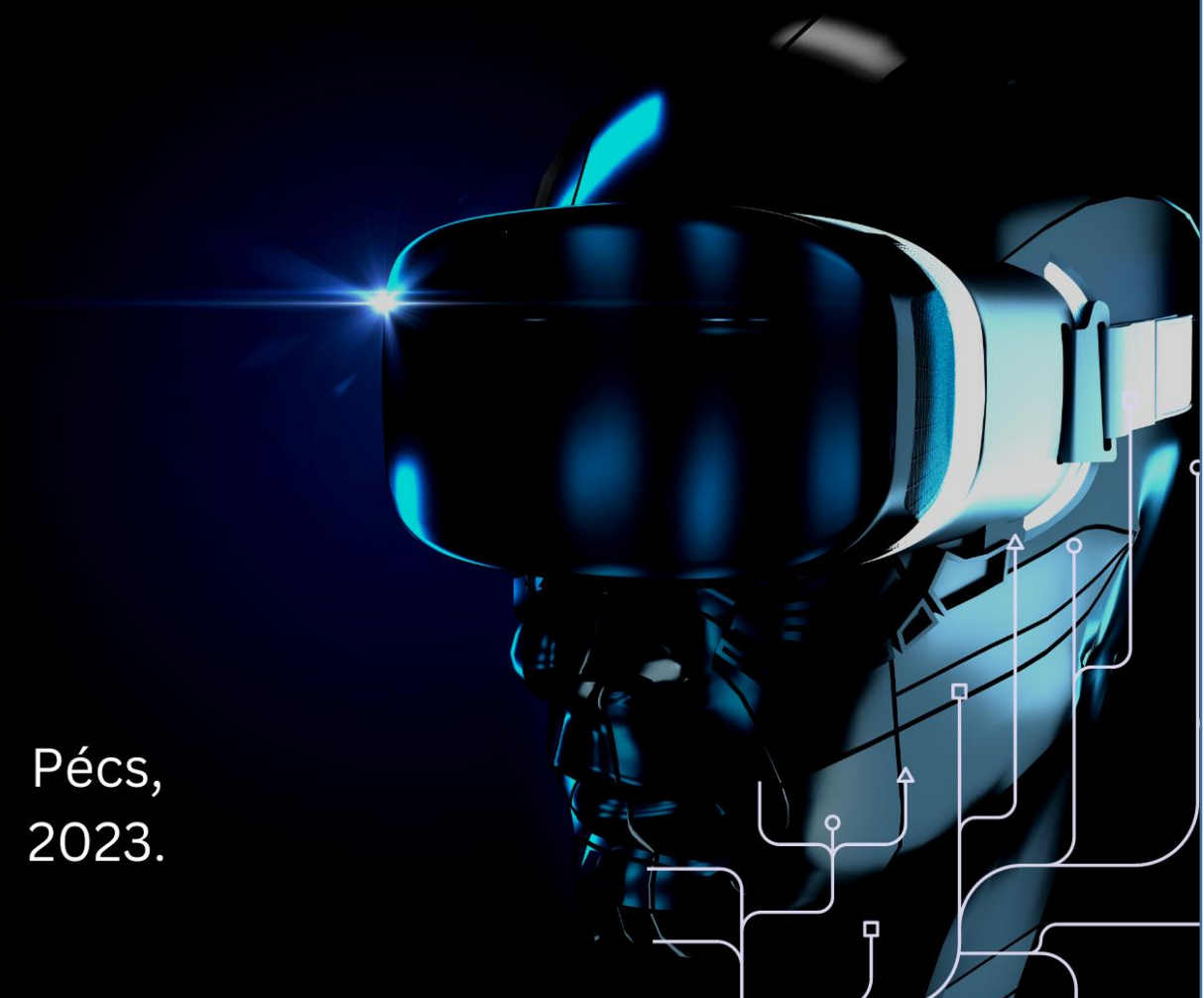
BIZTONSÁG A KIBERTÉRBEN

KONFERENCIAKÖTET

PTE-ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék



Pécs,
2023.

Biztonság a kibertérben
Konferenciakötet

Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék
Pécs, 2023.

Biztonság a kibertérben
Konferenciakötet

Szerkesztette:

Takács Ildikó
Tóth Dávid

Kiadja: Pécsi Tudományegyetem Állam- és Jogtudományi Kar,
Kriminológiai és Büntetés-végrehajtási Jogi Tanszéke
7622 Pécs, 48-as tér 1.
Felelős Kiadó: Prof. Dr. Fábián Adrián dékán

ISBN: 978-963-626-125-2

Tartalomjegyzék / Table of content

Balázs Gáti* –The Effects of Economic Crisis on Personal Data Protection and its Criminal Law Aspects

1. Introduction

The world has once again been confronted with the concept of crisis since the beginning of the 2020s. [1] However, we're not primarily thinking of major historical economic crises, such as the 1929-1933 Great Depression or the 2008 global financial and capital market crisis. The COVID-19 pandemic, which started in Wuhan, Central China in December 2019, has led to a socio-economic crisis, with restrictions imposed to control the pandemic, changes in everyday life, and the transformation of the digital environment becoming part of our daily lives. The forced digitization can be attributed as a consequence of the defense against the pandemic, with the Internet of Things (IoT, IoMT) and blockchain technologies coming to the forefront in many areas of medical science. The transformation of the digital environment and the higher number of users significantly increased the number of potential victims in cyberspace. Correspondingly, modes of committing crimes have changed, increasing the frequency of cybercrime. [2] The number of legal violations committed in cyberspace has multiplied, with computer crime, including malware, identity theft[3], financial and other online frauds, coming to the fore and putting the security of organizations' and individuals' data at risk. In cybercrimes, the data are the primary targets for the perpetrators. [4,5] Numerous Hungarian

* PhD hallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

[1] KŐHALMI, László: A biztonság bűvöletében In: Barabás, Andrea Tünde; Christián, László (szerk.) Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére : Navigare necesse est ,Budapest, Magyarország : Ludovika Egyetemi Kiadó (2021) p.530 pp. 309-318.

[2] GÁTI, Balázs: A kiberbűnözés jellegzetességei és a COVID-19 járvány kapcsolata a statisztikák tükrében. In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Rendészet a rendkívüli helyzetekben: húsz éves a Szent László napi konferencia. Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2021. p. 111-120. , p. 115.

[3] TÓTH, Dávid: Személyiséglopás az interneten. = Büntetőjogi Szemle 2020/9, p. 113-119., p. 119.

[4] MARAS, Marie-Helen: Cybercriminology. Oxford, Oxford University Press, 2016.

[5] FENYVESI, Csaba: Future Developments and Challenges in Criminalistics as Part of Criminal Justice. = Journal of Eastern-European Criminal Law 2019/6.2, pp. 72-85., p. 80.

publications have also been written about the legal consequences of the pandemic and the economic crisis. [6,7,8,9,10]

The European Parliament, the Council of the European Union, and the European Commission have developed a political and legislative agenda for the legislative cycle lasting until 2024, emphasizing the damages caused by the COVID-19 pandemic. [11]

Even before overcoming the impacts of the COVID-19 pandemic, a new crisis is looming: Russia's war against Ukraine is having a significant impact on energy and food markets within the Union. [12]

Recession is fundamentally an economic concept, a part of the business cycle characterized by a decline in economic activity. According to the most widely used definition, it refers to a decrease (or in other common terms, negative growth) in Gross Domestic Product (GDP) for at least two consecutive quarters compared to the previous quarter. In terms of economics, the triggers are:

1. Financial imbalances: Excessive debt accumulation, asset bubbles, and other financial imbalances can cause instability in the economy, which may result in a crisis.
2. Speculation and market bubbles: In some cases, speculation and market bubbles can lead to short-term growth, but eventually result in a crash. [13]

In general, alongside economic factors, crises can be intensified, even provoked, by wars, pandemics, natural disasters – the latter exemplified

---

[6] AMBRUS. István: A Covid-19-világjárvány hatásai. In: Ambrus, István (szerk.) Magyarázat a compliance jogszabályairól I.: Általános és büntetőjogi compliance. Budapest, Wolters Kluwer Hungary, 2021. p. 435-443., 440.

[7] WINDT. Szandra: A világjárvány hatása az emberkereskedelemre az első két év tapasztalatai alapján. = Belügyi Szemle: A Belügyminisztérium Szakmai Tudományos Folyóirata 2022/70.2, p. 327-344., p. 344.

[8] GÁL, László István: The Possible Impact of the COVID-19 On Crime Rates in Hungary. = Journal of Eastern-European Criminal Law 2020/7:1, p. 165-177., p. 167.

[9] Társadalomtudományi Kutatóközpont Jogtudományi Intézet: Kéziratvita: Jogi diagnózisok: a COVID-19 világjárvány hatásai a jogrendszerre II. kötet. https://jog.tk.hu/esemeny/2021/11/covid-19-vilagjarvany-hatasai-a-jogrendszerre-ii-kotet, 2021. https://jog.tk.hu/esemeny/2021/11/covid-19-vilagjarvany-hatasai-a-jogrendszerre-ii-kotet, Accessed: May 24, 2023.

[10] DORNFELD, László: A koronavírus-járvány hatása a kiberbűnözésre. = In Medias Res: Folyóirat a sajtószabadságról és a médiaszabályozásról 2020/9:2, p. 193-204., 198.

[11] Az Európai Parlament, az Európai Unió Tanácsa és az Európai Bizottság: Együttes következtetések a 2020–2024-es időszak szakpolitikai célkitűzéseiről és prioritásairól (2021/C 451 I/02).

[12] Az Európai Unió Tanácsa: Oroszország Ukrajna elleni inváziójának hatása a piacokra: uniós válaszlépések. https://www.consilium.europa.eu/hu/policies/eu-response-ukraine-invasion/impact-of-russia-s-invasion-of-ukraine-on-the-markets-eu-response/. Accessed: May 24, 2023

[13] Gazdasági recesszió. https://hu.economy-pedia.com/11039627-economic-recession. Accessed: May 24, 2023.

by the 2008 crisis, which is associated with the hurricane in New Orleans. [14]

In relation to interdisciplinary and comparative legal analysis, primarily economic, financial, constitutional, and civil law analyses were produced following the 2008 crisis. [15]

Generally speaking, the legal challenges of a recession can be associated with the increase in business costs and issues related to the application of law. The former generally affects the business world and companies, making it harder for businesses to fulfill their financial obligations, including legal costs. The issues related to the application of law involve, on one hand, the increased criminal activity generated by the recession and the consequent tasks associated partly with prevention and resolution, as well as financial questions. On the other hand, I would highlight that, within the application of law, criminal law often comes to the forefront in protecting individuals and society.[16]

The study analyzes the data protection aspects of the altered economic situation due to the recession, also considering its relation to criminal law.

2. Challenges Related to Data Protection and Data Security During the COVID-19 Pandemic

One typical crisis situation in the recent past is the COVID-19 pandemic that started in Central China in 2019. The data protection and data security challenges experienced during its socio-economic crisis, as well as its impact on crime, could resemble and potentially foreshadow the effects of the current crisis, given that the socio-economic structure of the 21st century is essentially the same, just like the prevailing legislative environment.

The data protection package adopted in May 2016, the Regulation (EU) 2016/679[17] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the Directive (EU)

[14] GÁL, István László: A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre. = Magyar Jog 2020/67:5, pp. 257-265., p. 260.

[15] AUER, Ádám; Papp, Tekla (szerk.): A gazdasági világválság hatása egyes jogintézményekre Magyarországon és az Európai Unióban: Interdiszciplináris és jogösszehasonlító elemzés. Budapest, Nemzeti Közszolgálati Egyetem (NKE), 2016. p. 272.

[16] RIPSZÁM, Dóra, GÁL László István: Gondolatok a járványügyi védekezés akadályozásáról. = Büntetőjogi Szemle 2022/11:2, pp. 53-56., p. 54.

[17] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT–vonatkozású szöveg) HL L 119., 2016.5.4., pp. 1-88.

2016/680[18] 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, both serve the free flow of data for the protection of natural persons by competent authorities. These were later joined by Regulation (EU) 2018/1725 (EUDPR) [19], 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.

Both Regulation (EU) 2016/679 (General Data Protection Regulation, hereafter GDPR) and Directive (EU) 2016/680, the so-called "Law Enforcement Directive" (hereafter LED), as well as Regulation (EU) 2018/1725 (European Union Data Protection Regulation, hereafter EUDPR) have the goal of preparing EU countries for the digital age, while also formulating general rules for the conditions of automated data processing, including, for instance, rules regarding the use of artificial intelligence. In a broader sense, the Regulation on Privacy and Electronic Communications (ePrivacy Regulation) [20,21] can also be classified under the topic of data protection.

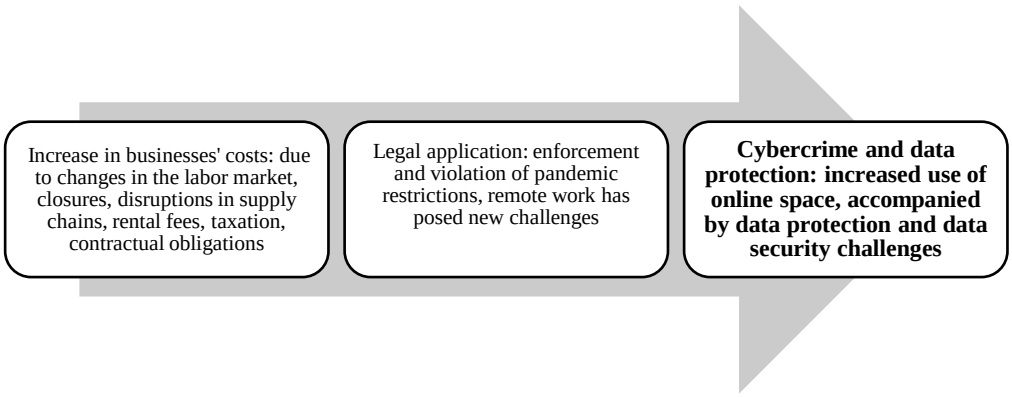
Figure 1 summarizes the outstanding economic and legal impacts of the COVID-19 pandemic.

[18] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről. HL L 119., 2016.5.4., pp. 89-131.

[19]Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (EGT–vonatkozású szöveg.) HL L 295., 2018.11.21., pp. 39-98.

[20] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) HL L 201., 2002.7.31., 37—47. o

[21]GÁTI, Balázs: Az adatvédelmi jog fejlődésének főbb állomásai. = Studia Iurisprudentiae Doctorandorum Miskolciensium–Miskolci Doktoranduszok Jogtudományi Tanulmányai 2022, pp. 153-168



The specific impacts resulting from pandemic restrictions may not generally apply to economic recessions, but the increase in crime statistics can generally be observed during times of economic crises. [22]

[22] GÁL, László István: The Relationship between Economic Crises and Criminality from the 18th Century to Today. = JOURNAL ON EUROPEAN HISTORY OF LAW 2020/11, pp. 138-144.

Figure 2 shows some aggregated data of VARONIS COVID-19 specific cyber security statistics. [23]

Since the beginning of the epidemic, the FBI has reported a 300% increase in reported cybercrimes.	In April 2020, Google blocked 18 million COVID-19-related malware and phishing emails per day. (Google)	Half a million Zoom user accounts were compromised or sold on a dark web forum in April 2020. (CPO Magazine)
27% of cyber-attacks related to COVID-19 target banks or healthcare organizations. In relation to the year 2020, a 238% increase in cyber attacks against banks is attributed to COVID-19. (Fintech News)	52% of legal and compliance executives are concerned about third-party cyber risks from remote work since COVID-19. (Gartner)	Cloud-based cyber-attacks increased by 630% between January and April 2020. (Fintech News)
In 2020, the number of confirmed data breaches in the healthcare industry increased by 58%. (Verizon)	Telecommuting increased the average cost of data protection incidents by §137,000 (IBM)	People working remotely caused a security breach in 20% of organizations. (Malwarebytes)
In May 2020, 33,000 unemployed applicants of the Epidemic Unemployment Assistance Program were exposed to the possible consequences of data security breaches. (NBC)	47% of employees cited distraction as a reason for falling victim to phishing scams while working from home. (Tessian)	

[23] Varonis: Cybersecurity Statistics.: https://www.varonis.com/blog/cybersecurity-statistics/ idézi: Gáti Balázs, A kiberbűnözés jellegzetességei és a Covid-19 járvány kapcsolata a statisztikák tükrében, p. 115

US citizens have lost more than $97.39 million due to COVID-19 and stimulus check scams. (Atlasvpn)	81% of Cyber Security Professionals Report Their Job Role Has Changed During the Pandemic (ISC)	

In this summary, the 300% increase in computer crime reported by the FBI is particularly notable. In April 2020, Google blocked 18 million malware programs and phishing emails related to COVID-19 daily. In addition, the impact on the banking sector and the healthcare industry is clearly visible, as is the increase in the number of data protection incidents and the large number of attacks against commonly used internet communication platforms - in this table, against Zoom.

Domestic data also indicated an increase in cybercrime. According to data from the Electronic Crime Record (EBNY), the number of online scams in Hungary increased by 32% in 2020 compared to the previous year. [24] According to a survey conducted by the Association of IT Businesses (IVSZ) in 2020, 31% of Hungarian businesses were affected by phishing attacks, and the number of data thefts also increased. According to the National Police Headquarters (ORFK), there were a total of 2696 phishing attacks in Hungary in 2020, which is 36% more than the previous year. [25] According to data from Magyar Telekom, the number of computer viruses and malicious software in Hungary increased by 25% in 2020 due to the COVID-19 pandemic. [26] Data from the National Cybersecurity Institute show that there were a significant number of events in March-April 2020, followed by a decrease in the number of events with smaller periodic changes. [27]

In the current economic crisis, a decrease in cybercrime statistics is not expected compared to the pandemic. According to the 2022 KPMG report on technology maturity and corporate uncertainty: "From the Russian invasion of Ukraine to the general COVID-19 disruptions, widespread economic uncertainty, volatility - and thus cyber risk and uncertainty - has increased

[24] BSR: Dokumentum.https://bsr.bm.hu/Document#, Accessed: May 25, 2023.

[25] MABISZ: Kiberbűnözés Magyarországon: már a rendőrségi statisztikákban is kimutatható a dinamikus növekedés. 2020. https://mabisz.hu/szemle/?p=49132, Accessed:May 25, 2023.

[26]Magyar Telekom: Fenntarthatósági Jelentés 2022. [online] URL: https://www.telekom.hu/static-tr/sw/file/MagyarTelekom_FenntarthatosagiJelentes2022_07Erdekelt-feleink.pdf , Accessed: May 25, 2023.

[27] PALICZ, Tamás, Bencsik Balázs, Szócska Miklós: Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai. = SCIENTIA ET SECURITAS 2021/2, pp. 78-87.

globally." [28] According to the World Economic Forum's 2023 global cybersecurity outlook, 93% of cybersecurity leaders and 86% of business leaders consider it "moderately likely" or "very likely" that global geopolitical instability will lead to a far-reaching, catastrophic cyber event in the next two years. [29]

3. Expected increase in cybercrime and digitalization

Every day, roughly one million more people connect to the internet. [30] According to the World Economic Forum, in 2022, 6 billion people will connect to the internet, up from 5 billion in 2020, and by 2030, there will be more than 7.5 billion internet users.

According to a report from CISCO, by 2023, there will be three times more networked devices on Earth than humans. [31] By 2022, 1 trillion networked sensors will be embedded in our surrounding world, and within 20 years, this number could reach up to 45 trillion. [32]

Cybersecurity Ventures predicts that by 2025, the world will store 200 zettabytes of data. This includes data stored on private and public IT infrastructures, utility infrastructures, private and public cloud-based data centers, personal computers – including PCs, laptops, tablets, and smartphones – and IoT (Internet of Things) devices. [33]

Forecasts suggest that by 2025, the total volume of data stored in the cloud – which includes public clouds operated by providers and social media companies (such as Apple, Facebook, Google, Microsoft, Twitter, etc.), government-owned clouds that are accessible to citizens and businesses,

---

[28]KPMG: World economy navigates potential crises. https://kpmg.com/xx/en/home/insights/2022/11/world-economy-navigates-potential-crises.html, Accessed: May 25, 2023.

[29]World Economic Forum, Global Risks Report 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf, Accessed: May 25, 2023.

[30] World Economic Forum: The Global Risks Report. 2020.

[31] CISCO: New Cisco Annual Internet Report Forecasts 5G to Support More Than 10% of Global Mobile Connections by 2023. 2020. [online] URL: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2020/m02/new-cisco-annual-internet-report-forecasts-5g-to-support-more-than-10-of-global-mobile-connections-by-2023.htm Accessed: May 25, 2023.

[32] CISCO: Enterprises Are Leading The Internet of Things Innovation. 2017. [online] URL: https://www.huffpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_b_59a41fcee4b0a62d0987b0c6 Accessed: May 25, 2023.

[33] MORGAN, S.: Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. = Cybersecurity Ventures Cybercrime Magazine 2018. https://cybersecurityventures.com/annual-cybercrime-report-2019-to-2020/, Accessed: May 25, 2023.

private clouds owned by medium and large enterprises, and cloud-based storage services – will reach 100 zettabytes, representing 50% of the world's data at that time, compared to around 25% of data stored in the cloud in 2015.[34] Data is the cornerstone of the digital economy, and the role of data protection and cybersecurity has become increasingly important.

Cybersecurity Ventures predicts a 12-15% annual growth in the cybersecurity market by 2025. While this could be a substantial growth, it pales in comparison to the costs associated with cybercrime. Over half of all cyberattacks are committed against small and medium enterprises (SMEs), and 60% of them cease to exist within six months of falling victim to a data breach or hacking incident. [35]

According to Mastercard, 66% of small and medium enterprises have experienced at least one cyber incident in the past two years. [36]

A survey by the Better Business Bureau found that for small businesses - which make up over 97% of all businesses in North America - a lack of resources or knowledge is a primary challenge for more than 55% when it comes to developing a cybersecurity plan. This illustrates the critical need for effective, affordable cybersecurity solutions and education for SMEs. [37]

4. Data protection and crisis

The recession amplifies the challenges of the digital age, as visible in reports by KPMG and the World Economic Forum. The background of privacy challenges is fundamentally found in changes determined by the digital age and the Fourth Industrial Revolution.

Cybercrime, with the spread of IT and networks, has become a global problem. The rate of cybercrime has significantly increased due to exponential technical development. The justice system cannot avoid these changes, so the justice system itself must face the challenges of the digital age. [38] However, the regulatory environment will always be at a disadvantage against the rapid development of emerging new technologies, as regulators first need to learn the practical operation and risks of the technologies to make appropriate rules.

---

[34]Cybersecurity Ventures Cybercrime Magazine ,2020

[35]Cybersecurity Ventures: 60 percent of small companies close within 6 months of being hacked. [online] URL: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/ Accessed: May 25, 2023.

[36] Mastercard Trust Center. [online] URL: https://www.mastercard.us/en-us/business/overview/safety-and-security/trust-center.html, Accessed: May 25, 2023

[37]BBB: SCAMS AND YOUR SMALL BUSINESS RESEARCH REPORT. [online] URL: https://www.bbb.org/content/dam/bbb-institute-(bbbi)/files-to-save/bbb_smallbizscamsreport-final-06-18.pdf

[38] MOLNÁR, Benedek: A jogi szolgáltatói szektor helyzete a koronavírus járványt megelőzően és a pandémia alatt. DOI: 10.55052/themis.2021.2.37.63, Accessed: May 25, 2023

The changes in the FinTech sector excellently illustrate the necessary changes in compliance, which carry the protection of personal data and data security challenges beyond business and ethical compliance, which have already intensified during the pandemic. According to Harkácsi and Szegfű, the recession further exacerbates all these, and in addition, "for proper data security design, it is essential that market players fully assess the data assets they manage, including various financial sector laws classified as secret data, business secrets, public but protectable data, and sensitive data that do not have legal regulations but can affect the proper operation, security, or even market situation of the institution." [39]

Cost reduction is a demand or necessity triggered by the crisis, which can apply to both actors in economic life and individuals. For economic actors, maintaining data protection measures may be cumbersome due to cost burdens, so cybercriminal activity may increase. For the same reason, the number of data protection incidents may also increase, and businesses may show reduced willingness to strengthen infrastructure. An example of this is that the United Kingdom has announced its plans to ease certain data protection requirements under the European Union's General Data Protection Regulation, which businesses welcomed but data protection groups criticized.

The regulations introduced last summer, which resulted in cost savings by reducing compliance burdens for British companies, were reviewed following consultation with businesses and data protection stakeholders - the Ministry of Science, Innovation and Technology reported. [40]

While this solution may be cost-effective, its consequences can cause greater damage to businesses. One-third of organizations[41] in the United Kingdom lose their customers after a data breach, and four out of ten customers say they won't return to a business after a security issue. [42] Businesses of any size and sector can become vulnerable to cyber-attacks and data leaks. However, a cost-effective data protection program allows organizations to build a culture of ongoing data protection compliance in the long term.

---

[39] HARKÁCSI, Gábor József – Szegfű László Péter: A megfelelőségbiztosítási funkció szerepe a digitalizáció, mesterséges intelligencia és robotizáció idején a pénzügyi szektorban. = Hitelintézeti Szemle, 2021/1, pp. 152–170.

[40] SOLON, Olivia: UK to Relax EU Data-Protection to Cut Business Costs. = Bloomberg.: https://www.bloomberg.com/news/articles/2023-03-09/uk-to-relax-eu-gdpr-data-protection-law-to-save-business-costs#xj4y7vzkg Accessed: May 25, 2023

[41] Redseal B2b Research, https://www.redseal.net/files/PDFs/RedSeal%20UK%20B2B%20Research%20SUMMARY_July2019.pdf, Accessed: May 25, 2023

[42] Businesswire: New Global Research Shows Poor Data Security Practices Have Serious Consequences for Businesses Worldwide. 2019. https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security, Accessed: May 25, 2023

Data protection and security are two areas that experts consider to be almost "recession-proof," as these two areas are just as important, if not more so, during a recession as they are under economically prosperous circumstances. During the 2008/9 recession, a survey covering the US, Europe, and the Asia-Pacific region found that 31% of organizations planned to increase their budget for external data protection assistance. Only 13% planned to reduce it. [43]

The average length of a recession is 13 months, based on an examination of the period from January 1913 to December 2007. [44] Similar to the time of a pandemic, such uncertainty can serve more as a catalyst for rethinking and innovation rather than cost-cutting. Forrester predicts that 80% of companies will shift their innovation spending from creativity to resilience, and overall, companies will "collect less data and pay more attention" when it comes to data protection. This means they need to examine what data a business has and what it's used for. This is not only one of the first steps in a data protection governance program but also an opportunity to discover business opportunities. [45]

Data protection is a real business necessity. At the 2022 World Economic Forum meeting, it was concluded that the recent stock market downturns are explained by the effects of COVID-19 and the war in Ukraine, but the main reason was data protection. Data protection has shown its ability to move markets, as many consumers are dissatisfied with the tracking of digital advertisements. Leaders need to step up for data protection and security and recognize that they can present risks and opportunities, similar to other global corporate issues. [46] The stakes will only get higher. Currently, globally, we generate 2.5 quintillion bytes of data daily (one quintillion is 1 followed by 18 zeros). [47]

Security issues related to data are significant in themselves. Last year, it was predicted that data breaches would cost the global economy $6.1 trillion. If

---

[43] IAPP: Privacy in a Recession. [online] URL: https://iapp.org/news/a/2009-02-privacy-in-a-recession/, Accessed: May 25, 2023

[44] NAGY, Attila: Tények és tévhitek a tőzsdéről, befektetésről. Budapest, Elemzésközpont.hu - Nemere-Print Kkt., 2020. p. 324

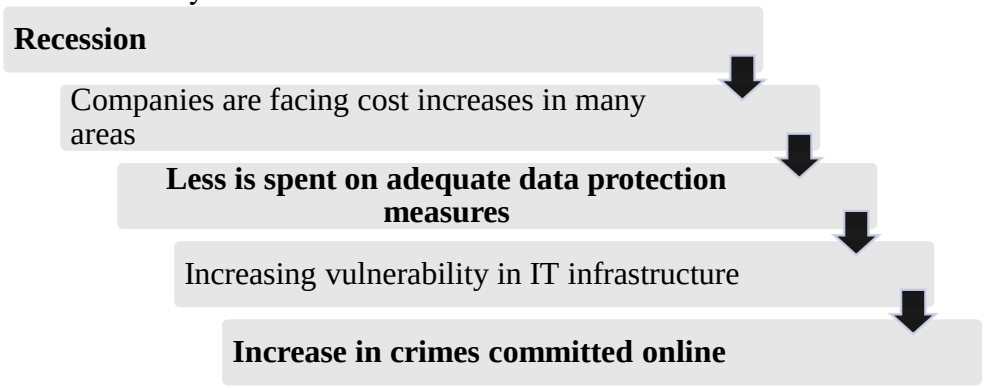
[45]What to Expect in 2023: IT Spending, Recession, Talent Crisis, Privacy, https://www.informationweek.com/strategic-cio/what-to-expect-in-2023-it-spending-recession-talent-crisis-privacy, idézi: EMMA SHEPPARD, Why a recession requires a value-based approach to privacy, https://www.privacycompliancehub.com/gdpr-resources/why-a-recession-requires-a-value-based-approach-to-privacy/ Accessed: May 25, 2023.

[46] SHEPPARD, Emma: Why a recession requires a value-based approach to privacy. 2022. https://www.privacycompliancehub.com/gdpr-resources/why-a-recession-requires-a-value-based-approach-to-privacy/, Accessed: May 25, 2023

[47] Marr, Bernard: How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. = Forbes.https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=35c1814860ba, Accessed: May 25, 2023

data breach were a country, it would be the third largest, behind the United States and China. [48] The pandemic has shown that every company is a data company, and problems appearing on the markets are not limited to the technology sector. The largest sector of digital services includes consumer goods, financial services, and healthcare. During a recession, while data protection can tighten stock prices, it can also be mentioned as a positive that it can increase them. The world's most profitable companies have made data protection a distinctive feature of their brand. The two technology companies that have made data protection and security a distinctive feature of their brand have upper market caps of $2.5 billion[49] and $2.055 trillion[50], respectively.

The survey conducted by the World Economic Forum ranked "cyberattacks on critical infrastructure" as the fifth most prominent global risk out of the current 15 global risks they listed. [51]
In figure 3, I present a possible mechanism of the relationship between recession and cybercrimes.



Recession, which is a fundamental part of economic life, holds special significance from a data protection perspective. It reinforces the protection of data assets against cyberattacks, strengthens the trust developed towards companies, thus aiding their survival and continuity.

---

[48] Cybercrime Magazine: Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [online] URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[49]Yahoo Finance: AAPL - Apple Inc. https://finance.yahoo.com/quote/AAPL?p=AAPL&.tsrc=fin-srch, idézi Dominique Shelton, How attention to data privacy will stabilize our financial markets, https://europeansting.com/2022/06/01/how-attention-to-data-privacy-will-stabilize-our-financial-markets/ Accessed: May 24, 2023.

[50]Yahoo Finance: MSFT - Microsoft Corporation. https://finance.yahoo.com/quote/MSFT%3B/, idézi Dominique Shelton, How attention to data privacy will stabilize our financial markets, https://europeansting.com/2022/06/01/how-attention-to-data-privacy-will-stabilize-our-financial-markets/ Accessed: May 24, 2023.

[51] VMF.2023

5. Actions to be Taken – Prevention – Data Protection Consciousness

Cybersecurity is in a state of flux, and data holds more importance than ever before. Given these circumstances, corporations must henceforth bolster their safeguards in areas that are pivotal from a security perspective. As organizations undergo digital transformations, the budget must also keep pace with this process by making investments towards cybersecurity and data protection. Increasingly, these areas should be perceived as intrinsic parts of strategic objectives and incorporated into initiatives to foster trust amongst stakeholders. The concept of "digital trust" has surfaced in this context. [52]

In this digitized world we inhabit, every facet of business hinges on the fairness, integrity, and transparency of information collection and processing. Systems must exhibit flexibility and reliability, with the capacity to swiftly respond to disruptions. During transactions involving an organization, digital trust becomes of utmost importance not just to partners, investors, and regulatory authorities, but also to every constituent of the broader ecosystem enveloping all organizations. [53]

Cybersecurity and data protection play key roles in establishing and maintaining this trust. Businesses ramp up data collection, extend the use of artificial intelligence (AI) and machine learning (ML) technologies, and adopt the environmental, social, and governance (ESG) agenda, all while confronting increasingly stringent regulatory standards.

In our current digitized world, every facet of business depends on the fairness, integrity, and transparency of information collection and processing. Systems must be flexible and reliable, and capable of swiftly responding to disruptions. In the KPMG - Cyber Trust Insights 2022 research, KPMG International surveyed 1881 leaders and conducted discussions with corporate executives and professionals from around the world to uncover how much the C-suite recognizes this, and how they respond to the challenge and what they need to do next. It also reveals the crucial role that Chief Information Security Officers (CISO) can play in assisting them and identifies five key steps in building trust through cybersecurity and data protection. [54] Over 80 percent of respondents recognized the need to improve cybersecurity and data protection, including

---

[52] It has been used in this context since 2017. Tufts University's Fletcher School and Mastercard have launched a research initiative to study the state of digital trust in 42 countries. CHAKRAVORTI, BHASKAR; Bhalla, AJAY; Chaturvedi, RAVI Shankar: The 4 Dimensions of Digital Trust, Charted Across 42 Countries. = Harvard Business Review.: https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries Accessed: May 25, 2023 ,

[53] KPMG: Cyber Trust Insights 2022.https://assets.kpmg.com/content/dam/Tóth /xx/pdf/2022/10/kpmg-cyber-trust-insights-2022.pdf, Accessed: May 26, 2023

[54] KPMG, KPMG Cyber Trust Insights 2022.

increased transparency in data usage, and 51 percent deemed the protection of IT resources against attacks to be extremely important.
The five important steps to build trust through cybersecurity and data protection are:

- Emphasize cybersecurity and data protection.
- Integrate cybersecurity and data protection into business processes, governance, and organizational culture - i.e., they should be integral parts of corporate life.
- Rethinking the role of the CISO (Chief Information Security Officer) - acknowledging the potential for wide-ranging contributions, from ESG (Environment, Social, Governance) standards to AI ethics.
- Identify and collaborate with key partners within the organization's ecosystem to improve trust and resilience.
- Develop internal collaboration networks to strengthen trust.

During the 2022 Cyber Trust Insights survey, more than a third of respondents, 38%, believed that their data protection concerns hinder the formation of external cybersecurity collaborations. Additionally, 36% fear that their security protocols may be endangered by excessive exposure. Further obstacles are regulatory restrictions, a lack of support at the top executive level, and a lack of necessary resources.
According to the KPMG report, CISOs currently play a crucial role. "45% of C-suite respondents consider the CISO as a key leader, and the profile of the CISO role has rapidly increased over the past five years due to digital transformation, the growth of cybercrime, and increasing regulatory expectations." [55] According to the 2023 British DP Index report[56], data protection awareness, which is also reflected in the corporate budget, is present among DPOs in the United Kingdom at a rate of 30%.[57]
In response to the question, "Do you expect your organization's data protection budget to increase or decrease over the next 12 months?" posed since 2021, 57% of respondents predicted that their budget would remain the same, which is 8% more than in the previous quarter. 30% still expect an increase, and 13% expect a decrease. Data protection officers were more confident in their organization's data protection compliance. The DP Index's recommendation for cost efficiency during the current crisis is outsourcing.

---

[55] KPMG, KPMG Cyber trust insights 2022
[56] UK Data Protection Index. [online] URL: https://www.dpocentre.com/resources/uk-data-protection-index/ Accessed: May 26, 2023
In the UK since 2020, the DP Index has asked a quarterly panel of over 550 data protection officers (DPOs).
[57] DPO centre.com,https://www.dpocentre.com/the-dpindex-results-stability-in-uncertain-times/ , Accessed: May 26, 2023

Outsourcing is an extremely cost-effective way to support the organization's compliance requirements. It ensures that the organization continues to fulfill its data protection obligations, but without the cost of a full-time position. Outsourcing not only provides access to an experienced and competent data protection officer, but also, for instance, in the case of The DPO Centre, to one supported by one of the largest available teams of experts.

6. Summary

The study analyzes the interrelationships between data protection, data security, and economic crises in relation to associated criminal behavior. EU data protection laws, including the 2018 data protection package, were created in preparation for the digital age. Reviewing the history of data protection, it is clear that technological advancements have driven changes in data protection legislation from the OECD guidelines to the present day. The recent COVID-19 pandemic has generated a social and economic crisis. Although there are specific characteristics related to the pandemic, such as restrictive measures and, as a result, the increased role of the online space, the accelerated processes of digitalization have also changed the lives of actors in the economy. "In idem flumen bis non descendimus," says ancient philosophy, and this applies to technical changes as well; innovation continues to race ahead. Numerous scientific publications primarily reported a significant increase in the number of cybercrimes. The target of cyberattacks is data assets, which today can be measured in hundreds of zettabytes (one zettabyte is equivalent to one billion terabytes).
According to a PWC survey [58], "amid rising geopolitical tensions and consumer data protection concerns, 40% of business leaders see cybersecurity as the number one serious risk their companies face." Therefore, cybersecurity is a strategic factor in business life, and data protection and data security should also be considered as strategic factors. In uncertain economic environments, during times of crisis, the players in business life grapple with risks. However, those companies that build greater trust with stakeholders do not lose them. Recognizing this, leaders are making increasing investments in digital transformation, IT, cybersecurity/data protection, and customer experience according to the PWC survey. [59]

[58] PWC, PwC Pulse Survey: Managing business risks, https://www.pwc.com/us/en/library/pulse-survey/managing-business-risks.html, Accessed: May 26, 2023

[59] PWC, PwC Pulse Survey: Managing business risks. According to the PWC survey, the proportion of investments in digital transformation (53%), IT (52%), cyber security/data protection (49%) and customer experience (48%).

This can be considered a good practice in crisis management as well, i.e., data protection - and data security must become part of crisis management, as this can mitigate the negative effects of a crisis.

Bibliography

- **AMBRUS,** István: *A Covid-19-világjárvány hatásai*. In: AMBRUS István (szerk.): *Magyarázat a compliance jogszabályairól I.: Általános és büntetőjogi compliance*. Wolters Kluwer Hungary, Budapest, 2021. pp. 435 – 443.
- **AUER,** Ádám – **PAPP** Tekla (szerk.): *A gazdasági világválság hatása egyes jogintézményekre Magyarországon és az Európai Unióban: Interdiszciplináris és jogösszehasonlító elemzés*. Nemzeti Közszolgálati Egyetem (NKE), Budapest, 2016. p. 272.
- **CHAKRAVORTI**, Bhaskar; **BHALLA**, Ajay; **CHATURVEDI**, Ravi Shankar: The 4 Dimensions of Digital Trust, Charted Across 42 Countries. HARVARD BUSINESS REVIEW. https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries
- **FENYVESI,** Csaba: *Future Developments and Challenges in Criminalistics as Part of Criminal Justice*. JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 2019/6.2. pp. 72 – 85.
- **DORNFELD,** László: A *koronavírus-járvány hatása a kiberbűnözésre*. IN MEDIAS RES: FOLYÓIRAT A SAJTÓSZABADSÁGRÓL ÉS A MÉDIASZABÁLYOZÁSRÓL 2020/9:2. pp. 193 – 204.
- **GÁL,** László István: *A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre*. MAGYAR JOG 2020/67:5. pp. 257 – 265.
- **GÁL,** László István: *The Relationship between Economic Crises and Criminality from the 18th Century to Today*. JOURNAL ON EUROPEAN HISTORY OF LAW 2020/11. pp. 138 – 144.
- **GÁL,** László István: *The Possible Impact of the COVID-19 On Crime Rates in Hungary*. JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 2020/7:1. pp. 165 – 177.
- **GÁTI,** Balázs: *A kiberbűnözés jellegzetességei és a COVID-19 járvány kapcsolata a statisztikák tükrében*. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.) Rendészet a rendkívüli helyzetekben: húsz éves a Szent László napi konferencia. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2021. pp. 111 – 120.
- **GÁTI,** Balázs: *Az adatvédelmi jog fejlődésének főbb állomásai*. STUDIA IURISPRUDENTIAE DOCTORANDORUM MISKOLCIENSIUM – Miskolci Doktoranduszok Jogtudományi Tanulmányai 2022. pp. 153 – 168.

- **HARKÁCSI,** Gábor József – **SZEGFŰ** László Péter: *A megfelelőségbiztosítási funkció szerepe a digitalizáció, mesterséges intelligencia és robotizáció idején a pénzügyi szektorban*. HITELINTÉZETI SZEMLE, 2021/1. pp. 152 – 170.
- **KŐHALMI,** László: *A biztonság bűvöletében* In: BARABÁS Andrea Tünde – CHRISTIÁN László (szerk.) Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est. Ludovika Egyetemi Kiadó, Budapest, 2021. pp. 309 – 318.
- **MARAS,** Marie-Helen: *Cybercriminology*. Oxford University Press, Oxford, 2016.
- **MARR,** Bernard: *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read.* Forbes. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/
- **MOLNÁR,** Benedek: *A jogi szolgáltatói szektor helyzete a koronavírus járványt megelőzően és a pandémia alatt.* DOI: 10.55052/themis.2021.2.37.63
- **MORGAN**, S.: *Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021*. CYBERSECURITY VENTURES CYBERCRIME MAGAZINE 2018. https://cybersecurityventures.com/annual-cybercrime-report-2019-to-2020/
- **NAGY,** Attila: *Tények és tévhitek a tőzsdéről, befektetésről*. Elemzésközpont.hu - Nemere-Print Kkt., Budapest, 2020., 324.o.
- **PALICZ,** Tamás – **BENCSIK** Balázs – **SZÓCSKA** Miklós: *Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai*. SCIENTIA ET SECURITAS 2021/2. pp. 78 – 87.
- **RIPSZÁM,** Dóra – **GÁL,** László István: *Gondolatok a járványügyi védekezés akadályozásáról*. BÜNTETŐJOGI SZEMLE 2022/11:2. pp. 53 – 56.
- **SHEPPARD,** Emma: *Why a recession requires a value-based approach to privacy.* 2022. https://www.privacycompliancehub.com/gdpr-resources/why-a-recession-requires-a-value-based-approach-to-privacy/
- **SOLON,** Olivia: *UK to Relax EU Data-Protection to Cut Business Costs. Bloomberg.* https://www.bloomberg.com/news/articles/2023-03-09/uk-to-relax-eu-gdpr-data-protection-law-to-save-business-costs
- **TÓTH,** Dávid: *Személyiséglopás az interneten.* BÜNTETŐJOGI SZEMLE 2020/9. pp. 113 – 119.
- **WINDT,** Szandra: *A világjárvány hatása az emberkereskedelemre az első két év tapasztalatai alapján*. BELÜGYI SZEMLE: A

Belügyminisztérium Szakmai Tudományos Folyóirata 2022/70.2. pp. 327 – 344.

Kőhalmi László* – Variációk a biztonságra

1.A biztonság fogalmáról

A biztonság fogalmának szabatos meghatározása rendkívül nehéz feladat, hiszen „a biztonságnak a lehetséges vagy valóságos alanyok, az érintett tárgyak és a tényleges tartalom szerint szinte felsorolhatatlanul sokféle változata képzelhető el" – állapította meg korunk egyik legismertebb hazai teoretikusa, ÁDÁM Antal professzor.[1] Véleménye szerint általánosságban elmondható, hogy a biztonság annak hiányával áll **korrelatív** viszonyban. „A biztonság hiánya pedig fenyegetést, veszélyt, ártalmat, károsodást, hátrányt jelent és félelemmel, szenvedéssel jár. A biztonság tehát a fenyegetések, veszélyek és ártalmak hiányát, illetve az azokkal szembeni hatékony védettséget, oltalmat jelenti."[2]
A biztonságnak – vagy annak hiányának – bármely élőlény lehet a részese, de annak antropológiai megközelítésben alapvetően az emberközpontú hatásai érdekesek konferenciánk témája szempontjából.
A biztonság történelmi, földrajzi megközelítésben rendkívül változatos képet mutat, sőt eltérő lehet annak világnézeti, műszaki, művészeti stb. megközelítése.
ÁDÁM Antal szerint a biztonság megítélésében az állam szempontjából jelentős változást hozott a nemzetállamok kialakulása, mivel ekkor „lépett előtérbe az állambiztonság, a nemzetbiztonság és a közbiztonság jelentősége és állami garantálása".[3]
A biztonság fenntartására irányuló erőfeszítésekre azonban – véleményem szerint – erősen rávetül annak erőszakos eszközökkel történő garantálása. Ma ugyan már túl vagyunk a hidegháborúnak nevezett történelmi időkön, de sajnos a világon számtalan helyen jelenleg is háború folyik.
Nincs már bipolárisnak nevezett szembenállás, de van helyette terrorizmus, emberkereskedelem és sok-sok aljas emberi megnyilvánulás.
Miközben a terror ellen hirdetnek háborút a világ katonai nagyhatalmai, addig számtalan a demokráciával nehezen összeegyeztethető „megelőző" intézkedésként aposztrofált szörnyű pusztításokat fogadtatnak el a közvéleménnyel a hatalom birtokosai.

---

* Pécsi Tudományegyetem Állam-és Jogtudományi Kar Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, egyetemi tanár
[1] ÁDÁM Antal: A jogi alapértékek harmóniája és versengése. Polgári Szemle 2006/7-8.sz.
[2] ÁDÁM (2006) i.m.
[3] ÁDÁM Antal: A biztonság mint jogi érték. In: Tanulmánykötet Erdősy Emil professzor 80. születésnapja tiszteletére (szerk: Balogh Ágnes – Hornyák Szabolcs). Studia Iuridica Auctoritate Universitatis Pécs Publicata 136. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2005. 13.o.

Egy új világrend kialakulásának lehetünk szemtanúi, s ebben az útkeresésben „egyre inkább előtérbe került az embert és az emberi közösségeket fenyegető valamennyi hagyományos és újszerű veszélyt figyelembe vevő, összetett biztonságfogalom kimunkálása és alkalmazása."[4]
Az ENSZ keretében 1994-ben a „Redefining Security: The Human Dimension" c. jelentéshez alapmunkaként szolgál az ún. **humán biztonság** tartalmi összetevőinek meghatározása, melynek igénye „lehetővé és egyben szükségessé teszi, hogy holisztikus szemlélettel az embert és az emberi közösségeket fenyegető valamennyi veszélyt és ártalmat figyelembe vegyük és ezeket **interdependensen**, tehát kölcsönös összefüggéseikben kezeljük."[5]
ÁDÁM professzor mellőzhetetlennek tartja „az emberi méltóság kiemelt szolgálatát, a kivetettek, a hátrányos helyzetűek, a testi és szellemi fogyatékosok előnyösen megkülönböztetett védelmét, az éhínség, a szegénység, a munkanélküliség, a tiltott diszkrimináció elleni küzdelmet, a fertőző és gyógyíthatatlan emberi, állati és növényi betegségek, a szenvedélybetegségek, a természeti és műszaki katasztrófák, a természet-, illetve környezetkárosodások, a megrázó közlekedési akcidenciák, a szervezett és egyéb bűnözés, a terrorizmus, valamint a bizonyos okok miatt, vagy események kapcsán felbőszült tömeg vandál pusztítása elleni lokális, regionális, állami, államközi és globális, de minden esetben összehangolt fellépést. Sokan jutottak már el az embert, az emberi közösségeket, a jelenlegi és jövő generációkat fenyegető súlyos veszélyek ismeretében arra a felismerésre, hogy a kimerítően fel nem sorolt problémákkal szemben eredményes küzdelmet egyedül és elkülönítetten sem az egyén, sem a társadalmi közösségek, sem az állam, sem az államok tömörülése nem folytathat. A jelzett veszélyekkel szemben az összehangolt, együttes küzdelem folytatása korparancs. Ennek a küzdelemnek természetesen szerves része a veszélyt, a károsodást kiváltó körülmények, az előidéző okok feltárása, a megelőzési feltételek körültekintő építése, a hatékony védelmet szolgáló, korszerű műszaki eszközöket alkalmazó, folytonos monitoring szolgálat alkalmazása, az összehangolt védelmi erőfeszítések kifejtése és a mégis bekövetkezett járványok, kataklizmák, katasztrófák, balesetek vagy más károsodások megszüntetése, valamint az olyan helyreállító aktivitás, amely a tapasztalatok hasznosításával az újabb veszélyek vagy ártalmak elleni elhárító mechanizmusok gyarapítását is magában foglalja."[6]
A **human security** – szintén ÁDÁM Antalt hivatkozva – elvileg tehát „korszakunk valamennyi veszélyétől és ártalmától való mentességet jelenti. Mivel azonban ilyen tartalmú biztonság sajnos elérhetetlen, az emberközpontú biztonság rendkívül kiterjedt, összetett követelményrendszert, megelőző,

[4] ÁDÁM (2005) i.m. 14.o.
[5] ÁDÁM Antal: A biztonság az értékek között. Jura 2005/1., 34.o.
[6] ÁDÁM i.m. 34.o.

védekező, oltalmat és rehabilitációt nyújtó, sokrétű erőfeszítést igényel. A humán biztonsághoz elválaszthatatlanul kapcsolódik a védelem, az ún. **human security defence** és a megelőzést, elhárítást, helyreállítást is magában foglaló oltalom, a **safety** elérése. A holisztikus szemlélet, a komplex és koordinált megelőzés és elhárítás követelménye nem zárja ki, hanem logikusan magában foglalja a veszélyek változatainak közelségéhez és súlyosságához ésszerűen igazodó, ezért elkerülhetetlenül változtatandó prioritások alkalmazását is."
ÁDÁM Antal fenti gondolait hallgatójaként, kollégájaként hallva, olvasva meglehetősen újszerű megközelítést jelentett számomra, így jelen előadásban professzor Úr szellemi örökségét is feleleveníteni szándékoztam.

2. Néhány teoretikus gondolat a biztonságról

A világ különböző országai, politikai rendszerei maguk döntik el, hogy milyen ráfordításokat hajlandóak eszközölni a biztonságért. Uwe VOLKMANN szerint két tényező: a biztonság és a szabadság bizonyos mértékig kölcsönösen függ egymástól, de ezek egymással konfliktusba is kerülhetnek. Egyrészt aki – mint a világ néhány rendkívül veszélyes megavárosában – már nem hagyja el a saját házát sötétedés után, mert fél, hogy megtámadják, ebből a szempontból nem szabad. Másrészt, akit az állam bezár a házukba vagy lakásukba egy veszélyes vírus terjedésének megakadályozása érdekében – mint Sanghaj lakosai a korona-pandémia lezárások idején –, az nem szabad, csakúgy mint akit azért börtönöztek be, mert megszegte a kijárási tilalmat. „A szabadságot tehát a **túl kevés** és a **túl sok biztonság** egyaránt veszélyeztetheti."[7]
A demokratikus rendszerekben folyamatosan újra kell tárgyalni a szabadság és a biztonság relációját. Minderre nincs recept, nincs előre kész **jogi fogatókönyv**, legfeljebb csak néhány nagyon általános **szabályozási kulcspont** határozható meg.
Egy jogállamban a biztonság-szabadság relációja folyamatosan **monitorizálandó**. „Úgy tűnik, hogy a **hangsúlyok** idővel eltolódtak, az utóbbi években, évtizedekben egyre határozottabban a **biztonság** garantálása irányába. Legutóbb a koronavírus-járvány elleni küzdelem megmutatta, mekkora szabadságot hajlandó feladni a társadalom annak érdekében, hogy megvédje magát a fontosabbnak tartott élet és egészség jogi érdekeit fenyegető veszélyektől."[8]
A modern állam létrejötte, illetve a később kialakuló jogállamiság – VOLKMANN szerint – egy-egy sajátos **biztonsági probléma** megoldásaként írható le: az állam jelenti a választ az embereket fenyegető veszélyekre.

[7] VOLKMANN, Uwe: Zwischen individueller Freiheit und staatlicher Sicherheitsgewähr – Wandlungen des Rechtsstaats in unsicheren Zeiten. APUZ 32-33/2022. 17.o.
[8] VOLKMANN i.m. 17 – 18.o.

Mindenkit ellenőrzés alatt tartó erő nélkül senki sem lehet biztonságban, sem az életében, sem a tulajdonában. Az állam megoldásnak tűnt a „mindenki háborúja mindenki ellen" problematikájára. Ennek akkor lehet véget vetni, ha az állam harmadik félként a versengő felek fölé emelkedik, és **erőszakkal** rákényszeríti őket a „békekötésre", azaz biztonságot[9] teremt.[10]
Idővel azonban az állam hatalma – véleményem szerint – túlzott méretűvé vált: a szuverenitás, a legitim fizikai erőszakmonopólium szinte korlátlan beavatkozást enged az emberek életébe, legyen szó szabadságról, tulajdonról vagy magánéletről. Mindez természetesen a biztonság ígéretének zászlaja alatt. A szabadság és a biztonság egyensúlyának megteremtése, és különösen a jogállamiság és a szabadság biztosításának összehangolása rendkívül ingoványos terület, különösen a **biztonsági oldalról** érezhető nyomásgyakorlás miatt.[11]
A biztonság fogalma folyamatosan bővül. Az éghajlatváltozás miatt a biztonság fogalma kiegészül egy **prospektív** dimenzióval, és utal egy olyan részben közelgő, részben jelen lévő veszélyek elleni védekezésre, amely részleteiben még természetesen bizonytalan, de összességében rendkívüli **fenyegetőnek** tűnik.
A – SZIKINGER Istvántól kölcsönzött kifejezést használva[12] – **biztonságiasítás** a digitális világ zűrzavarai elleni védekezést is felölei, más kérdés a küzdelem sikeressége. Ezzel a gondolati felvezetéssel el is érkeztünk konferenciák témaköréhez.

3. A kiberbiztonság

A biztonság fogalma, mint korábban megállapításra került **nem statikus** fogalom, s mindez különösen igaz a kiberbiztonságra, hiszen a fenyegetések, a szereplők, a technológiák, de a környezet paraméterei is folyamatosan változnak.[13]
Matthias SCHULZE szerint a biztonsági – én ide sorolnám a kiberbiztonsági – stratégiáknak biztosítaniuk kell „a lehető legnagyobb **összhangot** az állami intézkedések és a környezeti feltételek között. Az eltérés végzetes következményekkel járhat."[14]A stratégiai környezet paraméterei a technológia révén az offenzíváról a **védekezésre** változtak[15].

[9] A biztonság a mai napig az állam egyik klasszikus célja.
[10] VOLKMANN i.m. 18.o.
[11] VOLKMANN i.m. 18.
[12] SZIKINGER István : Téveszmék a biztonságról. In: OKRI Szemle (szerk.: Virág György). Országos Kriminológiai Intézet, Budapest, 2012. 28.o.
[13] SCHULZE, Matthias: Sicherheitslogik der Cyberdomäne. APUZ 22-24/2023. 23.o.
[14] SCHULZE i.m. 23 – 24.o.
[15] GLASER, Charles L. – KAUFMANN, Chaim: What is the offense-defense balance and can we measure it? International Security Vol 22, Issue 3 1998. 44.o.: "Offense-defense theory (or

A neves kiberteoretikusok, Michael P. FISCHERKELLER, Emily O. GOLDMAN és Richard J. HARKNETT számára az internet és a globális kiber- és információs tér teljesen **új stratégiai környezetet** jelent az államközi hatalom gyakorlásához, s mindez gondolkodásunk átalakítását kívánja meg.[16]
A kibertérben zajló konfliktusoknak – SCHULZE szerint – nem sok közük van a klasszikus háborúk jellemzőihez. „A kiberműveleti tevékenység nagy része a **kiberbűnözés** területéhez köthető. Itt nem az ellenfél katonai legyőzése a cél, hanem többnyire a pénzkeresés, például zsarolással vagy hozzáférési adatok adathalászatával. A kiberbűnözés egyik alkategóriája a **hacktivizmus**, ami különösen szembetűnő Oroszország Ukrajna elleni támadóháborújával összefüggésben: az aktivisták átmenetileg zavaró DDoS (Distributed Denial of Service) támadásokkal ideiglenesen megbénítják a szolgáltatásokat és a webszervereket, például az online banki ügyintézéshez."[17] A hatások általában reverzibilisek, ezért viszonylag csekélyek."[4]

---

security dilemma theory) is a quite optimistic theory of international politics, since it argues that when defense has the advantage over offense major war can be avoided. In addition, the likelihood of arms races and war can sometimes be further reduced by carefully designed arms control. Over the past two decades the theory has come to play an increasingly important role in both international relations scholarship and the analysis of foreign policy…Scholars have employed the theory to address a wide array of theoretical and policy issues, including alliance behavior, comparative grand strategy, military doctrine, military competition and cooperation, nuclear strategy and policy, and conventional arms control…Offense-defense logic has also been used to explain the causes of World War I, the causes and possible solutions of ethnic and civil wars, and the foreign policies of revolutionary states; to criticize U.S. grand strategy; and to predict the future of political relations in post-Cold War Europe as well as the size and number of independent states in the international system."

[16] SCHULZE i.m. 23.o.

[17] SCHULZE , Schulze: Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022. Ukraine-Analysen Nr. 267, 02.05.2022. 4.o.: „Neben verborgener staatlicher Aktivität ist die digitale Dimension des Ukraine-Krieges von einer Vielzahl kleinerer Scharmützel zwischen pro-russischen und proukrainischen Hacktivist:innen gekennzeichnet. Weltweit schlossen sich IT-Expert:innen und Hacker:innen dem ukrainischen Aufruf zur Bildung einer IT-Army an. Mittlerweile haben sich um die 70 Hacktivist:innengruppen, von GhostSec, Anonymous, Network Battalion 65, aber auch Cyberkriminelle wie RansomwareGruppen auf die ukrainische Seite geschlagen. Es gibt aber auch Gruppen, die Russland unterstützen wie Conti, KillDisk oder Xaknet, die bereits Cyber-Angriffe auf westliche Ziele gestartet haben. Der Begriff Hacktivist beschreibt den losen Zusammenhang global verteilter Hacker:innen, die sich ad hoc für gemeinsame Aktivitäten verbünden, aber nicht zentral gesteuert werden. Ein Großteil ihrer Aktivität ist insbesondere durch zahlreiche Distributed Denial of Service-Angriffe (DDoS) gekennzeichnet. Immer wieder werden russische Websites wie vom Kreml, von Ministerien, Botschaften, von Geheimdiensten wie dem FSB, Banken, aber auch russischen Staatsmedien temporär überlastet. DDoS-Angriffe dauern meist nur kurz an und sind reversibel. Sie werden auch immer wieder gegen ukrainische Internetdienstanbieter (ISP) gerichtet, was teilweise zu partiellen Konnektivitätsverlusten in einzelnen Regionen führt. Daneben gibt es auch zahlreiche Website-Defacement-Angriffe, bei denen Anti-Kriegsbotschaften und die berühmte »Guy Fawkes«-Maske auf Websites platziert werden."

Egyes államok **kiberbűnözési stratégiákat** is alkalmaznak pl.Észak-Korea arról ismert, hogy az állam nevében feltör mindent, amivel pénzt lehet keresni az interneten, hogy az állami költségvetést kiegészítse saját nukleáris programjának finanszírozására.[18]

SCHULZE kutatási alapján a fenti kiberdeliktumok mellett „a politikai vagy gazdasági célú kiberkémkedés az egyik leggyakoribb jelenség a kibertérben. A szellemi tulajdon „kiberkampányokon" keresztül történő szisztematikus ellopásával, azaz több egymást követő kiberakcióval – például egy gazdasági szektor központi vállalatai ellen, – az államok növelhetik erőforrásaikat. A kínai szereplők intenzív **kiberkémkedést** folytatnak azokban az ágazatokban, amelyekben Kína 2025-re globális vezető vagy a nyugati technológiáktól független akar lenni, ideértve a **mesterséges intelligenciát**, az **autonóm vezetést**, a repülést, a **fotovoltaikát**, a félvezető technológiát és még sok mást."[19]

Kínát a sajtóban érte olyan vád, hogy napelemes technológiai megoldáshoz nem tisztázott módon jutott hozzá és ezzel versenyelőnyre tehetett szert. Kína jelenleg a világ piacvezetője a napelemek gyártásában, és ezt hatalmi eszközként használhatja fel a Nyugat ellen.

FISCHERKELLER, GOLDMAN és HARKNETT kiberteoretikusok a kibertér stratégiai környezetét a következőképpen jellemzik: „az összes **hardver** és **szoftver összessége**, amelyet hálózatok kötnek össze, és amelyeket emberek alkotnak, és ezért változtathatók. Ez azt jelenti, hogy a szereplőknek nagyrészt **saját biztonsági feltételeiket** alakíthatják és kell alakítaniuk hardverük és szoftverük módosításával. Ez magában foglalja a hálózatok **védelmi technológiáinak** telepítését, a biztonsági rések megszüntetését vagy új szervezeti szabályzatok létrehozását, például a felhasználói jogok kezelését és a biztonsági mentési stratégiákat."[20]

A kibertérben zajló konfliktusok központi dinamikája – SCHULZE szerint – „a **biztonsági rések** kihasználása és azok megszüntetésére vagy csökkentésére

---

[18] SCHULZE, Matthias: Cyberspace: Asymmetrische Kriegführung und digitale Raubzüge. In: Hilpert, Hanns Günhter – Meier, Oliver (Hrsg.): Facetten des Nordkorea-Konflikts Akteure, Problemlagen und Europas Interessen. SWP-Studie 18. Stiftung Wissenschaft und Politik, Berlin, 2018. 78.o.: „Natürlich sind nordkoreanische IT-Experten aufgrund des Sanktionsregimes auf das Know-how und die Infrastruktur anderer Akteure angewiesen. Ein großer Teil des nordkoreanischen Internetverkehrs wird beispielsweise über chinesische Serviceprovider abgewickelt. Cyber-Operationen werden zudem regelmäßig über gekaperte Server im Ausland ausgeführt. Die IT-Sicherheitsfirma Recorded Future verfolgte nordkoreanische Internetaktivitäten bis nach China, Indien, Malaysia, Neuseeland, Nepal, Kenia und Indonesien zurück. Im Ausland stationierte ITSpezialisten, die in legalen IT-Firmen arbeiten, könnten im Konfliktfall als digitale Guerillakräfte operieren. Die südkoreanische Polizei schätzt, dass rund 10 000 nordkoreanische Software-Entwickler legal in China ansässig sind und regelmäßig Geld nach Nordkorea transferieren."

[19] SCHULZE (223) i.m. 24.o.

[20] SCHULZE (2023) i.m. 24.o.

irányuló kísérlet: a támadók megkísérelnek **jogosulatlan hozzáférést** szerezni a rendszerekhez, és rontják azok **bizalmasságát**, **integritását** vagy elérhetőségét. A hálózatvédők viszont a terepen, azaz saját hálózati és szoftveres infrastruktúrájuk módosításával próbálják ezt meghiúsítani. E dinamika miatt a kibertér **makroszinten ellenálló** – nehéz egyszerre lekapcsolni az egész internetet –, ugyanakkor **mikroszinten sérülékeny**, mivel bármely egyedi rendszer kellő erőfeszítéssel feltörhető, és soha nem 100 %-ban biztonságos."[21]

SCHULZE arra hívja fel a figyelmet, hogy a biztonság a kibertérben csak **globálisan** érhető el – így a tisztán nemzeti (kiber)biztonsági stratégiára való összpontosítás önmagában kevés. „A globálisan hálózatba kapcsolt tér **minden résztvevőjének** javítania kell biztonsági feltételein, hogy az mindenki számára biztonságosabb legyen."[22] Minimalizálandóak a **digitális sebezhetőségek** és így a kibertér mindenki számára biztonságosabb lehet.

A digitális védelem megteremtése viszont nem az elszigetelődés logikája mentén valósítandó meg, mivel az internet hatalmas értékteremtő potenciálja éppen az **összekapcsolhatóságban** rejtezkedik.

A kibertámadások **nagy műveleti sebessége** és a technológiai fejlesztés nyomása állandó **befektetést** igényel az IT biztonságba. A másik oldal, a támadók, anyagilag könnyebb helyzetben vannak a **támadási infrastruktúra** alacsony **belépési költségei** miatt, illetve könnyen tudják pótolni veszteségeiket. Sajnos működik olyan komplex „földalatti gazdaság" a **kiberbűnözők** számára, amelyben a kiberműveletekhez szükséges összes komponens olcsón és névtelenül megvásárolható.[23]

A kibertérben az „elrettentés", vagy a „megtorlás" paradigmája nehézkesen működik, hiszen az elkövetők – gyakori – **anonimitása** miatt nincs kit megbüntetni. Ez viszont az egész kibervédelem **hitelességét** képes aláásni.

Létezik olyan felfogás is, miszerint nem kizárólag az ellenség támadási **infrastruktúrájának deaktiválására** kell fókuszálni, hanem tanuljunk a

---

[21] SCHULZE (2023) i.m. 25.o.

[22] SCHULZE (2023) i.m. 25.o.

[23] SCHULZE, Matthias: Ransomware: technische, nationale und multilaterale Gegenmaßnahmen. SWP-Aktuell, 56/2021. 3.o.: „Die Professionalisierung folgt einer marktorientierten Entwicklung. Ransomware als äußerst profitables Geschäftsmodell hat eine ganze Untergrundökonomie mit spezialisierten Dienstleistungen entstehen lassen. Schadsoftwareentwickler vermieten ihre Software an »affiliates«, die Gewinne werden geteilt. Spezialisierte Dienstleister bieten mietbare Botnetze zum automatisierten Verbreiten von Schadsoftware über Emails an. Gegen Strafverfolgung abgesicherte besondere Server (»bullet proof hosts«) werden als »Command & Control«- Infrastruktur zur Steuerung von Schadsoftware vermietet. Den Zugang zu bereits kompromittierten und damit weiter infizierbaren Rechnern verkaufen sogenannte »access broker«. Dank grafischer Benutzeroberflächen und automatisierter Prozesse lässt sich Ransomware zudem immer einfacher bedienen. So übernehmen zum Beispiel Dienstleister arbeitsintensive Prozesse wie Zahlungsabwicklung, Kundensupport und Lösegeldwäsche in Kryptowährungen."

támadótól! „Az ötlet az, hogy megfigyeljék a támadókat saját támadási infrastruktúrájukban vagy fenyegetésvadászat során az áldozathálózatokban, és felhasználják az ott összegyűjtött információkat viselkedésükről és védekezési tervükről. Ezt a tudást azért gyűjtjük, hogy **proaktívan** igazítsuk saját védelmi rendszereinket."[24]

4. Kritikus vélemények a biztonságról

A biztonság, az emberi biztonság modern felfogása – KORINEK László szerint – feloldja az emberi jogok és a biztonság között általában feltételezett ellentétet.[25] Az emberi jogok kiterjesztése és élvezetük minél teljesebb körű biztosítása az emberek számára nem akadálya, hanem egyenesen célja, siker esetén pedig eredménye a biztonságvédelmi politikának.
A biztonság csak az emberi jogok, a szabadságjogok megnyirbálásával fokozható, és fordítva a szabadságok kiterjesztése a biztonsági szint csökkenésével jár együtt – állapítja meg FINSZTER Géza.[26]
Ennek a felfogásnak **eszmetörténeti** magvai – SZIKINGER István szerint – már Thomas HOBBES munkásságában felfedezhető, nevezetesen: az emberek a közhatalom által nem korlátozott szabadság állapotában képtelenek egyéni érdekeiket és törekvéseiket a társadalom általános elvárásai alá rendelni. A kölcsönös fenyegetettség miatt csak egy külső, cselekvési lehetőségeiben nem korlátozott erő képes a megfelelő védelmet biztosítani, s ez az erő lenne az **államhatalom**.[27]
Josef ISENSEE értelmezése alapján korunkban az állam szerepe átalakult és a szociális biztonság elvárható szintjének fenntartása érdekében meg kell haladni a tisztán szabadelvű hatalomfelfogást.[28] A pusztán őrködésre korlátozott működés helyett egyre inkább **beavatkozást** igénylő: szervező és szolgáltató feladatok ellátására van szükség. Az állam részéről továbbra is fennáll az alapjogok tiszteletben tartásának **negatív jellegű** kötelezettsége, amellett azonban – SZIKINGER István felfogásával egyet értve – az **aktivitást** feltételező **védelem** biztosítása is szükséges. Ez utóbbiaknak felel meg a biztonsághoz való alapjog.[29]
Uwe VOLKMANN viszont az állam valóban létező gondoskodási, **veszélyelhárítási** kötelezettsége mellett felhívja a figyelmet az állam

[24] SCHULZE (2023) 27.o.
[25] KORINEK László: Merre tart a világ? Fundamentum 2006/1. 83.o.
[26] FINSZTER Géza: Közrend – közbiztonság – jogbiztonság (2000-2015). In FINSZTER Géza – SABJANICS István (szerk.): *Biztonsági kihívások a 21.században*. Budapest, Dialóg Campus Kiadó, 2017. 153.
[27] Lásd SZIKINGER 2012, 18.
[28] Josef ISENSEE: *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen* Verfassungsstaates. Berlin – New York, Walter de Gruyter, 1983, 17 – 18.
[29] SZIKINGER 2012, 23.

túlbúzgóságából fakadó veszélyekre is. Az **állami aktivitás** ugyanis eljuthat egészen addig, hogy akár a még el sem követett bűncselekmények elkövetőit negligálja, likvidálja.[30] Ez viszont már a szocialista diktatúrák **gondolat-bűncselekményi** kategóriáját jelenti, s ekkor már levehető az adott államról a „jogállam" cégér (tábla), s helyette a rendőrállam **cetlit** kell kiakasztani.
A **biztonságra** való alapjog ISENSEE által képviselt felfogásának hiányossága az, hogy a gyakorlatban, a tényleges hétköznapi életben éppen a **közhatalom** jelent(heti) a legnagyobb veszélyt az emberi szabadságra.
Winfried HASSEMER szerint a rend iránti **fanatikus elkötelezettség**, az uralkodásra és mások alávetettségének elérésére irányuló törekvések miatt feltétlenül szükséges a klasszikus védelmi jogok **alkotmányos eszközökkel** történő oltalmazása. Látni kell, hogy a biztonságra való jog csak más alapjogok **korlátozásán** keresztül valósul meg. Ennek elfogadása esetén a saját szabadságunkat korlátozó **biankó csekket** írunk alá. A szabadságot nem lehet kiszolgáltatni a biztonság közhatalmi felfogása szerinti értéknek.[31] A biztonság **garanciáját** ígérő államhatalom ugyanis **leértékeli** a szabadságot, azt az üzenetet **sugározza** a polgároknak, hogy az alapjogok közül a biztonság „**primus inter pares**".[32]
A fenti megközelítések – Hans-Jörg ALBRECHT szerint[33] – még a jogállami kereteken belül képzelik el a biztonság megvalósítását, de vannak olyan koncepciók, melyek már átlépik a „rule of law" **Rubikonját**.[34] Egyes teoretikusok kivételes állapotok, kivételes helyzetek – pl. tömegkatasztrófa, lázadás, terroristák, szervezett bűnözők elleni küzdelem stb. – esetén megengedhetőnek tartják a jogállamra az „átmeneti üzemzavar miatt zárva" tábla kiakasztását. Nem véletlen a szakirodalomban és a politikában a „**biztonságiasítás**" (securitization) fogalmának meghonosodása. A securitization valójában a normál politikai folyamatok **kudarcát** jelenti, azt, hogy a demokratikus jogállam működési zavarban szenved.[35]
Mindez azért veszélyes, mert a biztonságot ígérő **diktátoraspiránsok** könnyen meghatározó politikai szereplővé válhatnak és „**stand by**" üzemmódba helyezik a demokratikus intézményrendszer garanciális szerveit (pl. bíróságok, alkotmánybíróság), amint ezeket napjaink politikai

---

[30] Uwe VOLKMANN: *Sicherheit und Risiko als Probleme des Rechtstatts*. Juristen Zeitung 2004/14., 700 – 703.
[31] Winfried HASSEMER: Staat, Sicherheit und Information. In: (Johann BIZER – Bernd LUTTERBECK – Joachim RIEß.): *Umbruch von Regelungssystemen in der Informationsgesellschaft - Freundesgabe für Alfred Büllesbach*. Stuttgart, J.F. Steinkopf Druck, 2002. 232 – 233.
[32] SZIKINGER 2012, 25.
[33] Hans-Jörg ALBRECHT*:* A büntetőjog európaizálódása és a belső biztonság Európában. Belügyi Szemle 2000/3., 36 – 37.
[34] SZIKINGER István: Terrorizmus és jogkorlátozás. Fundamentum 2005/3.,73.
[35] SZIKINGER 2012, 28.

ingamozgásai is bizonyítják.
Egyes politikai szereplők lényegében egy folyamatos **virtuális háborús helyzetet** generálnának saját politikai és jogi rémtetteik legitimálásához. Ennek a politikai hangulatkeltésnek a jogi leképeződése az **antiterrorista jog**, ugyanis a biztonság jogi alapértéke jelenti a **legitimáló bázist** a kivételes rendelkezések meghozatalára és alkalmazására pl. rögtön ítélő bíróság, fellebbezés kizárása.
Az antiterrorista jogi normák minden eddiginél súlyosabb, radikálisabb **jogkorlátozást** tesznek lehetővé, a „szép új világ" ígéretére hivatkozva. Ebben a politikai klímában természetesen szimpatikus, a magvaiban már Jeremy BENTHAMNÁL fellelhető, de posztmodern változatában Alan DERSHOWITZ munkáiban olvasható **jogszerű kínzás koncepciója**.[36] Néha előfordul, hogy a bűnüldöző apparátus téved, olyan személyt vetnek tortúra alá, akiről később kiderül, hogy nem terrorista, de ilyen „üzemeltetési költségveszteség" bárhol előfordulhat.
Az a biztonság – és FINSZTER Géza gondolataival zárom előadásomat –, amely a büntetőeljárás garanciális szabályainak leépítésével[37], az emberi jogok megsemmisítésével érhető el, semmit nem ér, mert az ilyen állapot a társadalom teremtő erejét pusztítja el.[38]

[36] Alan M. DERSHOWITZ: The torture warrant: a response to professor Strauss. New York Law School Review 2003/2., 275 – 278.
[37] FINSZTER Géza – KORINEK László: Maradhat-e alkotmányos jogállam Magyarországon? Jogtudományi Közlöny 2015/12., 575.
[38] FINSZTER Géza: Közbiztonság és jogállam. Jog-Állam-Politika 2009/3.,168.

Irodalomjegyzék

- **ALBRECHT**: Hans-Jörg: *A büntetőjog európaizálódása és a belső biztonság Európában*. BELÜGYI SZEMLE 2000/3. 17 – 41.o.
- **ÁDÁM** Antal: *A biztonság az értékek között*. JURA 2005/1. 33 – 41.o.
- **ÁDÁM** Antal: *A biztonság mint jogi érték*. In: Tanulmánykötet Erdősy Emil professzor 80. születésnapja tiszteletére (szerk: Balogh Ágnes – Hornyák Szabolcs). Studia Iuridica Auctoritate Universitatis Pécs Publicata 136. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2005. 13 – 30.o.
- **ÁDÁM** Antal: *A jogi alapértékek harmóniája és versengése*. POLGÁRI SZEMLE 2006/7-8.
- **DERSHOWITZ**: Alan M.: *The torture warrant: a response to professor Strauss*. NEW YORK LAW SCHOOL REVIEW 2003/2., 275 – 294.o.
- **FINSZTER** Géza: *Közbiztonság és jogállam*. JOG-ÁLLAM-POLITIKA 2009/3. 173 – 196.o.
- **FINSZTER** Géza: Közrend – közbiztonság – jogbiztonság (2000-2015). In FINSZTER Géza – SABJANICS István (szerk.): *Biztonsági kihívások a 21.században*. Budapest, Dialóg Campus Kiadó, 2017.
- **FINSZTER** Géza – **KORINEK** László: *Maradhat-e alkotmányos jogállam Magyarországon?* JOGTUDOMÁNYI KÖZLÖNY 2015/12., 570 – 579.o.
- **GLASER**, Charles L. – **KAUFMANN**, Chaim: *What is the offense-defense balance and can we measure it?* INTERNATIONAL SECURITY Vol 22, Issue 3 1998. 44 – 82.o.
- **HASSEMER**:, Winfried: Staat, Sicherheit und Information. In: (Johann BIZER – Bernd LUTTERBECK – Joachim RIEß.): *Umbruch von Regelungssystemen in der Informationsgesellschaft - Freundesgabe für Alfred Büllesbach*. Stuttgart, J.F. Steinkopf Druck, 2002. 232 – 233.
- **ISENSEE**, Josef: *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen* Verfassungsstaates. Berlin – New York, Walter de Gruyter, 1983.
- **KORINEK** László*: Merre tart a világ?* FUNDAMENTUM 2006/1. 74 – 85.o.
- **SCHULZE**, Matthias: *Cyberspace*: *Asymmetrische Kriegführung und digitale Raubzüge*. In: Hilpert, Hanns Günhter – Meier, Oliver (Hrsg.): Facetten des Nordkorea-Konflikts Akteure, Problemlagen und Europas Interessen. SWP-Studie 18. Stiftung Wissenschaft und Politik, Berlin, 2018. 75 – 79.o.
- **SCHULZE**, Matthias: *Ransomware: technische, nationale und multilaterale Gegenmaßnahmen*. SWP-Aktuell, 56/2021. 1 – 8.o.

- **SCHULZE** , Schulze: *Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022*. Ukraine-Analysen Nr. 267, 02.05.2022. 2 – 7.o.
- **SCHULZE**, Matthias: *Sicherheitslogik der Cyberdomäne*. APUZ 22-24/2023. 23 – 29.o.
- **SZIKINGER** István: *Terrorizmus és jogkorlátozás*. FUNDAMENTUM 2005/3.,73 – 80.o.
- **SZIKINGER** István: *Téveszmék a biztonságról*. In: OKRI Szemle (szerk.: Virág György). Országos Kriminológiai Intézet, Budapest, 2012. 17 – 36.o.
- **VOLKMANN**, Uwe *Sicherheit und Risiko als Probleme des Rechtstatts*. JURISTEN ZEITUNG 2004/14., 696 – 703.o.
- **VOLKMANN**, Uwe: *Zwischen individueller Freiheit und staatlicher Sicherheitsgewähr – Wandlungen des Rechtsstaats in unsicheren Zeiten*. APUZ 32-33/2022. 17 – 23.o.

Mitrovics Zoltán* – Fogvatartottak társadalmi reintegrációját segítő jogintézmények, programok

1. Alapgondolatok

A Bv.tv. hatályba lépését követően a hazai bv. intézetekben az addigi nevelést, a reintegráció váltotta, mely nem csak a fogalmi rendszer változását jelentette, hanem egyfajta szakmai szemléletváltást is.[1] A Bv.tv. megalkotásával több új jogintézmény is azt a célt hivatott szolgálni, mely a társadalmi reintegráció sikerességét erősíti. A reintegrációs tevékenység egy folyamat, amely a fogvatartott bv. intézetbe kerülésével megkezdődik és magában foglal minden olyan tevékenységet, amely hozzájárul a társadalmi reintegráció sikeréhez.[2] Ezen tevékenységek közé sorolhatjuk a bv. intézeteken belüli oktatást és szakképzést, a munkáltatást, illetve a szabadidős tevékenységeket, de ide sorolható a családi és társadalmi kapcsolatok megőrzésének, ápolásának támogatása is.

Mind a hazai, mind a nemzetközi kutatások a társadalmi reintegráció fogalmát, sikerességének feltételeit, kritériumait különbözőképpen határozzák meg, a fogvatartottak sikeres társadalmi reintegrációjak egyik fő ismérve azonban mindenképpen közös, mégpedig az ismételt bűnelkövetés elkerülése. A nemzetközi szakirodalomban Solomon és munkatársainak megállapításai szerint a visszailleszkedés a börtön elhagyása és a társadalomba történő visszatérés folyamata.[3] Crow inkább egy folyamatként értelmezi a visszailleszkedést, mely megállapítása szerint a lakhatási és jövedelemszerzési lehetőségek megtalálásának, a régi kapcsolatok feleleventésének és újak kialakításának a menete.[4] Maruna és munkatársai egyszerre tekintik folyamatnak és egyszeri eseménynek, melyhez szükséges a szabadult

---

* PhD hallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

[1] Dr. Bencze Béla [et. al.]: Korszakváltás a büntetés-végrehajtásban. Útmutató a 2013. évi CCXL. (Bv.) törvény megismeréséhez. (szerk.: Schmehl János, dr. Pallo József). Büntetés-végrehajtás Tudományos Tanácsa. Budapest, 2015.

[2] Ranga Attiláné, Vörös Erzsébet – Büntetés-végrehajtási reintegrációs ismeretek. Jegyzet. Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, Budapest, 2018.

[3] Solomon, A.L. – Waul, M. – Van Ness, A. –Travis, J. (2004) Outside the walls: A national snapshot of community-based prisoner reentry programs. Washington. Idézi: Albert Fruzsina – Bíró Emese (2015): A sikeres reintegráció. In: Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek.

[4] Crow, I. (2006) Resettling Prisoners: A Review. Sheffield: University of Sheffield. Idézi: Albert Fruzsina – Bíró Emese (2015): A sikeres reintegráció. In: Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek.

fogvatartott közösség általi befogadása, a folyamat már a börtönben megkezdődik és a szabadulást követően is tart.[5]
A fogvatartottak reintegrációjának kérdéskörét vizsgáló hazai kutatások közül Hegedűs Judit és Ivaskevics Krisztián vizsgálatának célja volt a fogvatartottakkal kapcsolatba kerülő személyi állomány nézeteinek, kommunikációs eszközöknek, mozgósítási technikáknak a vizsgálata, elemző bemutatása. A kutatás keretében a személyi állomány körében félig strukturált interjúkat készítettek. Az interjúk alapján, a személyi állomány körében a fogvatartottakról kialakított kép vizsgálatának keretében elemezték a társadalomba való visszailleszkedés esélyeit, a támogató és a gátló tényezőket. A kutatók a vizsgálatuk során kapott eredmények alapján arra jutottak, hogy a személyi állomány többsége tipizálja a fogvatartottakat, két nagy csoportot kialakítva, a korábban integrált, reintegrálhatók és a soha nem integrált, nem reintegrálhatók. A sikeres reintegráció feltételeként az interjúalanyok többsége említette a motivációt, a munkavállalást, a családi hátteret, valamint az iskolázottságot. A fogvatartottakkal közvetlenül kapcsolatba kerülő szakemberek, munkavállalók válaszai alapján a családi támogatásnak kiemelt szerepe van abban, hogy a sikeres reintegráció feltételeinek megteremtésében, kialakításában, újraépítésében segítséget nyújtson.[6]
A fogvatartottak reintegrációjának lehetőségeit egy 2012 és 2015 között zajló, „Szubjektív reszocializációs esélyek" elnevezésű OTKA kutatás keretében vizsgálták Albert Fruzsina és Bíró Emese. Az utánkövetéses vizsgálat keretében interjúkat készítettek a 3-6 hónappal a szabadulás előtt álló és körülbelül 6 hónapja szabadult fogvatartottakkal. A kutatás során elsősorban arra keresték a választ, hogy hogyan befolyásolják a családi kapcsolatok a sikeres társadalmi reintegrációt a börtönből szabadultak esetében. A kutatás eredményeiről több publikációban is beszámolnak, melyekből azt a következtetést tudjuk levonni, hogy a családi kapcsolatok, illetve a társas támogatás kiemelt jelentőségűek lehetnek a sikeres reintegráció tekintetében. A családi kapcsolatok a prizonizációs hatások elleni védőfaktort jelenthetik, hiszen a fogvatartottak számára elsősorban a családtagok azok, akik támogatást nyújthatnak a szabadságvesztés időtartama alatt és azt követően is.[7]

---

[5] Maruna, S. – Immarigeon, R. – LeBel, T. P. (2004) Ex-offender reintegration: theory and practice. In Maruna, S. – Immarigeon, R. (eds.) After Crime and Punishment: pathways to offender re-integration. Cullompton: Willan. Idézi: Albert Fruzsina – Bíró Emese (2015): A sikeres reintegráció. In: Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek.

[6] Hegedűs Judit – Ivaskevics Krisztián (2016): Büntetés-végrehajtásban dolgozók nézetei a reintegrációról. Alkalmazott Pszichológia, 16. évf. 4. sz. 71–92.

[7] Bíró Emese (2015): A fogvatartottak családi kapcsolatainak szerepe a bűnelkövetésben, a börtönélményben és a reintegrációban. In Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek. MTA Társadalomtudományi Kutatóközpont (Szociológiai Intézet). Forrás:

A kutatás során az is bebizonyosodott, hogy az interjúalanyok többségénél a családba történő sikeres reintegráció szorosan összefügg a sikeres munkavállalással, lakáshelyzettel, jövedelmi helyzettel és tulajdonképpen a sikeres társadalmi reintegrációt jelentő egyéb más élethelyzetekkel, összetevőkkel.
Ugyanakkor amennyiben a fogvatartott családi kapcsolati diszfunkcionálisak, a családtagok maguk is részt vettek az adott bűncselekmény elkövetésében vagy egyéb módon szerepet játszottak abban, hogy a fogvatartott bv. intézetbe került, ezekben az esetekben a bűnismétlés veszélye nagymértékben növekedhet.[8]
Borbíró Andrea és Szabó Judit 2011. évben induló kutatásának célja a hazai bv. intézetek társadalmi reintegrációt elősegítő programjainak és tevékenységének a vizsgálata volt, elsősorban a harmadlagos prevenció érvényesítésével, eredményességével összefüggő kérdéseket vizsgálták, illetve a dezisztencia és a sikeres reintegráció összefüggéseit. A kutatás során komplex módszertant alkalmaztak, jogszabályelemzést, dokumentumelemzést, fókuszcsoportos és félig strukturált interjúkat is készítettek. Az ő kutatási eredményeik is arra engedtek következtetni többek közt, hogy a család, a külső társas kapcsolatok a reintegráció szempontjából nagyon fontos tényezők.
A fentiek alapján elmondható, hogy mind a nemzetközi, mind a hazai kutatások eredményei arra engednek következtetni, hogy a sikeres társadalmi reintegráció egyik – talán legfontosabb – összetevője a támogató környezet megléte. A pozitív párkapcsolat, illetve a családi támogatás, amellett, hogy érzelmi biztonságot nyújthat, pozitív hatással lehet a munkaerő-piaci helyzetre, lakhatásra, pozitív jövőkép kialakítására, melyek a sikeres társadalmi reintegráció összetevőjének tekinthetők. A bv. intézet elhagyásának lehetőségével járó jogintézmények jó alkalmat teremthetnek az elítéltek számára ahhoz, hogy a sikeres társadalmi reintegráció szempontjából fontos társadalmi kapcsolataikat megerősítsék, szükség esetén megkezdjék azok újjáépítését.

2. Társadalmi reintegrációt segítő jogintézmények

Hazai büntetés-végrehajtási rendszerünkben számos olyan jogintézményt, programot tudunk említeni, amely a fentiek alapján a társadalmi reintegráció

real.mtak.hu/31000/1/albert_biro_sikeres%20reintegracio_bortonon%20innen%20es%20tul.pdf (letöltés ideje: 2021.12.30.)

[8] Bíró Emese-Albert Fruzsina: Hogyan befolyásolják a családi kapcsolatok a börtönből szabadultak társadalmi reintegrációját?, In.: Magyar Tudomány. Családszociológiai kutatások Magyarországon a 21. század elején. (szerk.: Csányi Vilmos), Budapest. 177. évfolyam. 2016/2. szám. 179-187.old.

sikerességét hivatottak elősegíteni. Ilyenek lehetnek az oktatás, munkáltatás, csoportfoglalkozások, különböző programok, eltávozás, kimaradás, látogatófogadás, társadalmi kötődés program, enyhébb végrehajtási szabályok alkalmazása, reintegrációs őrizet, stb. Ezen programok közül azoknak a bemutatására törekszem részletesebben, amelyek alkalmazása során a fogvatartottnak oly módon van lehetősége a sikeres társadalmi reintegráció szempontjából fontos kapcsolatait erősíteni, újraépíteni, fenntartani, hogy a bv. intézetet elhagyhatja, ugyanakkor büntetés-végrehajtási jogviszonya folyamatos, szabadságvesztés büntetésének letöltése nem szakad meg.

3. Eltávozás

Az eltávozásnak 2023.01.01. óta négy formáját különböztethetjük meg. Az eltávozás első formájára a vonatkozó jogszabályok eltávozásként hivatkoznak, azaz nem különítik el más módon a másik három formától, ezért a tanulmányban is eltávozásként hivatkozom rá. Az eltávozás engedélyezésének egyik objektív feltétele, hogy az elítélt szabadságvesztés büntetésének legalább egyharmadát letöltötte [Bv tv. 180.§ (1)], további feltétel, hogy a szabadságvesztésből letöltött időtartam, a szabadságvesztés végrehajtási fokozatához igazodóan fegyház esetén nem lehet kevesebb, mint egy év, börtön esetén fél év, míg fogház esetén három hónap. A szabadságvesztés legszigorúbb végrehajtási módja esetén az eltávozás csak kivételesen engedélyezhető, nem engedélyezhető azonban a tényleges életfogytig tartó szabadságvesztésre ítéltek esetében, illetve azon fogvatartottak esetében sem, akiket szigorú rezsimbe soroltak. [Bv tv. 100.§ (2)] Az eltávozás egy évben összesen engedélyezhető időtartamának maximuma is a végrehajtási fokozatokhoz igazodik, így fegyházban legfeljebb öt nap, börtönben legfeljebb 10 nap, fogházban és átmeneti részlegen legfeljebb 15 nap lehet. [Bv tv. 180.§ (2)]

Az eltávozás második formája a rendkívüli eltávozás. A rendkívüli eltávozást a fogvatartó bv. intézet parancsnoka engedélyezheti, melynek során az elítélt meglátogathatja orvos által igazoltan súlyos beteg közeli hozzátartozóját vagy részt vehet közeli hozzátartozója temetésén. [Bv tv. 123.§ (1)] A rendkívüli eltávozás maximális időtartama öt nap lehet. Amennyiben az elítélt a temetésen nem tudott részt venni, úgy rendkívüli eltávozás keretében engedélyezhető részére, hogy a temetést követő 30 napon belül kegyeltét az elhunyt temetési helyénél lerója.

Az eltávozás harmadik formája a jutalom eltávozás. Az elítéltek a szabadságvesztésük során bizonyos esetekben különböző jutalomban részesülhetnek. A jutalmak felsorolását a Bv. tv. tartalmazza, mely szerint az elítélt példamutató magatartásáért, a munkában elért eredményéért, a tanulásban tanúsított szorgalmáért, a közösség érdekében végzett

tevékenységéért, élet vagy jelentős anyagi érték megmentéséért vagy súlyos veszély elhárításáért jutalomban részesíthető. [Bv.tv. 165.§ (1)-(2)]. A jutalom egyik formája a jutalom eltávozás, melyre engedélyezés esetén az eltávozás szabályai érvényesek.
Az eltávozás negyedik formája a reintegrációs eltávozás. Az eltávozás formái közül a reintegrációs eltávozás a legújabb kapcsolattartási forma, melynek alkalmazására 2023.01.01. napjától van lehetőség. A reintegrációs eltávozás alkalmazásának jogszabályi feltételeit *a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvényt* is módosító az *egyes büntetőjogi tárgyú és ehhez kapcsolódóan egyéb törvények módosításáról* szóló, 2022. évi LX. törvény teremtette meg. A reintegrációs eltávozás a jogszabály részletes indokolása alapján elsősorban a reintegrációs őrizet „előszobájaként" értelmezhető, ugyanis a jogintézmény alkalmazása során tapasztaltak nagyban segíthetik a reintegrációs őrizet engedélyezése kapcsán a döntést. A reintegrációs őrizethez való szoros kapcsolódást erősíti, hogy engedélyezési feltételeik egyezők. A reintegrációs eltávozás időtartama a befogadást követő három hónap letöltése után legfeljebb öt nap, négy hónap letöltése után legfeljebb tíz nap, öt hónap letöltése után legfeljebb tizenöt nap lehet. [Bv.tv. 180/B.§ (2)] A reintegrációs eltávozást az elítélt elektronikus távfelügyeleti eszköz alkalmazása mellett veheti igénybe, engedélyezéséről a bv. intézet parancsnoka dönt.
A fentiek alapján elmondható, hogy az eltávozás fontos kapcsolattartási forma, amelynek során az elítélt az eltávozás típusától függően akár több napra is elhagyhatja a büntetés-végrehajtási intézetet. Ezen alkalmak során erősítheti családi kapcsolatait, előkészítheti munkavállalását vagy oktatásban, képzésben való részvételét, mely tevékenységek nagyban hozzájárulhatnak a sikeres társadalmi reintegráció előkészítéséhez.

4. Kimaradás

A kimaradás az eltávozáshoz hasonló jogintézmény, a különbség leginkább az időtartamban van a két kapcsolattartási forma között. Kimaradás esetén a büntetés-végrehajtási intézet legfeljebb 24 órára hagyható el. [Bv tv. 179.§ (2)] Az eltávozáshoz hasonlóan ez az időtartam felhasználható többek közt az elítélt szabadulását követő időszak rendezésére, a családi és társadalmi kapcsolatok fenntartására, erősítésére, de elősegítheti az oktatásban, képzésben való részvételt, megkönnyítheti például a vizsgákon való megjelenést, könnyebbé teheti a lakás és a munkahely keresését. Az eltávozáshoz hasonlóan a kimaradás engedélyezésénél is alapvető feltétel, hogy az elítélt a szabadságvesztésének egyharmadát már letöltötte, valamint a szabadságvesztés végrehajtási fokozatához igazodóan a szabadságvesztésből letöltött időtartam fegyház esetén nem lehet kevesebb, mint egy év, börtön

esetén fél év, míg fogház esetén három hónap. A másik fontos különbség, hogy a büntetés-végrehajtási intézet parancsnoka csoportos kimaradást is engedélyezhet kísérővel vagy kísérő nélkül. [Bv tv. 179.§ (4)] Kimaradás az eltávozáshoz hasonlóan jutalomként is engedélyezhető, melyre ugyanúgy a kimaradásra vonatkozó szabályok érvényesek.

5. Enyhébb végrehajtási szabályok alkalmazása

Az enyhébb végrehajtási szabályok (továbbiakban: EVSZ) alkalmazásának lehetőségét 1993-ban tette lehetővé a jogalkotó. Az EVSZ keretében eltávozásban részesülő fogvatartottak száma 1999-ig dinamikusan emelkedett, míg 1993-ban ez kb. 200 fő fogvatartottat érintett, addig 1999-ben ez a szám 800 fő fölé emelkedett. Majd 1999-ben két nagy sajtóvisszhangot kiváltó esemény is történt, mindkét esetben EVSZ-es eltávozáson lévő fogvatartott követett el emberölést, mely következtében az EVSZ engedélyezésére vonatkozó részletszabályokat jelentősen szigorították. A változás eredményeképpen az EVSZ kapcsán engedélyezett eltávozások száma nagymértékben csökkent.[9]
A hatályos szabályozás alapján az EVSZ alkalmazásáról a bv. intézet tesz előterjesztést a bv. bíró felé, az eljárást az elítélt vagy védője is kezdeményezheti. Az EVSZ alkalmazására csak azon elítéltek esetében van lehetőség, akik börtön vagy fogház végrehajtási fokozatban töltik szabadságvesztés büntetésüket. Amennyiben a bíróság az ügydöntő határozatban fegyház fokozatban rendelte végrehajtani a szabadságvesztést, de utólag a szabadságvesztés fokozatának enyhítése történt az EVSZ alkalmazása nem lehetséges. Az EVSZ engedélyezésének objektív feltétele, hogy az elítélt a szabadságvesztésből, a feltételes szabadságra bocsátásig esedékes időtartam felét már letöltötte, továbbá börtön fokozat esetén legalább hat hónapot, míg fogház fokozat esetén legalább három hónapot letöltött büntetéséből. Nem lehetséges az EVSZ engedélyezése abban az esetben sem, ha az elítélttel szemben más büntetőeljárás van folyamatban és az eljárást lefolytató bíróság vagy ügyészség nem járul hozzá ahhoz, hogy az elítélt a bv. intézetet őrzés nélkül elhagyja, valamint abban az esetben sem, ha több szabadságvesztés végrehajtására érkezik értesítés és ezen szabadságvesztések nincsenek összbüntetésbe foglalva.[Bv.tv. 104.§ (2)]
Az EVSZ alkalmazása iránti előterjesztés, illetve az elítélt vagy védője által benyújtott kérelem megalapozottságának ellenőrzése céljából a bv. szerv az elítélt által eltávozásra megjelölt lakcím, illetve tényleges tartózkodási hely szerint illetékes bv. pártfogó felügyelő útján környezettanulmány elkészítését

[9] Garami Lajos - Balogh Attila: Az enyhébb végrehajtási szabályok és a bv. intézet ideiglenes elhagyásával járó jutalmazási módok. In.: Börtönügyi Szemle. Büntetés-végrehajtás Országos Parancsnoksága, 2004. 2. sz. pp. 49-64.

rendelheti el. A bv. pártfogó felügyelő a környezettanulmány keretében vizsgálja és értékeli az elítélt által az eltávozás során tartózkodása helyeként megjelölt lakóingatlant, az ott életvitelszerűen tartózkodó kapcsolattartók fogadókészségét, a kapcsolattartás minőségét és azt, hogy a befogadó környezet megfelelően szolgálja-e az elítélt társadalmi visszailleszkedését.
Az EVSZ elrendelése esetén az elítéltnek lehetősége nyílik a bv. intézetet havonta akár négy alkalommal, alkalmanként 24-48 órára elhagyni. [Bv.tv. 104.§ (3)] A gyakoriságról és az időtartamról a bv. intézet parancsnoka dönt. Az eltávozáshoz és kimaradáshoz hasonlóan az EVSZ keretében történő eltávozás során az elítélt a családtagjaival töltheti idejét, a sikeres társadalmi reintegrációjához szükséges feltételek megteremtését elkezdheti.

6. Társadalmi kötődés program

A Társadalmi Kötődés Program (továbbiakban: TKP) a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény és ehhez kapcsolódóan más törvények módosításáról szóló 2016. évi CX. törvénnyel került bevezetésre 2017.01.01. napjától. A TKP-ba bevont elítélteknek lehetőségük van arra, hogy havonta legalább 5 legfeljebb 10 nap időtartamra a bv. intézetet elhagyják. [Bv tv. 187.§ (6) a)] A TKP célja, hogy elősegítse az elítélt társadalmi reintegrációját, lehetőséget biztosít a családi kapcsolatok helyreállítására, megerősítésére, munkahely keresésére, valamint akár tanulmányok folytatására, képzések elvégzésére is. A TKP alkalmazására két esetben kerülhet sor.

TÁRSADALI KÖTŐDÉS PROGRAM		
	Alkalmazásának 1. esete	Alkalmazásának 2. esete
A szabadságvesztésre történő elítélés száma alapján	Csak azon elítéltek esetében alkalmazható, akiket első alkalommal ítéltek végrehajtandó szabadságvesztésre	
Bűncselekmény súlya alapján történő alkalmazási lehetőség	Csak vétség esetén alkalmazható	Nincs erre vonatkozóan korlátozás
A szabadságvesztés időtartama alapján	A szabadságvesztés időtartama nem haladja meg az egy évet	A szabadságvesztés időtartama nem haladhatja meg a két évet

Programba vonás diszkrecionalitása alapján	Az elítélt kérelme esetén kötelező bevonni TKP-ba	Az elítélt vagy védője kérelme esetén TKP-ba bevonható

1. számú táblázat: A társadalmi kötődés program
Forrás: Saját szerkesztés, 2023.

A két esetben közös, hogy csak azon elítéltek esetében alkalmazható, akiket első alkalommal ítéltek végrehajtandó szabadságvesztésre. Az első esetben további feltétel, hogy akkor alkalmazható, ha az elítéltet vétség miatt ítélték el és a szabadságvesztésének időtartama nem haladja meg az egy évet. A második esetben a bűncselekmény súlyát tekintve nincs korlátozás egyetlen további feltétel, hogy a szabadságvesztés időtartama nem haladhatja meg a két évet. Míg az első esetben az elítélt kérelme esetén kötelező a TKP-ba helyezése, a második esetben a bv. intézet TKP-ba vonhatja az elítéltet, az erről szóló döntést a bv. intézetben működő Befogadási és Fogvatartási Bizottság hozza meg. A szabadságvesztés, az elzárás, az előzetes letartóztatás és a rendbírság helyébe lépő elzárás végrehajtásának részletes szabályairól szóló 16/2014. (XII. 19.) IM rendelet (továbbiakban: Rendelet) a végrehajtási fokozathoz és rezsim besoroláshoz igazodóan további feltételként írja elő, hogy társadalmi kötődés programba börtön fokozatú, enyhébb rezsimbe sorolt és fogház fokozatú, általános és enyhébb rezsimbe sorolt elítélt vonható be. [Rendelet 115.§ (1)]
A TKP második esetben történő alkalmazását megelőzően a Bv. tv. 187. § (2) bekezdésére, valamint a Pártfogó Felügyelői Szolgálat tevékenységéről szóló 8/2013. (VI. 29.) KIM rendelet (továbbiakban: Pfr.) 62/A.§ (3b) bekezdésére figyelemmel a bv. intézeti döntés megalapozása érdekében az elítélt által megjelölt letelepedés helye szerint illetékes büntetés-végrehajtási pártfogó felügyelő útján környezettanulmányt készül. A környezettanulmány elkészítése során a bv. pártfogó felügyelő elsődleges feladata az elítélt által megjelölt lakóingatlan TKP-ra való alkalmasságának, az ingatlanban életvitelszerűen tartózkodók fogadókészségének felmérése, valamint annak vizsgálata, hogy a befogadó környezet a társadalmi reintegrációt, visszailleszkedést elősegíti vagy veszélyezteti.
A környezettanulmány elkészítését követően, amennyiben az elítélt TKP-ba helyezése megvalósul a bv. pártfogó reintegrációs gondozásba vonja a fogvatartottat, mely keretében reintegrációs programot készít. A reintegrációs program célja, hogy a TKP-ba vont elítélt társadalmi reintegrációja sikeres legyen, ennek érdekében az elítélt a pártfogó felügyelővel köteles együttműködni a reintegrációs programban foglaltak végrehajtása kapcsán. A program megvalósulását a bv. pártfogó felügyelő nem csak intézeti keretek

között monitorozza, hanem a TKP keretében engedélyezett eltávozások során szúrópróba szerű ellenőrzéseket is végez.
A TKP során tehát egy reintegrációs program megvalósítása zajlik, melynek célja a szabadulást követő sikeres társadalmi reintegráció előkészítése. A TKP lehetőséget ad az elítéltnek arra, hogy megtegye mindazon lépéseket, melyeket csak a szabadulását követően lenne lehetősége, így a TKP keretében már a fogvatartás ideje alatt megkezdődhet a prizonizációs hatások tompítása.

7. Reintegrációs őrizet

A Magyar Országgyűlés 2014. november 18. napján fogadta el a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény és ehhez kapcsolódóan más törvények módosításáról szóló 2014. évi LXXII. törvényt, amely 2015. április 1-jei hatállyal a reintegrációs őrizet intézményéről rendelkezett.[10] Az újonnan bevezetett jogintézmény nem egy alternatív büntetési forma, hanem a büntetés-végrehajtásának egyik lehetséges eszköze, amely egyrészt az elítéltek társadalmi reintegrációjának elősegítését, másrészt a börtönpopuláció létszámának csökkentését szolgálja.
A reintegrációs őrizet alkalmazására vonatkozó általános feltételeket a Bv.tv. tartalmazza, mely alapján, az elítélt akkor helyezhető reintegrációs őrizetbe, ha a szabadságvesztés így is eléri a célját és az elítélt nyilatkozik, hogy vállalja a reintegrációs őrizetre vonatkozó szabályok betartását. Az általános feltételeken túl a Bv.tv. az elítélt bűnösségéhez kapcsolódóan rendelkezik további elvárásokról. Gondatlan elkövetés esetén a jogintézmény további feltételek nélkül alkalmazható, szándékos elkövetés esetén azonban a reintegrációs őrizet csak abban az esetben engedélyezhető, ha az elkövetett bűncselekmény nem a Btk. 459. § (1) bekezdés 26. pontjában meghatározott személy elleni erőszakos bűncselekmény, a bűnismétlés tekintetében csak azon fogvatartottak esetében alkalmazható, akiket első ízben ítéltek végrehajtandó szabadságvesztésre vagy visszaesőnek nem minősülő bűnismétlők, valamint a kiszabott szabadságvesztés időtartama az öt évet nem haladhatja meg. A szándékos elkövetés esetére előírt feltételek konjunktívak. [Bv.tv. 187/A.§ (1)]
A fentieken túl a Bv.tv. meghatároz kizáró feltételeket is, melyek alapján nem helyezhető reintegrációs őrizetbe az a fogvatartott, akinek további végrehajtandó szabadságvesztés büntetése van, vagy a letartóztatását a szabadságvesztés végrehajtására tekintettel megszakították, vagy a korábban engedélyezett reintegrációs őrizetet önhibájából megszüntették, vagy az egy évet meg nem haladó tartamú szabadságvesztésből legalább három, egy évnél

[10] Veszeli Dániel: A reintegrációs őrizet bevezetése a büntetés-végrehajtás tevékenységrendszerébe. In: Börtönügyi Szemle. Büntetés-végrehajtás Országos Parancsnoksága, 2015. 3. sz. pp. 87-99.

hosszabb tartamú szabadságvesztésből legalább hat hónapot nem töltött le, vagy a megjelölt ingatlan az elektronikus távfelügyeleti eszköz elhelyezésére alkalmatlan, illetve, akinek a kiutasításáról a bíróság vagy az idegenrendészeti hatóság rendelkezett.
A feltételek alapján látható, hogy a reintegrációs őrizet intézménye nem minden fogvatartott számára érhető el, a jogalkotó csak azon elítéltek részére tette ezt lehetővé, akik a társadalomra kevésbé veszélyesek, az általuk elkövetett deliktum tárgyi súlya kisebb, a bűnismétlés tekintetében nem tekinthetők visszaesőnek, különös vagy többszörös visszaesőnek.
A Bv.tv. 187/A. § (1) bekezdésében kerültek szabályozásra a jogintézmény időtartamának részletei. A reintegrációs őrizet időtartama tekintetében elmondható, hogy a szabályozás differenciál a gondatlan és szándékos elkövetés között oly módon, hogy gondatlan elkövetés esetén a reintegrációs őrizet maximális időtartama 12 hónap, szándékos elkövetés esetén 10 hónap lehet. Mind a 10 hónapos, mind a 12 hónapos időtartam generális maximuma a reintegrációs őrizetnek, tehát a tényleges időtartam ennél rövidebb is lehet. Fontos, hogy ezen időtartamokat feltételes szabadságra bocsátás lehetősége esetén annak esedékességétől kell számítani. A jogintézmény időtartamára vonatkozóan a fogvatartottak szempontjából kedvező változást eredményezett a veszélyhelyzet ideje alatt egyes büntetés-végrehajtási szabályok eltérő alkalmazásáról szóló 6/2023. (II. 21.) BM rendelet, mely a gondatlan bűncselekményt elkövetők esetében lehetővé tette, hogy amennyiben a szabadságvesztés időtartama a két évet meghaladja, a reintegrációs őrizet időtartama legfeljebb a szabadságvesztés időtartamának a fele legyen.
Amennyiben tehát az elítélt esetében a reintegrációs őrizet alkalmazásának feltételei fennállnak és kizáró feltételei nincsenek, a reintegrációs őrizet elektronikus távfelügyeleti eszköz[11] alkalmazása mellett biztosítható. A reintegrációs őrizet engedélyezéséről a fogvatartás helyszíne szerint illetékes Törvényszék dönt. A bv. bíró engedélyezés esetén a reintegrációs őrizetet elrendelő végzésben meghatározza a reintegrációs őrizet kezdő napját és befejező napját, valamint a reintegrációs őrizet helyszínéül szolgáló ingatlant is. Mindezeken túl a bv. bíró rendelkezik arról, hogy a kijelölt ingatlant az elítélt milyen időtartamban és milyen területi mértékben hagyhatja el. A reintegrációs őrizet időtartama alatt az elítéltnek lehetősége van többek közt a nyílt munkaerő-piacon elhelyezkedni, vagy képzésben vehet részt. Az ingatlan elhagyására vonatkozó magatartási szabályok módosítására az elítélt kérelme esetén van lehetőség, erről a reintegrációs őrizetre kijelölt ingatlan elhelyezkedése szerint illetékes Törvényszék dönt. A fentieken túl a reintegrációs őrizetbe helyezett elítéltnek a reintegrációs őrizet időtartama alatt

[11] Az elektronikus távfelügyeleti eszköz fogalma a Bv. tv. meghatározása szerint: „az elítélt vagy az egyéb jogcímen fogva tartott mozgását nyomon követő technikai eszköz.” [Bv.tv. 3.§ 6.]

olyan életvitelt szükséges folytatnia, mely a reintegrációs célokkal összeegyeztethető (pl.: nem fogyaszthat kábítószert, kerülnie szükséges a nagymértékű, rendszeres alkoholfogyasztást, magatartása nem veszélyeztetheti a vele közös háztartásban életvitelszerűen tartózkodókat stb.). A magatartási szabályok betartását a bv. pártfogó felügyelő rendszeresen, havonta legalább egy alkalommal személyesen ellenőrzi. A bv. pártfogó felügyelő az ellenőrzés mellett támogatja az elítélt társadalmi reintegrációjának megvalósulását, folyamatosan figyelemmel kíséri az elítélt kisközösségi-, családi-, baráti kapcsolatait és értékeli az azokból eredő, esetlegesen bűnismétléshez vezető veszélyforrásokat.
A fentiek alapján elmondható, hogy a reintegrációs őrizet alapvető célja az elítélt családi, társadalmi, valamint munkaerő-piaci reintegrációjának előmozdítása a szabadságvesztés céljának szem előtt tartásával. A reintegrációs őrizet időtartama alatt az elítélt visszanyeri szabadságát, de csak korlátozottan, hiszen a reintegrációs őrizet helyszínéül kijelölt ingatlant csak a bv. bíró által meghatározott módon és időszakban hagyhatja el, valamint távfelügyeleti eszköz kell viselnie a nap 24 órájában. A reintegrációs őrizet időtartama a szabadságvesztés időtartamába beszámít, tehát büntetés-végrehajtási jogviszonya továbbra is fennáll, mely alapján köteles együttműködni a büntetés-végrehajtási intézet szakembereivel. A jogintézmény jelentősége a fogvatartottak társadalmi reintegrációjának elősegítése szempontjából kiemelkedő, alkalmazása esetén a társadalomba történő visszailleszkedés egyszerre fokozatos és teljes mértékű, továbbá a börtönártalmak csökkentésében is lényeges szerepe van.[12]

8. Összegzés

A szabadságvesztés célja sokat változott, alakult a kezdeti célokhoz képest. Napjainkra amellett, hogy a büntetés-végrehajtás célja, az elítéltek vagy más okból fogvatartott személyek társadalomtól való elkülönítése, illetve az elrettentés a bűncselekmények elkövetésétől, egyre hangsúlyosabb szerepet kap az elkövető társadalmi reintegrációjának elősegítése. Célként és feladatként jelenik meg a büntetés-végrehajtás rendszerében, hogy a fogvatartás során segítséget nyújtson ahhoz, hogy az elítéltek szabadulásukat követően sikeresen munkát találjanak, újjáépítsék családi társadalmi kapcsolataikat. A társadalmi reintegráció a büntetés-végrehajtási intézetekből szabadultak tekintetében hatványozottan nehéz feladat, hiszen az esetlegesen meglévő hátrányokat (pl.: alacsony iskolai végzettség, rossz lakhatási körülmények, rossz egészségi állapot, lakhatási depriváció, stb.) a

[12] Schmehl János (2017). Stabilitás és fejlődés: A büntetés-végrehajtási törvény által bevezetett speciális jogintézmények helyzete. Belügyi Szemle, 65(11-12), 18-39.

prizonizációs hatások tovább nehezíthetik, a börtönben töltött évek stigmaként állandósulhatnak. A szabadulás utáni újrakezdés, visszakapcsolódás a mindennapokba sokszor lehetetlen kihívásnak tűnik az elítélt és a társadalmi környezete számára is. A sikeres társadalmi reintegráció érdekében jogalkotói részről is egyre szélesedik azon lehetőségek palettája, melyek segítségével a fogvatartottak a sikeres reintegráció feltételeinek számító családi, társadalmi kapcsolataikat erősíthetik. A magyarországi bv. intézetek egyre sokoldalúbb támogatást nyújtanak a fogvatartottak részére, melyek kiemelt célja a fogvatartás biztonságának megőrzése mellett, a fogvatartottak minél hatékonyabb felkészítése a szabadulásra, annak érdekében, hogy a társadalmi reintegráció minél sikeresebb legyen és ezáltal az ismételt bűnelkövetés aránya csökkenjen.

Mind a hazai, mind a nemzetközi szakirodalom számos olyan kutatási eredményt tart számon, amelyből azt a következtetést lehet levonni, hogy a társas támogatás, a szabadulást követő támogató környezet pozitív irányba tudja befolyásolni az említett célok elérését. A szabadságvesztés büntetés során az elítélteknek számos lehetőségük van kapcsolatot tartani a családtagjaikkal, barátokkal. A tanulmányban bemutatott jogintézmények oly módon járulnak hozzá a kapcsolattartás, illetve a társadalmi reintegráció sikeréhez, hogy egyfajta hidat képeznek a bv. intézet és a „szabad” társadalom között. Az elítéltnek lehetősége van még a fogvatartása alatt megtenni mindazokat a lépéseket, melyek a szabadulást követő munkavállaláshoz, oktatáshoz, lakhatáshoz szükségesek, így a tényleges szabaduláskor akár egy olyan élethelyzet várja a fogvatartottat, melyben lehetősége van dolgozni, tanulni. A szabadulást előkészítő programok, jogintézmények másik nagy előnye, hogy lehetőséget biztosítanak a családtagokkal, barátokkal, a szabadulást követő társadalmi környezettel való tényleges interakciókra, kapcsolatok újraépítésére.

Irodalomjegyzék

- Bíró Emese (2015): A fogvatartottak családi kapcsolatainak szerepe a bűnelkövetésben, a börtönélményben és a reintegrációban. In Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek. MTA Társadalomtudományi Kutatóközpont (Szociológiai Intézet). Forrás: real.mtak.hu/31000/1/albert_biro_sikeres%20reintegracio_bortonon%20innen%20es%20tul. df (letöltés ideje: 2021.12.30.)
- Bíró Emese-Albert Fruzsina: Hogyan befolyásolják a családi kapcsolatok a börtönből szabadultak társadalmi reintegrációját?, In.: Magyar Tudomány. Családszociológiai kutatások Magyarországon a 21. század elején. (szerk.: Csányi Vilmos), Budapest. 177. évfolyam. 2016/2. szám. 179-187.old.
- Crow, I. (2006) Resettling Prisoners: A Review. Sheffield: University of Sheffield. Idézi: Albert Fruzsina – Bíró Emese (2015): A sikeres reintegráció. In: Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek.
- Dr. Bencze Béla [et. al.]: Korszakváltás a büntetés-végrehajtásban. Útmutató a 2013. évi CCXL. (Bv.) törvény megismeréséhez. (szerk.: Schmehl János, dr. Pallo József). Büntetés-végrehajtás Tudományos Tanácsa. Budapest, 2015.
- Garami Lajos - Balogh Attila: Az enyhébb végrehajtási szabályok és a bv. intézet ideiglenes elhagyásával járó jutalmazási módok. In.: Börtönügyi Szemle. Büntetés-végrehajtás Országos Parancsnoksága, 2004. 2. sz. pp. 49-64.
- Hegedűs Judit – Ivaskevics Krisztián (2016): Büntetés-végrehajtásban dolgozók nézetei a reintegrációról. Alkalmazott Pszichológia, 16. évf. 4. sz. 71–92.
- Maruna, S. – Immarigeon, R. – LeBel, T. P. (2004) Ex-offender reintegration: theory and practice. In Maruna, S. – Immarigeon, R. (eds.) After Crime and Punishment: pathways to offender re-integration. Cullompton: Willan. Idézi: Albert Fruzsina – Bíró Emese (2015): A sikeres reintegráció. In: Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek.
- Ranga Attiláné, Vörös Erzsébet – Büntetés-végrehajtási reintegrációs ismeretek. Jegyzet. Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, Budapest, 2018.
- Schmehl János (2017). Stabilitás és fejlődés: A büntetés-végrehajtási törvény által bevezetett speciális jogintézmények helyzete. Belügyi Szemle, 65(11-12), 18-39.

- Solomon, A.L. – Waul, M. – Van Ness, A. –Travis, J. (2004) Outside the walls: A national snapshot of community-based prisoner reentry programs. Washington. Idézi: Albert Fruzsina – Bíró Emese (2015): A sikeres reintegráció. In: Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek.
- Veszeli Dániel: A reintegrációs őrizet bevezetése a büntetés-végrehajtás tevékenységrendszerébe. In: Börtönügyi Szemle. Büntetés-végrehajtás Országos Parancsnoksága, 2015. 3. sz. pp. 87-99.

Takács Ildikó* – A kibertér fogalmi meghatározásának sokszínűsége

1. A kibertér nemzetközi fogalmi meghatározásai

A kibertér (angolul: cyberspace) a görög kyber (jelentése: hajózni, navigálni) szóból ered, és hajózásra alkalmas teret jelent. Azaz már ez a kifejezés olyan mozgásra utal, amit térben végezhetünk, amellett, hogy irányítunk is.[1]
A „kibertér" kifejezés a képzőművészetben először az 1960-as évek végén jelent meg, amikor Susanne USSING dán művész és partnere, Carsten HOFF építész megalakították az Atelier Cyberspace nevű műhelyt. Ezen a néven "érzéki terek" címmel installációk és képek sorozatát készítették, amelyek a különböző hatásokhoz - például az emberi mozgáshoz és az új anyagok viselkedéséhez - alkalmazkodni képes nyitott rendszerek elvén alapultak [2]
Ugyanakkor az irodalomban a kibertér szót (kibernetika + tér) William GIBSON tudományos-fantasztikus (sci-fi) szerző alkotta meg 1982-ben megjelent "Burning Chrome" (Izzó króm) című novellájában és 1984-es Neurománc (Neuromancer) című regényében, [3] mely magyar nyelven is olvasható (2021 évben új magyar fordítással jelent meg).
Ezen regényében GIBSON kibertérnek nevezi el a hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális, navigálható teret. Olyan összetett mátrixnak írja le, amely színes, elektronikus, karteziánus adattájkép (dataspace), ahol vagy inkább amelyben az egyének és a cégek interaktív kapcsolatba lépnek az információval, sőt, kereskednek vele. [4]
GIBSON a kiberteret zordnak írja le, de igyekszik azt ismerőssé tenni. Fontos, hogy GIBSON szerint test nélküli tudatok élnek a kibertérben, az eseményeket ismerős képek bemutatásával ábrázolja, azt állítja, hogy a kibertér

---

* PhD hallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

[1] Lásd még: GÉMES Csaba: A kibertér szereplői. Hadmérnök 2018/3. 404.o.: „A fogalom eredetét keresve először a görög „*kübernétész*" görög (jelentése: kormányos) szóból eredő kibernetikával találkozunk. A kibernetika egy komplex tudományos irányzat, amely a szabályozás, vezérlés, információfeldolgozás, -továbbítás általános törvényeit kutatja. A kibernetika alapítójának az amerikai matematikus Norbert Wienert tartják, aki a második világháború alatt a légvédelmi rendszerek matematikai problémáival foglalkozva 1940-ben fogalmazta meg a korszerű számítógépekkel szemben támasztott alapkövetelményeket."

[2] LILLEMOSE, Jacob – KRYGER, Mathias https://web.archive.org/web/20150826204717/http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/ 1.o.

[3] GIBSON, William: Neurománc. Vallhala Páholy, Budapest, 1999. 50-65.o.

[4] MÉSZÁROS Rezső: A kibertér társadalomföldrajzi megközelítése. Magyar Tudomány 2001/7. 769 – 770.o.

információból áll, továbbá megjeleníti a halhatatlanság lehetőségét, ami a kibertéren keresztül akár elérhetővé is válhat.
Érdekesség még e körben, hogy William GIBSON írótól származik a meatspace (tükör fordításban: hús-tér) kifejezés is, amelyet a kibertér ellentéteként használ a fizikai világ jelölésére.
John Perry BARLOW 1991 évben az alábbiak szerint fogalmazta meg a kibertér lényegét: „a szülőföldje az információs korszaknak, és a hely ahol a jövő polgárai arra vannak utalva, hogy itt elidőzzenek".[5]
BARLOW felfogásában a kibertér olyan alternatív virtuális világ, amely először „elektronikus határvidék"-ként jelenik meg, és minőségileg több mint a számítógéphez kapcsolt telefonvonalak hálózata.[6]
Michael BENEDIKT 1991 évben megjelent „Cyberspace: Some Proposals" című kötetében akként határozta meg a kibertér fogalmát, hogy az egy többdimenziós mesterséges vagy virtuális valóság, globális hálózattal rendelkezik, számítógépek tartják fenn, és teszik általánossá. [7]
Az 1994-ben publikált „Cyberspace and the American Dream: Magna Charta for the Knowledge Age" című munkában Esther DYSON és szerzőtársai a kihívás oldaláról közelítette meg a kibertér fogalmát. A kibertér megismerése álláspontjuk szerint a civilizáció egyik legnagyobb kihívása lehet. [8]
Douglas Mark RUSHKOFF a korai cyberpunk-kultúrához való kötődéséről ismert. Az 1994 évben megjelent „Cyberia" című könyvében a kiberikus

---

[5] MORRISON, Aimée Hope: An impossible future: John Perry Barlow's 'Declaration of the Independence of Cyberspace'. New Media & Society March 5. 2015. 53 – 57.o.:"Barlow's declaration aims specifically to fix a particular kind of cyberspace in the wider imaginary, and he employs metaphor to do so. On offer in the declaration are battles between mind and body, parent and child, government and citizen, freedom and censorship, hygiene and infection and 'pig iron' and ideas."

[6] MÉSZÁROS Rezső: A kibertér, és ami körülötte van: Társadalomföldrajzi megközelítés. JATEPress, Szeged, 2008. 56.o.; Lásd még: MÉSZÁROS Rezső: A kibertér, mint új földrajzi tér. In: KISS Andrea – MEZŐSI Gábor –SÜMEGHY Zoltán (szerk.) Táj, környezet és társadalom: ünnepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére = Landscape, environment and society: studies in honour of professor Ilona Bárány-Kevei on the occasion of her birthday. Szegedi Tudományegyetem Éghajlattani és Tájföldrajzi Tanszék – Szegedi Tudományegyetem TTIK Természeti Földrajzi és Geoinformatikai Tanszék, Szeged, 2006. 493 – 494.o.: A kibernetikai tér „terének" számos aspektusa van. Térgeometriáinak meghatározása igen nehéz feladat. A több milliárdnyi bináris számjegyből felépülő kibertér úgy létezik, mint sok különféle forma együttese, többek között weblapokból, társalgókból, hirdetőtáblákból, MUD-okból, a virtuális valóságot megjelenítő, a virtuális valóság környezetét adó helyekről, információs adatbázisokból áll, mindegyiknek megvan a maga „jellegzetes hely- és térhangulata és saját földrajza" (Batty, M. 1997). A kibertér olyan világokat képes kínálni, amelyek első pillantásra
a földrajzi tér és a világűr folytatásának tűnnek, de ha közelebbről is megvizsgáljuk, világosság válik, hogy itt a tér-idő fizikai törvényeinek alig van értelme".

[7] MÉSZÁROS Rezső (2008), 57.o.

[8] MÉSZÁROS Rezső (2008),59.o.

ellenkultúrát hangsúlyozza, amely a valóság újra definiálására törekszik, ahol az emberek kezdik megérteni a technológiai civilizáció kiépítésének rendszerszintű, kulturális és spirituális következményeit.
A kiberteret háromdimenziós világként ábrázolja, ahol a felhasználók információs és kommunikációs csatornákat, számítógépes programokat és adatokat használva időtől és helyszíntől függetlenül kerülnek egymással kölcsönhatásba, kilépve a fizikai valóság szabályai alól. [9]
Az 1995-ös évben a Cybermap Gazetteer: Maps of the On-line World of Browaing and Business című munkában John DECEMBER azt állította, hogy különböző elektronikus kommunikációs rendszerek önálló belső tereiből áll a kibertér.[10]
William MITCHELL a „City of Bits" című közleményében arra az álláspontra helyezkedett, hogy a kibertérnek nincs köze a térhez, mondhatni térellenes megközelítést alkalmazott. Nézete szerint nem lehet megmondani, hogy hol van a kibertér, milyen alakja van, miként néz ki, azaz nincs sehol, de mégis mindenhol jelen van.[11]
Az 1996-ben leközölt a „Lost in Cyberspace: Cultural Geography of Cyberspace" című kötetében Steve MIZRAH azt állította, hogy a kibertér egy kulturális vidék, ahol bizarr és furcsa dolgok is létezhetnek például a folyók felfelé folynak.[12]
Az 1999-ben Margaret Wertheim WERTHEIM visszaté Michael BENEDIKT fogalmi meghatározáshoz, melyet továbbfejleszt azzal, a hogy a kibertér szerinte kapcsolatot is formál a résztvevők és a közvetítők között a való világban. [13]
Martin DODGE és Rob KITCHIN a jelen téma egyik legismertebb kutató párosa. Közösen írták a „Mapping Cyberspace"[14] és az „Atlas of Cyberspace"[15] című könyveket, melyekben kibertér fogalmát magának a tér megragadásával definiálták. Álláspontjuk szerint a kibertér (vagy virtuális tér, mivel e kettőt nem választották el) az valójában egy számos tulajdonsággal és funkcióval rendelkező társadalmi tér, annak is egy speciális formája.[16]
David SILVER 2000 évben megjelent „Cyberculture Studies 1990-2000" kötetében három fő szakaszt különített el a kibertér életében az 1990-2000 időszakra vonatkozóan, melyek a következők voltak: a kezdeti népszerű

[9] KISS Tibor: A kibertér fogalma. In: KISS Tibor (szerk.): Kibervédelem a bűnügyi tudományokban. Dialóg Campus, Budapest, 2020. 11.o.
[10] MÉSZÁROS Rezső (2008), 59.o.
[11] MÉSZÁROS Rezső (2008), 59.o.
[12] MÉSZÁROS Rezső (2008), 59.o.
[13] MÉSZÁROS Rezső (2008), 59.o.
[14] Routledge, 2000.
[15] Addison-Wesley, 2001.
[16] MÉSZÁROS Rezső (2008), 59.o.

szakasz, majd az elméleti szakasz, míg elérkeztünk a vita szakaszához, mely jól tükrözi, hogy a terület kezd érettebbé válni. [17]

Az „An Introduction to Cyberculture" (2001) művében David BELL azt az álláspontot képviseli, hogy a kiberteret alapvető térkategóriának ismeri el. Eszerint a kibertér nemcsak hardware, hanem szimbolikus definíciók, úgynevezett „trópok" sorozata, amelyek ötletek hálózatát csak úgy, mint bitek kommunikációját alkotják. [18]

Jason WHITTAKER a 2004. évben megjelent „The Cyberspace Handbook" című kötete egy átfogó útmutató az új média, az információs technológiák és az internet minden aspektusáról. Áttekintést nyújt a kibertér gazdasági, politikai, társadalmi és kulturális összefüggéseiről, továbbá gyakorlati tanácsokat ad az új technológiák kutatásra, kommunikációra és publikálásra való felhasználásához. Álláspontja szerint a kibertér egy hibrid tér, melybe beletartozik az internet, a virtuális valóság és a hagyományos telekommunikációs hálózatok is. [19]

FANG Binxing a „Cyberspace Sovereignty című művében négy alapvető elem együtteseként ábrázolja a kiberteret, melyek a következők: információs és kommunikációs infrastruktúra, adatok összesége, a felhasználók és a szerepkörök összessége, valamint a műveletek és tevékenységek összessége. FANG álláspontja szerint az elmúlt években az infrastruktúrák, adatok, emberek és műveletek kombinációja mentén háromféle definíciós nézőpont került a figyelem középpontjában:

1. Nyilvános nézőpont, mely szerint a kibertér az ember által gyártott olyan elektromágneses tér terminálokkal, számítógépekkel, hálózati eszközökkel, amelyeken keresztül a felhasználók létrehozzák, tárolják, továbbítják, megjelenítik és használják az adatokat. A kibertérben az ember, a gép és az adat kapcsolódásával, kölcsönhatásával valósítható meg az információszolgáltatás, ami befolyásolja az emberek életét.
2. Akadémiai nézőpont: a kibertér olyan ember által alkotott hely, ahol a felhasználó információs és kommunikációs technológiák által általános jeleket (pl. optikai, elektromos, mágneses, akusztikus jeleket) generálhat, továbbíthat, tárolhat, dolgozhat fel, jeleníthet meg és ezzel kifejezheti akaratát.
3. A nemzetközi szervezetek definícióiból ered. A kibertér olyan mesterséges tér, mely az információs és kommunikációs technológia infrastruktúrájára épülve támogatja az emberek információs tevékenységét, vagyis az adatok generálását, tárolását, átvitelét,

[17] MÉSZÁROS Rezső (2008), 56.o.
[18] MÉSZÁROS Rezső 82008), 57.o.
[19] KISS Tibor (2020), 10.o

megváltoztatását, használatát és megjelenítését megvalósító műveleteket. [20]

Tisztában kell lennünk azzal, hogy a kibertér fogalom meghatározása nem szűkíthető le kizárólag a társasdalomföldrajz, a jogtudomány, a matematika vagy éppen az informatika oldalára, mivel a kibertér definíciója az irodalomban is megjelenik.

Már fentebb említettem GIBSON 1982-ben megjelent „Burning Chrome" című novelláját és 1984-es Neurománc (Neuromancer) című regényét, mely bemutatja, hogy az 1980-as években a sci-fi irodalomnak kifejlődött egy változata, mely fiktívnek állította be a társadalmat és a benne működő technikát. Ezt az irányzatot nevezzük cyperpunk vagy kiberpunknak.

Azaz a cyberpunk a sci-fi egy alműfaja a disztópikus futurisztikus környezetben, amely hajlamos az "alvilág és a csúcstechnológia kombinációjára" összpontosítani, olyan futurisztikus technológiai és tudományos vívmányokkal, mint a mesterséges intelligencia[21] és a kibernetika, szemben a társadalmi összeomlással, disztópiával vagy hanyatlással.[22]

A kibertér fogalmi meghatározására a cyberpunknak abban volt nagy hatása, hogy a művekben az írók próbálták leírni, bemutatni, ábrázolni magát a kiberteret, és azt is szabadon vizsgálhatták, hogy a tudomány fejlődése, az elektronika, az új képzeletbeli vívmányok milyen befolyással vannak az emberekre, és ennek milyen következményei vannak.

2. A kibertér magyar fogalom meghatározásai

A kibertér fogalmának a magyar szakirodalomban megjelenő valamennyi meghatározására nem vállalkozom, de bemutatok néhány – általam mértékadónak tekinthető – definíciót.

---

[20] KISS Tibor (2020), 10.o.

[21] Lásd még: GÁTI Balázs: A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései. In: BUJTÁR Zsolt – GÁSPÁR Zsolt – SZILOVICS Csaba – BRESZKOVICS Botond – FERENCZ Barnabás – ÁZSÓTH Szilvia (szerk.): Fintech – Defi – Kriptoeszközök gazdasági és jogi lehetőségei és kockázatai. Konferenciakötet. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2022. 61 – 65.o.

[22] Ehhez lásd még: KISS Kata Dóra: Cyberpunk disztópiák és biohatalom a Ghost in the Shell elemzésén keresztül. Filmszem 2018/4. 16.o. „A cyberpunk világkép alapvonása, hogy egy olyan nem túl távoli jövőt ábrázol, ahol a technológia az élet minden területét behálózva az emberi létezés alapfeltételévé válik. A technológia ezzel a kontroll eszköze is: általa az ember képes normál funkcióit kierjeszteni, de egyben befolyásolja a szubjektivitást és a szubjektum státuszát. Az olyan létbiztosító tevékenységek mint alvás, evés, reprodukció ezekben a fiktív világokban módosulnak, egyszerűsödnek vagy kiiktatódnak a technológia eszközeinek segítségével. A cyberpunk disztópiák atmoszférájára jellemző az elidegenedés, a technológia emberi mimikrije, az ember dehumanizálódása, a totalitariánus államok vagy megavállalatok, és a nem túl távoli múlt természeti katasztrófái, amik egy poszt-indusztriális disztópikus életteret képeznek."

SZABÓ Katalin és HÁMORI Balázs[23] felelevenítik WHEELER és kollégái meghatározásához, amikor azt az álláspontot képviselik, hogy „az absztrakt tér (cyber) egy-, két- vagy háromdimenziós térre vonatkozó fogalom, tekintet nélkül bármely földfelszíni vonatkozási pontra. Az absztrakt tér minden vonatkozásában homogén, és a benne való mozgás minden irányban egyformán könnyű."[24]

SZKÁLA Károly és MUNK Sándor szerint a „kibertéri informatika és számítástechnika új fogalmakat, technológiai körülményeket és környezetet hoz be mindennapi életünkbe. A kibertér napjainkban különböző alkalmazási területek, szakmai körök, sőt a mindennapi közbeszéd gyakran használt, népszerű kifejezése. A fejlett számítás- és információtechnológia eredményeként kialakuló hálózatalapú rendszerek egy olyan kommunikációs szolgáltatási, virtuális működési környezetté váltak, amelyek mindenki számára hozzáférhető virtuális térként, világként megélhető környezetet alkotnak".[25]

MUHA Lajos informatikus megfogalmazásában a kibertér nem más, mint: egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszerek és beágyazott processzorokat és vezérlőket.[26]

PARTI Katalin és KISS István definíciójában a kiberbűnözés (informatikai bűnözés) a számítástechnikai bűnözés (computer crime) és az internetes bűnözés (internet crime, cyberspace crime) kategóriájába tartozó

---

[23] SZABÓ Katalin – HÁMORI Balázs: Információgazdaság: Digitális kapitalizmus vagy új gazdasági rendszer? Akadémiai Kiadó, Budapest, 2006.

[24] MÉSZÁROS Rezső (2008), 59.o.

[25] SZKÁLA Károly és MUNK Sándor: A kibertér fogalma, értelmezése és fejlődése. Földrajzi Közlemények 2018/4. 344.o. Ehhez lád még: MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány 2018/1. 114.o.: „… a kibertér fogalmának értelmezéséhez fel kell tennünk, ahhoz kapcsolódik, hogy minek tekintjük a kiberteret, vagyis hogy egy arisztotelészi definíció esetében mi a legközelebbi fölérendelt nem-fogalom (genus proximum). A kibertér – mint szinte bármelyik más fogalom – szakirodalomban megtalálható definíciói természetesen nem mind felelnek meg a filozófia, a logika követelményeinek, azonban legtöbb esetben így is feltárható belőlük hogy a meghatározás megalkotói szerint a kibertér milyen magasabb szintű fogalom körébe tartozik. A legközelebbi nem-fogalom meghatározása segíti az értelmezést, de látnunk kell, hogy nem teszi egyértelművé, mivel általában a magasabb szintű fogalom értelmezése sem egyértelmű, sokszor köznapi értelmezések által befolyásolt."

[26] MUHA Lajos – KRASZNAY Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem, Budapest, 2018. 117.o. Megjegyzés: Eredetileg W. GIBSON regényéből átvett science-fiction kifejezés, mely a számítógép-kommunikáció birodalmát, annak virtuális világát kívánja megnevezni. Eszerint a kibertér nem más mint a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben.

magatartásokat kizárólagos módon magában foglaló kategória, amely egyben a kétfajta bűncselekmény közös halmazát is tartalmazza.[27]
SZÁSZI Antónia szerint a kibertér számítógéprendszerek és -hálózatok által alkotott metaforikus tér, ahol elektronikus adatok kerülnek tárolásra, valamint online adatforgalom és kommunikáció zajlik. Ezen kiindulópont alapján a kiberbűnözés számítógépek és számítógépes rendszerek segítségével, illetve azok kárára elkövetett bűncselekmények gyűjtőfogalma; a kibertérben zajló bűnözés.[28]
HAIG Zsolt szerint a kibertér „az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot."[29]
A magyar jog világa is megalkotta a saját kibertér fogalmát, melyet Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 1. melléklet 3-as pontja az alábbi meghatározást tartalmazza: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett. [30]
A fenti definícióból kitűnik, hogy a kibertér meghatározása nem szűkíthető le csak és kizárólag az internet közegre. A kibertér szélesebb, az internet globális hálózata egyes interakciók megfigyelése esetén a kibertér reprezentatív kutatási terepe.
Bizonyított tény, hogy a kibertér képes befolyással lenni a közösségekre és az éntudatra. Lehetőséget ad élményeket úgy megtapasztalni, hogy fizikálisan az

[27] PARTI Katalin – KISS István: Informatikai bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., Budapest, 2016. 491.o.
[28] SZÁSZ Antónia: A kiberbűnözés társadalmi kontextusa. In: Kovács Janka – Kökényessy Zsófia – Lászlófi Viola (szerk.): A normán innen és túl: Tanulmányok a Történeti Kollégium konferenciájának előadásaiból. ELTE BTK Történeti Kollégium, Budapest, 2017. 95.o.
[29] HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest, 2018. 226 – 227.o.
[30] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat

ember nem mozdul el, hanem például csak ül a saját számítógépe vagy más erre alkalmas eszköz előtt.
Egyre inkább felmerül a kibertér használata más területeken, mint például a politikában, mivel új helyet kínál a kampány tevékenységek lefolytatására, hiszen a cél az, hogy minél több embert el lehessen érni.

3.A kibertér meghatározása a kiberbűnözés fogalmán keresztül

A kibertér nem csak előnyökkel, hanem veszélyekkel[31] is jár, gondolok itt a kiberbűnözésre. KISS Tibor szerint a kibertér fogalmának használatakor egyrészt célszerű a jogi-bűnüldözési megközelítést alapul venni, másrészről azokat a technodiskurzusokat, amelyekben a kiberteret technikai megközelítésből vizsgálják és építik fel.[32]
NAGY Zoltán arra hívja fel a figyelmet, hogy az informatikai deliktumok meghatározására tett kísérletek részben „korfüggők", tehát az adott történelmi periódusban[33] megjelenő jogsértések definíciós nyomvonalként szolgálnak a kutatók számára.[34]

---

[31] Lásd bővebben: KRASZNAY Csaba: Kiberbiztonság a XXI.században. Katonai Nemzetbiztonsági Szolgálat, Budapest, 2022. 33.o. A szerző egyebek mellett utal a hálózatosodás veszélyeire. ; Andrea KRAUT – László KŐHALMI – Dávid TÓTH: Digital Dangers of Smartphones. Journal of Eastern-European Criminal Law 2020/1. 36-39.o.; GÁL István László – BARTKÓ Róbert: A kibertérben megjelenő büntetőjogi kihívások és fenyegetések büntetőjogi kezelésének tendenciái. Military and Intelligence CyberSecurity Research Paper 2022/12. 3 – 4.: „Ebben a formálódásban, „fejlődésben" jelentős szerepet játszott az informatika, fejlődése, a technológia új vívmányainak megjelenése, az internet világméretűvé válása is, mely a terrorista hadviselés számára egyértelműen új távlatokat nyitott. Az ún. konvencionális terrorizmus mellett „a paletta színesedett" a tömegpusztító fegyvereket alkalmazó, valamint a számítógépes terrorizmussal is10 (összefoglaló nevén: „ABC - Terrorizmus"), utóbbi pedig a kibertérben rejlő lehetőségeket is kiaknázta."
[32] KISS Tibor: A kibertér fogalma. In: KISS Tibor (szerk.): Kibervédelem a bűnügyi tudományokban. Dialóg Campus, Budapest, 2020. 9.o.
[33] NAGY Zoltán András: Informatikai bűncselekmények. Magyar Tudomány 2001/8. 946 – 949.o. „Az informatikai bűnözés a bűncselekmények konkrét megjelenési formáinak, valamint a veszélyeztetett jogtárgyak sokrétűsége miatt csak gyűjtőfogalommal írható le. A szakirodalomban eddig nem született olyan fogalom, amely széles körben elfogadottá válhatna. Ennek magyarázatául az szolgál, hogy egyfelől ez a kriminális jelenség új keletű, másfelől az informatika fejlődésével a veszélyeztetett értékek és érdekek köre is gyarapszik."
[34] NAGY Zoltán: Az informatikai bűncselekmények. PhD-dolgozat. Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskola, Pécs, 2000. 39 – 45.o. Lásd még: NAGY Zoltán András: A számítógépes bűncselekmények hazai szabályozása. In: Tóth Mihály – Gál István László (szerk.): Gazdasági büntetőjogi tanulmányok. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2005. 302 – 305.o.

Azzal, hogy a kibertér rohamosan fejlődik, természetszerű, hogy ezen a területen is megjelentek a bűnelkövetők. A technika rohamos fejlődésével a kibertér veszélyei is megnövekedtek.[35]
Az 1980-as és 1990-es években ez a veszély leginkább vírus, illetve féreg (worm) támadásokban merült ki, melyek a felhasználónak kárt okoztak és nem kevés bosszúságot, de valójában jelentéktelen volt a hatásuk.
A számítógépes vírus befűzi magát a gazdaprogramba és elkezdi multiplikálni önmagát. A vírusok egyik legveszélyesebb fajtáját a makrovírusok jelentik, melyek rendkívül virulensek. Létezik egy ritka példányuk, ami például kifejezetten a merevlemezt próbálja megformázni. A féreg bár nagyon hasonlít a vírusra, de ugyanakkor nem igényel gazdaprogramot önmaga sokszorosításához, továbbá másolatait gyakran a hálózaton terjeszti.[36]
A kiberbűnözés fogalma sem egységes, több elhatárolást ismer a szakirodalom. Mind nemzetközi, mind hazai szakirodalomban megjelentek fogalom meghatározások. Több szerző is gyűjtőfogalomként határozza meg a kiberbűnözés fogalmát, melynek két fő kategóriáját különbözethetünk meg:

- az egyik kategória a tisztán informatikai bűncselekmények vagy kiberbűncselekmények, az úgynevezett cyber-dependent crime (pl. számítógépes vírusok használata, hacking stb.), mivel ebbe a körbe azokat a bűnelkövetéseket sorolják, melyeket kizárólag információs rendszerekkel követnek el;
- a másik kategória az úgynevezett cyber-enabled crime, mely azokat a bűncselekményeket foglalja magába, melyeket az információs rendszerek felhasználásával követnek el, mint például a csalás, a zsarolás, a pénzmosás stb. [37]

Más meghatározás szerint a kiberbűnözés számítógépek és számítógépes rendszerek segítségével, vagy számítógépek és hálózatok kárára elkövetett bűncselekmények gyűjtőfogalma.
Találkozunk olyan megközelítéssel, mely szerint a kiberbűncselekmény általános fogalma alatt „az informatikai eszközök és/vagy rendszerek segítségével, vagy az informatikai eszközök és hálózatok ellen elkövetett bűncselekmények értendők, amelyek céljai lehetnek a rendszerben tárolt adatok megszerzése, a jogosultak számára hozzáférhetetlenné tétele, továbbá az elektronikus rendszerbe vetett bizalommal visszaélés”[38]

---

[35] Lásd bővebben: PARTI Katalin – KISS Anna: A számítástechnikai bűnözésről akkor és most. In: BÁRD Petra – HACK Péter – Holé Katalin: Pusztai László emlékére. Országos Kriminológiai Intézet – ELTE Állam-és Jogtudományi Kar, Budapest, 2014. 297 – 310.o.
[36] BÁTORFI Botond a kibertér veszélyei: https://fintech.hu/a-kiberter-veszelyei/ 2.o.
[37] MEZEI Kitti: A kiberbűnözés szabályozási kihívásai a büntetőjogban. Ügyészek Lapja 2019/4-5.o.
[38] GYARAKI Réka (2018), 27.o.

A Számítástechnikai Bűnözésről szóló Egyezmény (Convention on Cybercrime, az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye, amelyet a 2004. évi LXXIX. törvénnyel hirdettek Magyarországon) cybercrime kifejezést használja, mely vissza eredeztethető William GIBSON tudományos-fantasztikus író cyberspace kifejezésére. E kontraktus – közismert nevén: Budapesti Egyezmény – az egyik legfontosabb jogi dokumentum ezen a területen, de a kiberbűnözés fogalmát nem határozza meg, annak „csak" csoportosítását végzi el:

- számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények,
- a számítógéppel kapcsolatos bűncselekmények,
- a számítástechnikai adatok tartalmával kapcsolatos és szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.[39]

Kiberbűnözésről tehát: egyrészt olyan új típusú bűncselekményekről beszélhetünk, amelyek kizárólag az információs rendszerek segítségével követhetők el és olyan speciális védett jogi tárggyal rendelkeznek, mint az információs rendszer vagy számítógépes adat; másrészt ide tartoznak azok a hagyományos bűncselekmények is, amelyek könnyebben elkövethetők az új elkövetési eszközök segítségével.[40]

Általánosságban tehát elmondható, hogy a kiberbűnözés általános definíciója szerint – amit lehet a számítástechnikai bűnözés egyfajta szinonimájaként is értelmezni – a kibertérrel összefüggésben elkövetett bűncselekmények összességét kell érteni..[41]

4. Zárógondolatok

A többféle megközelítés és definíció áttekintése után arra az álláspontra helyezkedem, hogy a kibertér (cyberspace) számítógép-rendszerek és -hálózatok által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak és online adatforgalom, valamint kommunikáció zajlik.[42]

A kibertér lehetővé teszi az emberek számára, hogy globálisan kommunikáljanak, információkat osszanak meg, üzleti tranzakciókat bonyolítsanak le és számos egyéb tevékenységet végezzenek online.

[39].MEZEI Kitti (2019), 4 – 5.o.
[40] MEZEI Kitti (2019), 4 – 5.o.
[41] SIMON Béla: A kiberbűnözés aktuális trendjei. Magyar Rendészet 2018/1. 161.o.
[42] KISS Tibor (2020), 12.o.

A kibertér határait nehéz meghatározni, mivel sokszor átfedik a való világ határait. A kibertérben új, komoly fenyegetést[43] jelent – AMBRUS István kutatásaiból megismert – a mesterséges intelligencia.[44]
A kibertér határai általában az internetes kapcsolat határai, azonban lehetnek politikai, jogi és kulturális határok is. Ezek a határok azonban dinamikusak és folyamatosan változnak a technológiai és társadalmi változások függvényében.

[43] NAGY Zoltán András: A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén. Belügyi Szemle 2018/10. 41– 45.o.; HERKE Csongor: A mesterséges intelligencia kriminalisztikai aspektusai. Belügyi Szemle 2021/10. 1713 – 1716.o.; Flóra JÓZAN – László KŐHALMI: Rule of Law and Criminal Law. Thoughts about the criminal justice of the Millenium Era. Journal of Eastern-European Criminal Law 2017/1. 214.o.; KŐHALMI László: Jogállam és büntetőjog – avagy kételyeim az ezredforduló kriminálpolitikája körül. In: Karsai Krisztina (szerk.): Keresztmetszet. Pólay Elemeér Alapítvány, Szeged, 2005. 128 – 129.o.; GÁSPÁR Zsolt – SZÍVÓS Alexander – BUJTÁR Zsolt: Beszámoló a „Kriptoeszközök világa a jog és a gazdaság szemszögéből" című nemzetközi tudományos konferenciáról. Külügyi Műhely 2021/1. 200.o.; ESZTERI Dániel – MÁTÉ István Zsolt: Identitáslopás a virtuális világban. Belügyi Szemle 2017/3. 79 – 107.o.
[44] AMBRUS István: Digitalizáció és büntetőjog.Woltzers Kluwer Hungary, Budapest, 2021. 164 – 188.o.

Irodalomjegyzék

- **AMBRUS** István: *Digitalizáció és büntetőjog*.bWoltzers Kluwer Hungary, Budapest, 2021. 164 – 188.o.
- **BÁTORFI** Botond: A kibertér veszélyei: https://fintech.hu/a-kiberter-veszelyei.
- **ESZTERI** Dániel – **MÁTÉ** István Zsolt: *Identitáslopás a virtuális világban*. BELÜGYI SZEMLE 2017/3. 79 – 107.o.
- **GÁL** István László – **BARTKÓ** Róbert: *A kibertérben megjelenő büntetőjogi kihívások és fenyegetések büntetőjogi kezelésének tendenciái*. MILITARY AND INTELLIGENCE CYBERSECURITY RESEARCH PAPER 2022/12. 1-30.o
- **GÁSPÁR** Zsolt – **SZÍVÓS** Alexander – **BUJTÁR** Zsolt: *Beszámoló a „Kriptoeszközök világa a jog és a gazdaság szemszögéből" című nemzetközi tudományos konferenciáról*. KÜLÜGYI MŰHELY 2021/1. 197 – 202.o.
- **GÁTI** Balázs: *A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései*. In: BUJTÁR Zsolt – GÁSPÁR Zsolt – SZILOVICS Csaba – BRESZKOVICS Botond – FERENCZ Barnabás – ÁZSÓTH Szilvia (szerk.): Fintech – Defi – Kriptoeszközök gazdasági és jogi lehetőségei és kockázatai. Konferenciakötet. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2022. 59 – 78.o.
- **GÉMES** Csaba: *A kibertér szereplői*. HADMÉRNÖK 2018/3. 403 – 415.o.
- **GIBSON**, William: *Neurománc*. Vallhala Páholy, Budapest, 1999.
- **GYARAKI** Réka: *A kiberbűncselekmények megjelenése és helyzete napjainkban* PhD-dolgozat. Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskola, Pécs, 2018. 27. oldal
- Flóra **JÓZAN** – László **KŐHALMI**: *Rule of Law and Criminal Law. Thoughts about the criminal justice of the Millenium Era*. JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 2017/1. 208 – 216.o.
- **HAIG** Zsolt: *Információs műveletek a kibertérben*. Dialóg Campus Kiadó, Budapest, 2018.
- **HERKE** Csongor: *A mesterséges intelligencia kriminalisztikai aspektusai*. BELÜGYI SZEMLE 2021/10. 1709 – 1724.o.
- **KISS** Kata Dóra: *Cyberpunk disztópiák és biohatalom a Ghost in the Shell elemzésén keresztül*. FILMSZEM 2018/4. 6 – 29.o.
- **KISS** Tibor: *A kibertér fogalma*. In: KISS Tibor (szerk.): Kibervédelem a bűnügyi tudományokban. Dialóg Campus, Budapest, 2020. 9 – 17.o.
- **KRASZNAY** Csaba: *Kiberbiztonság a XXI.században*. Katonai Nemzetbiztonsági Szolgálat, Budapest, 2022.

- **KŐHALMI** László: *Jogállam és büntetőjog – avagy kételyeim az ezredforduló kriminálj*oga körül. In: Karsai Krisztina (szerk.): Keresztmetszet. Pólay Elemeér Alapítvány, Szeged, 2005. 121 – 137.o
- Andrea **KRAUT** – László **KŐHALMI** – Dávid **TÓTH**: *Digital Dangers of Smartphones.* JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 2020/1. 36 – 49.o.
- **LILLEMOSE**, Jacob és **KRYGER**, Mathias: *The-reinvention of cyberspace* https://web.archive.org/web/20150826204717/http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/ 1.oldal.
- **MAGYARORSZÁG NEMZETI KIBERBIZTONSÁGI STRATÉGIÁJÁRÓL** szóló 1139/2013. (III. 21.) KORM. HATÁROZAT
- **MEZEI** Kitti: *A kiberbűnözés szabályozási kihívásai a büntetőjogban*. ÜGYÉSZEK LAPJA 2019/4-5. 21 – 33.o.
- **MÉSZÁROS** Rezső: *A kibertér társadalomföldrajzi megközelítése*. MAGYAR TUDOMÁNY 2001/7. 769 – 779.o.
- **MÉSZÁROS** Rezső: *A kibertér, mint új földrajzi tér*. In: KISS Andrea – MEZŐSI Gábor – SÜMEGHY Zoltán (szerk.) Táj, környezet és társadalom: ünnepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére = Landscape, environment and society: studies in honour of professor Ilona Bárány-Kevei on the occasion of her birthday. Szegedi Tudományegyetem Éghajlattani és Tájföldrajzi Tanszék – Szegedi Tudományegyetem TTIK Természeti Földrajzi és Geoinformatikai Tanszék, Szeged, 2006. 489 – 496.o.
- **MÉSZÁROS** Rezső: *A kibertér, és ami körülötte van: Társadalomföldrajzi megközelítés*. JATEPress, Szeged, 2008.
- **MORRISON**, Aimée Hope: *An impossible future: John Perry Barlow's 'Declaration of the Independence of Cyberspace'*. NEW MEDIA & SOCIETY March 5. 2015. 53 – 71.o.
- **MUHA** Lajos – **KRASZNAY** Csaba: *Az elektornikus információs rendszerek biztonságának menedzselése*. Nemzeti Közszolgálati Egyetem, Budapest, 2018.
- **MUNK** Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*. HADTUDOMÁNY 2018/1. 315 – 328.o.
- **NAGY** Zoltán: *Az informatikai bűncselekmények*. PhD-dolgozat. Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskola, Pécs, 2000.
- **NAGY** Zoltán András: *Informatikai bűncselekmények*. MAGYAR TUDOMÁNY 2001/8. 946 – 957.o.

- **NAGY** Zoltán András: *A számítógépes bűncselekmények hazai szabályozása*. In: Tóth Mihály – Gál István László (szerk.): Gazdasági büntetőjogi tanulmányok. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2005. 302 – 320.o.
- **NAGY** Zoltán András: *A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén*. BELÜGYI SZEMLE 2018/10. 36 – 55.o.
- **PARTI** Katalin – **KISS** Anna: *A számítástechnikai bűnözésről akkor és most*. In: BÁRD Petra – HACK Péter – Holé Katalin: Pusztai Lkiberászló emlékére. Országos Kriminológiai Intézet – ELTE Állam-és Jogtudományi Kar, Budapest, 2014. 297 – 310.o.
- **PARTI** Katalin – **KISS** István: *Informatikai bűnözés*. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft., Budapest, 2016. 491 – 517.o.
- **SIMON** Béla: *A kiberbűnözés aktuális trendjei*. MAGYAR RENDÉSZET 2018/1. 161 – 168.o.
- **SZABÓ** Katalin – **HÁMORI** Balázs: *Információgazdaság: Digitális kapitalizmus vagy új gazdasági rendszer?* Akadémiai Kiadó, Budapest, 2006.
- **SZÁSZ** Antónia: *A kiberbűnözés társadalmi kontextusa*. In: Kovács Janka – Kökényessy Zsófia – Lászlófi Viola (szerk.): A normán innen és túl: Tanulmányok a Történeti Kollégium konferenciájának előadásaiból. ELTE BTK Történeti Kollégium, Budapest, 2017. 95 – 122.o.
- **SZKÁLA** Károly és **MUNK** Sándor: *A KIBERTÉR FOGALMA, ÉRTELMEZÉSE ÉS FEJLŐDÉSE*. Földrajzi KÖZLEMÉNYEK 2018/4. 344 – 355.o.

Tóth Dávid* – A közösségi média és a bűnözös közötti összefüggéseket vizsgáló elméletek

1. Bevezetés

Az internet és azon belül a közösségi média egyre nagyobb szerepet játszik napról napra az emberek életében. Hatással van az emberek hírfogyasztási szokásaira, a kapcsolatokra, kommunikációra, szabadidős tevékenységekre. A világban végbemenő technológiai és globális változások kihatnak a bűnözésre is.[1] A jelen tanulmányomban ezt a közösségi média, avagy a web. 2.0 és a bűnözés közötti összefüggéseket elemzem elméleti szempontból.

2. A közösségi média térnyerése

A *DataReportal* a *We Are Social* és a *Hootsuite* társaság közös digitális jelentése[2] azt mutatja, hogy a digitalizáció továbbra is erősödik világszerte.
Az elmúlt egy évben több száz millió ember vált internet használóvá és jelentős részük a közösségi médián is megjelent felhasználóként.
A jelentés főbb megállapításait az alábbi ábra szemlélteti.

1.sz. ábra: A DataReportal Digitális jelentése 2022 júliásban az internethasználatról.

Az ábra alapján világ teljes populációja hamarosan (várhatóen még 2022-ben) eléri a 8 milliárd főt. A lakosság 66.9 százaléka rendelkezik okostelefonnal és

---

* adjunktus Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

[1] KŐHALMI László: Jogállam és büntetőjog – avagy kételyeim az ezredforduló kriminálj oga körül. In: Karsai Krisztina (szerk.): Keresztmetszet. Pólay Elemeér Alapítvány, Szeged, 2005. p. 124.

[2] https://datareportal.com/reports/digital-2022-july-global-statshot (2022. 07. 25.)

63.1 százaléka internettel. Az aktív közösségi médiát használók száma 4.7 milliárd fő, amely a világ össznépességének 59 százalékát teszi ki. Egy év alatt 178 millió új internethasználót regisztráltak, ami 3.7 százalékos növekedést jelent. Ez a növekedés még inkább tetten érhető a közösségi médián regisztrálók számában, ahol 5.1 százalékos a növekedés és 227 millió új felhasznó csatlakozott hozzájuk. A lakosság átlagosan 6 óra 49 percet tört az interneten és ezen belül 2 óra 29 percet a közösségi média felületeken, ami egy évvel korábbi állapothoz képest 6 illetve 5 perces növekedést jelentett.
Ha a lakosság 13 év feletti korosztályát nézzük a közösségi médiát használók aránya még magasabb, a föld népességének 75.5. százaléka regisztált legalább egy oldalon. A nők és a férfiak aránya 45.7, illetve 54.3 százalék.

2. sz. ábra a közössi média felhasználók aránya a világon

A fenti ábra a mutatja a közösségi média felhasználóknak a százalékos arányát a teljes lakkossághoz képest a különböző kontinenseken. A nyugati világban magasabb arányban regisztráltak a lakosságból (78-83% közötti arányban) viszont a keleti társadalmakban nagyobb lélekszámmal vannak jelen, például Indiában 2021 nyarán 416 millió 600 ezer regisztrált facebook felhasználót tartottak számon.[3] Magyarországon körülbelül 7 millió regisztrált ember található meg csak a facebookon.
Látható, hogy napjainkban mind statikus oldalról (hogy hány regisztált ember van az oldalakon) mind dinamikus oldalról (hogy milyen mértékben, módon és mennyiségben használják naponta az emberek e felületeket) meghatározó

[3] https://worldpopulationreview.com/country-rankings/facebook-users-by-country

szerepe van a közösségi médiának a jelenlegi társadalmakban, és ez hatással van a bűnözésre is.

3. A média és a bűnözés kapcsolatát vizsgáló elméletek

A kriminológia tudományában már régóta vizsgálják a média, az erőszak és a bűnözés lehetséges összefüggéseit.

3.1. A morális pánik elmélete

3.1.1. A morális pánik elméletéről általában

A média megjelenésének és elterjedésének köszönhetően ismereteink egy jelentős részét nem közvetlen forrásokból szerezzük meg. Az egyik legjelentősebb közvetett ismeretforrásunk a média lett napjainkra. A média hozzájárul a társadalmi valóságmeghatározáshoz.[4]
Ezek az állítások már a hagyományos vagy régi médiára (angol szakirodalomban ún. legacy media) is igazak voltak, de a közösségi médiára még inkább. A mesterséges intelligenciával kreált algoritmusok határozzák meg azt, hogy milyen hírek, információk jutnak el egyes emberekhez, és ez nagy befolyással bír a társadalom egészére. Ráadásul egyfajta diverzifikáció is megfigyelhető, mivel minden emberhez érdeklődése mentén is más más hír és információ jut el naponta ezzel létrehozva egy ún. buborékot, egy sajátos és egyedi információs valóságot, amellyel semelyik más ember nem rendelkezik, legfeljebb csak hasonlóval.
A média valamennyi formáján megfigyelhető a szenzációt, megbotránkozást, vagy nagy érdeklődést keltő híreknek a terjesztése, vagy előtérbe helyezése, amely elősegíti a hagyományos média nézettségét, illetve a közösségi média elérését (utóbbit szokták hívni a közösségi média kattintásvadászatának is). Így a publikum számára a hírek jelentős része deviáns viselkedéshez köthetőek lesznek és ezek könnyedén meg lehet őket személyesíteni a társadalmi problémákra, a népszerű morál nyelvezetére. Ahogy Kitzinger fogalmaz *„a morális pánik elméletének úttörői a konszenzuális valóság feletti ellenőrzés folyamatait vizsgálták egy médiatermeléssel erősen átitatott plurális társadalmi környezetben."*[5]
A szociológiai és kriminológiai kutatások mentén alakult ki a morális pánik bűnözési elmélete. A morális pánik alapja, hogy társadalom hogyan fókuszál és reagál (vagy éppen pánikol) egy bizonyos magatartásra, viselkedésre, problémára és hogyan démonizálhatnak egyes társadalmi csoportokat, akikben a felelőst látják.[6]

---

[4] KITZINGER Dávid: A morális pánik elmélete. In: Replika 2000/40. p 23.
[5] Uo.
[6] HAYES, Rebecca – M.; Luther, Kate: #Crime. Palgrave Studies in Crime, Media and Culture. Springer International Publishing. 2018. p. 15.

A morális pánik terminus technicust Jock Young használta először 1971-ben drogfogyasztásról szóló tanulmányában de Stanley Cohen 1972-ben a deviancia konstrukciójával foglalkozó kutatása tette azt széles körben ismertté. Eredetileg ezt az elméletet elsősorban a deviáns ifjúsági szubkultúrákra írták és alkalmazták, mint például a fiatalkorú rablókra, az erőszakos videókat néző gyerekekre stb.[7]

Cohen definíciója szerint morális pánikról akkor beszélhetünk, ha *„egy állapotot, történetet, személyt vagy személyek csoportját társadalmi értékeket és érdekeket fenyegető veszélyforrásként határoznak meg."*[8]

A folyamat úgy kezdődik, hogy megjelenik egy társadalmi probléma. E jelenség lényegében társadalom idealizált rendjét veszélyezteti, és a média, illetve a társadalom egy csoportot tekint a probléma eredőjének, bűnbakjának, vagy ahogy Cohen fogalmaz, népi ördögnek (folk devil). A népi ördögök szolgálnak egyfajta vizualizációs emlékezetőnek, hogy milyennek nem szabad lenni.[9] A média szenzációhajhász és szimplifikáló módon mutatja be a problémát kihegyezve a bűnbaknak kikiáltott társadalmi csoportra. A médiának e tevékenysége létrehoz egy közhangulatot, amelyre a jogalkotó jogszabályi szigorításokkal reagál. A jogszabályi változások miatt a jogalkalmazó szervek is ezek a normákat fokozott figyelemmel tartják vagy tartatják be és kriminalizálás esetén nőhet a regisztrált bűncselekmények száma ezzel pedig legimitálják a rend helyreállítása érdekében tett lépéseket. Ennek következtében a morális pánik hatással van a társadalom jogrendszerére, társadalmi rendjére, a hatóságokra, az intézményekre, és a közfelfogásra. A társadalom tagjaiban a média által leegyszerűsített valóságkép alakul ki a probléma kapcsán. A terminus technisuban a morális szó arra utal, hogy a társadalom számára problémaként felmerülő jelenség a megfigyelő értelmezésében fundamentális társdalmi értékeket érint, és az veszélyzezteti a társadalmi morált, illetve annak berendezkedését. *„A társadalmi morálon, mint szimbolikus rendszeren keresztül kerül kifejezésre az érdekek, a tradíciók és az életmód fenyegetettsége."*[10] A szakkifejezésben a pánik a jelenség intenzitását, illetve terjedését szemlélteti.[11]

Jewkes szerint a morális pániknak öt fontos jellegzetessége van:

1. Morális pánik akkor követhezhet be, ha a média egy hétköznapi történtést szenzáció jelleggel mutat be.
2. A média ezzel a tevékenységével beindít egy *„devancia erősítő spirált."*Ezen belül egy morális diskurzus jön létre újságírók és

[7] Uo.
[8] COHEN, Stanley: Folk devils and moral panics. Third edition Routledge, London-New York. 2002. p. 1.
[9] COHEN (2002) p. 2.
[10] KITZINGER (2000) p. 24
[11] Uo.

más hatóságok, véleményvezérek és erkölcsi szereplők által, akik együttesen démonizálják a vélt helytelen cselekvőket, ezzel fokozva az erkölcsi hanyatlást.
3. A morális világossá teszi az erkölcsi határokat a társadalomban, és ezzel konszenzust, illetve aggodalmat is kelt.
4. A morális pánik a gyors társadalmi változások időszakában szokott megjelenni.
5. A morális pánik általában a fiatalokat célozzák meg, mivel ők a jövő metaforája, viselkedésüket pedig barométernek tekintik, amellyel egy társadalom egészségét vagy betegségét tesztelik.

Jewkes tételei szerint a média a morális pánik fő mozgatórugója, de a közösségi médiával az irányítás a fiatalabb generációk (és azon belül különösen a fiatal felnőttek) felé billen, ami a régi médiában nem volt jelen. [12]

3.1.2. Miként jelenik meg a közösségi médián a morális pánik?

Milton Mueller szerint a közösségi média az emberek közötti interakciókat, a hipertranszparanssé teszi és sok esetben a felelősséget az elkövetők az őket elérhetővé tevő platformokat teszi feleősség. Ez a hipertranszparencia előmozdít egy morális pánikot a közözzégi média kapcsán. Csak úgy, mint a régi média esetén, itt is megfogalmazódnak olyan vádak, hogy a közösségi média elősegíti a terrorizmust, az extrémizmust, hozzájárulhat etnikai tisztogatásokhoz, választásokat befolyásolhat és tönkreteheti a demokráciát. A morális pánik pedig a közösségi médiát helyezi a probléma eredőjévé. Bűnözési aspektusból a problémaköröket emeli ki:

- Rémhírterjesztés (fake news)
- Extrémizmus, terrorizmus elősegítése,
- Rasszizmus fokozása, és különböző etnikum elleni verbális és erőszakos fellépések elősegítése.[13]

Mueller tehát rámutat arra, hogy a közösségi média körül is megjelenik a morális pánik, de emellett annak egyik eszköze is, csak úgy mint a régi média is az.[14]

Garland szerint egy jelentős elmozdulás van a morális pánik jelenségtől a kulturális háborúk irányába (vagy más néven szimbolikus politizálás). Meglátása szerinte manapsága egy magatartás jelentése és értékelése egyre inkább vitatott lesz és a hatalmi egyensúly a versengő csoportok között

[12] HAYES, Rebecca – M.; Luther, Kate: #Crime. Palgrave Studies in Crime, Media and Culture. Springer International Publishing. 2018. p. 15. hivatkozza: Jewkes, Yvonne Media and crime. Key Approaches to Criminology. London, UK: Sage. 2004. p. 19

[13] MUELLER, Milton. „Challenging the social media moral panic: preserving free expression under Hypertransparency." Cato Institute Policy Analysis 876 (2019).

[14] Uo.

kevésbé lesz asszimetrikus. Erre példaként hozza az elmúlt években megfigyelhető kihívásokat az illegális migráció és a jogi reform kapcsán, vagy a muzulmán nők hijab viseletének kérdése az iskolákban, amelyek kezdetben morális pánikként jelentkeztek és végül politikailag vitatott kulturális háborúvá váltak.[15] Cohen egyébként 2011-ben egyik tanulmányában is azt prognosztizálta, hogy a menekült, és migráns problémakör a morális pánik narratívájába fognak kerül. Ez mind Európában és az Egyesült Államokban is tetten érhető volt az elmúlt években. A muzulmán bevándorlók ebben a szemléletben az új népi ördögök.[16]

Garland szerint a kulturális háború kialakulásának két oka van. Egyrészt a jelenlegi társadalomban megfigyelhető egy fragmentáció és heterogenitás, másrészt pedig a média is proliferálódott, amely magába foglalja a közösségi médián keresztüli terjesztést is, amely most sokkal több alternatív ellenállási helyszín létrehozását teszi lehetővé a helyzet domináns definícióinak megkérdőjelezésére Itt a fentebb kiemelt „polgári újságírás" megjelenése és a közösségi média növekvő használata növeli a tiltakozás és ellenállás lehetőségeit: kibővíti az alternatív kollektív hangok meghallgatásának és üzeneteinek terjesztésének eszközeit.[17]

Giulliani, Garraio és Santos tanulmányában a digitális média szerepét vizsgálták a migrációval kapcsolatos „szexuális morális pánik" felerősítésében. Olaszországban és Németországban bekövetkezett tanulmányok elemzésén keresztül arra az álláspontra jutottak, hogy a digitális média nagy mértékben hozzájárult az inváziótól és a szexuális bűncselekményektől való félelmek kialakításához és terjesztéséhez és azok új rasszista indíttatású bűncselekményeket szültek. Az egyik jogesetben, 2018 januárjában Pamela Mastropietro-t, egy 18 éves nőt erőszakolt majd ölt meg Macerata városában három nigériai migráns. Az áldozat testrészeit fel is darabolták és zsákokban probálták Maceratan kívül eltűntetni. Mindhárom elkövetőt elfogták és életfogytig tartó szabadsávesztésre ítélték 2019 májusában.

A bűncselekményeket a szélsőjobboldali csoportok gyűlőletre uszításra használták fel. A közösségi médián megjelenő morális pánikot jól szemlélteti Salvini facebook posztja, amelyben az illegális migránsok tömeges kiutasítását, kémiai kasztrációt követelte, amely több mint 34 ezer tetszik gombot és majdnem 3700 megosztást ért el a facebookon. A több, mint 4500 kommentelő jelentős része halálbüntetést követelt az elkövetőkre nézve. Ezt követően 2018 februárjában Luca Traini egy szélsőjobboldali elkövető hat

[15] MARTIN, Greg. *Crime, media and culture*. Kindle edition. Routledge, New York. 2019. p. 68.

[16] COHEN, S. . Whose side were we on? The undeclared politics of moral panic theory. Crime, Media, Culture: An International Journal, 2011/3. pp. 237–243.

[17] MARTIN (2019) p. 74.

fekete embert lőtt le az autójából, azt kiáltva, hogy *Viva l'Italia* (éljen Itália). Traini állítása szerint a cselekményét a Mastropietro ellen elkövetett bűncselekményért való bosszúállás motiválta.[18]

3.2. A bűnözéstől való félelem

Korinek László tanulmányában megállapította, hogy a bűnözéstől való félelem egyre nagyobb méreteket ölt a tömegtájékoztatás korában. A média nem megfelelő bűnözésábrázolása befolyásolja a lakosság életvitelét, nő a társadalmi bizonytalanság, illetve a nyilvános intézményekkel szembeni bizalom hiánya. További negatív következménye a szociális dezintegrációs és a közösség széthullása.[19] A nyugati demokráciákban végzett kutatások azt mutatják, hogy az emberek félnek a bűnözéstől, és ez befolyásolja negatív irányva a biztonságérzetüket és a jólétüket. A vizsgálatok alapján a bűnözéstől való félelem nem áll arányban bűnözés valódi mértékével. Az előbb említett morális pánik folyamatok is tovább gyengítik az emberek biztonságérzet és növeli az aggodalmukat. Ez fokozottan igaz, ha bekövetkezik egy terrortámadás az országban. A bűnözéstől való félelmet a régi médiával kapcsolatban a televíziózási szokásokkal mérték. Azok, akik sokkal többet néztek TV-t sokkal azoknál nagyobb volt a bűnözéstől való félelem.[20]
Az új médiával kapcsolatban Intravia és mások[21] végzett egy kutatást. Fiatal felnőttek internethasználatával kapcsolatban vizsgálták a bűnözéstől való félelem jelenségét. Az anonim kérdőíves kutatást három egyetemi campusban végezték 2016 ősz és 2017 tavasza között. A bűnözéstől való félelmet úgy mérték, hogy megkérték a válaszadókat, hogy jelezzék a félelem szintjét (0-tól egyáltalán nem fél , 10-ig = nagyon fél) az alábbi hat bűnözéssel kapcsolatos eseményre:

- valaki behatol az otthonába,
- kirabolják az utcán,
- szexuális zaklatás / erőszak történik vele
- ellopják az autóját, kerékpárját
- idegenek megverték vagy megtámadták,

[18] SANTOS, Sofia José – Júlia Garraio – Gaia Giuliani: Online social media and the construction of sexual moral panic around migrants in Europe. In: Socioscapes. International Journal of Societies, Politics and Cultures 2019/1: pp. 155-174.
[19] KORINEK, László, A bűnözéstől való félelem és a tömegtájékoztatás. In: Belügyi Szemle 1989/4. pp. 31-38. p. 37.
[20] HALE, Chris: Fear of crime: A review of the literature. In: International Review of Victimology 1996/2. pp. 79–150
[21] INTRAVIA, J. – WOLFF, K. T. – PAEZ, R., – GIBBS, B. R.: Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. In: Computers in Human Behavior. 2017. pp. 158-168.

- vagy meggyilkolják.

Adataikkal kapcsolatban fontos megjegyezni, hogy a médiafogyasztás és a bűnözéstől való félelem közötti kapcsolat kölcsönös természetű lehet. Vagyis azok az egyének, akik jobban félnek a bűnözéstől és az erőszaktól, motiváltabbak lehetnek a médiatartalom felé fordulni, hogy megtanulják, feldolgozzák és megértsék a bûnözéssel kapcsolatos kérdéseket (Eschholz et al., 2003). Eredményeik alapján azt a következtetést vonták le, hogy a közösségi média rendszeres használata szignifikánsan összefügg bűnözéstől

3.2. Új elmélet – a Web. 2.0 teória.

Yar foglalkozott egy új teóriával az ún. Web 2.0-val. Rámutatott arra, hogy hogy az internet folyamatosan változó természete valószínűleg hatással van a bűnözésre és az áldozattá válásra. Az internetet úgy kell felfogni, mint egy *„technológiailag támogatott társadalmi gyakorlatot.”*[22] Az internetet az emberek a társadalomban való működésre használják, így gyakorlat a társadalmi konstrukciónak az egyik része. A Web 2.0 elmélet is rámutat arra, hogy az internet újfajta társadalmi és bűnözési problémákat hoz létre.
Például Az internet és a közösségi média lehetővé teszi lehetővé, hogy „szexuális ragadozók” és pedofilok könnyebben kiszemeljek a kiskorú áldozatukat. Yar viktimológiai oldalról vizsgálja a kérdéskört, szerinte a fiatalok közösségi média platformjain keresztül könnyen manipulálhatóak és olyan információkat tesznek ki magukról, amely növeli a sebezhetőségüket.[23]
Az elmélettel összhangban korábbi tanulmányban is rámutattam arra, hogy a közösségi médián új bűnözési formák jelenhetnek meg.[24]

4. Összegzés

A kutatás alapján összegezhető, hogy a közösségi média befolyása a társadalmi életviszonyokra jelentős. A közösségi média és a bűnözés kapcsolatait lehet vizsgálni a régi médián végzett elméleti megközelítésekkel, mint a morális pánik teóriával, vagy a bűnözéstől való félelem kutatásokkal. A régi médiához képest az új média globálisabb, könnyebben elérhető, gyorsabb és interaktív kommunikációs forma. Az elméleti megközelítések is hangsúlyozzák, hogy a

[22] YAR, Majid: E-Crime 2.0: the criminological landscape of new social media. In: Information & Communications Technology Law 2012/3. p. 207.
[23] YAR (2012) p. 210.
[24] TÓTH Dávid: The correlations between social media and crime. In: Garayová, Lilla Budúcnosť práva – Právo budúcnosti II. Zborník príspevkov z online vedeckej konferencie - The Law of the Future – The Future of Law II. Conference Proceedings. Paneurópska vysoká škola, Fakulta práva, Bratislava. 2022. pp. 149-164. ,

közösségi médián új bűncselekmények jelennek meg (pl.: cyberbullying). Másik oldalról a bűnelkövetők könnyebben találhatnak motívumot, felbujtást arra, hogy hagyományos bűncselekményeket kövessenek el.
Véleményem szerint a morális pánik elméletével végzett kutatások hatékonyan bemutatják, hogy a társadalomban mindig is jelen volt egyfajta bűnbakkeresési mechanizmus. Ez a közösségi médián még fokozottabban jelenik meg, mint ahogy láttuk az olasz jogeseten keresztül. Szemben a hagyományos médiával az ilyen indulatgerjesztő narratívákkal szemben az új médián nehezebb felvenni a harcot, mivel sokkal decentralizáltabb jelenségről van szó. A szolgáltatóknak felelőssége van és lesz a jövőre nézve, hogy az ilyen jellegű csoportokat, kommenteket és embereket kiszűrje a platformokról. A mesterséges intelligenciák és algoritmusok fejlődésével bízhatunk, hogy az ilyen jelenségeknek a száma csökkeni fog a jövőben.

Irodalomjegyzék

- **COHEN, S.**: "Whose side were we on? The undeclared politics of moral panic theory." *Crime, Media, Culture: An International Journal,* 2011/3.
- **COHEN, Stanley**: *Folk devils and moral panics.* Third edition, Routledge, London-New York, 2002.
- **HAYES, Rebecca M. – Luther, Kate**: *#Crime.* Palgrave Studies in Crime, Media and Culture. Springer International Publishing, 2018.
- **INTRAVIA, J. – WOLFF, K. T. – PAEZ, R. – GIBBS, B. R.**: "Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults." *Computers in Human Behavior,* 2017.
- **JEWKES, Yvonne**: *Media and crime.* Key Approaches to Criminology. London, UK: Sage, 2004.
- **KITZINGER, Dávid**: *A morális pánik elmélete.* In: *Replika* 2000/40.
- **KORINEK, László**: *A bűnözéstől való félelem és a tömegtájékoztatás.* In: *Belügyi Szemle* 1989/4.
- **KŐHALMI LÁSZLÓ**: Jogállam és büntetőjog – avagy kételyeim az ezredforduló kriminájloga körül. In: Karsai Krisztina (szerk.): Keresztmetszet. Pólay Elemeér Alapítvány, Szeged, 2005.
- **MARTIN, Greg**: *Crime, media and culture.* Kindle edition, Routledge, New York, 2019.
- **MUELLER, Milton**: "Challenging the social media moral panic: preserving free expression under Hypertransparency." *Cato Institute Policy Analysis* 876 (2019).
- **SANTOS, Sofia José – Garraio, Júlia – Giuliani, Gaia**: "Online social media and the construction of sexual moral panic around migrants in Europe." In: *Socioscapes. International Journal of Societies, Politics and Cultures* 2019/1:
- **TÓTH, Dávid**: "The correlations between social media and crime." In: *Garayová, Lilla (szerk.): Budúcnosť práva – Právo budúcnosti II. Zborník príspevkov z online vedeckej konferencie - The Law of the Future – The Future of Law II. Conference Proceedings.* Paneurópska vysoká škola, Fakulta práva, Bratislava, 2022.
- **YAR, Majid**: "E-Crime 2.0: the criminological landscape of new social media." In: *Information & Communications Technology Law* 2012/3.