

GS/ARF-003: Augmented Reality Framework architecture, available at https://www.etsi.org/deliver/etsi_gs/ARF/001_099/003/01.01.01_60/gs_ARF003v0101 01p.pdf.

IEEE standards

IEEE P7003: Algorithmic Bias Considerations, available at

https://standards.ieee.org/project/7003.html.

IEEE P7001: Transparency of Autonomous Systems, available at https://standards.ieee.org/project/7001.html.

IEEE P7000: Draft Model Process for Addressing Ethical Concerns During System Design, available at https://standards.ieee.org/project/7000.html.

IEEE P7009: Standard for fail-safe design of autonomous and semi-autonomous systems, available at https://standards.ieee.org/project/7009.html.

IEEE P2863: Recommended Practice for Organizational Governance of Artificial Intelligence, available at https://standards.ieee.org/project/2863.html.

IEEE 7010: Recommended Practice for assessing the impact of autonomous and intelligent systems on human well-being, available at https://standards.ieee.org/standard/7010-2020.html.

ITU standards

ITU-T Y.3531: Cloud computing: functional requirements for Machine Learning as a service, available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14484.

ITU-T Y. 4470: Reference architecture of Artificial Intelligence service exposure for smart sustainable cities, available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14503.

Y.Suppl.63 to ITU-T Y.4000 series: Unlocking the Internet of Things with Artificial Intelligence: Where we are and where we could be, available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14103.