Biztonság és jog konferenciakötet

PTE-ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

Pécs, 2022.

Biztonság és jog
Konferenciakötet

Szerkesztőbizottság:

Kőhalmi László
Kulcsár Gabriella
Tóth Dávid
Gáti Balázs
Sándor Enikő

Kiadja: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Kriminológiai és Büntetés-végrehajtási Jogi Tanszék
7622 Pécs, 48-as tér 1.

Felelős Kiadó: Prof. Dr. Fábián Adrián dékán

Digitális ISBN: 978-963-429-845-8

Pécs, 2022.

Tartalomjegyzék / Table of content

Előszó

Mindig is jelentős tudományos teher nehezedett azon kutatókra a társadalomtudományok terén, akik a „biztonság” – mint általános koncepció fogalmát - gazdasági, jogi, vagy iparági, szűk körben értelemezett szakmai szempontok alapján kívánták meghatározni.

A jogtudományok területén a biztonság hiánya számos álláspont szerint egyfajta fenyegetést, veszélyt, kárt, hátrányt jelent, így maga a „biztonság” egy sajátos védelmi, konzervációs állapotot testesít meg. Így az értelmezés terén a joggyakorlatban gyakran alkalmazott ún. negatív megközelítés szolgálhat kiindulópontként tekintettel arra, hogy a biztonság fogalma legegyszerűbben annak hiányán keresztül értelmezhető. Figyelemmel a jogi értelemben vett biztonság multilaterális jellegére, ahogyan a gazdasági -, úgy szükségszerűen a jogi érdekek esetleges sérelme sem zárható ki teljes mértékben, tekintettel a fogalom relatív jellegére.

Ugyanakkor az ember, mint jogalany biztonságát holisztikus megközelítéssel a személyét, valamint anyagi javait érő valamennyi fenyegetést és sérelmet figyelembe vevő, egymásra épülő megközelítés útján lehetséges értelmezni.

A negyedik ipari forradalom következtében a fentiek alapján vett biztonság kérdésköre új dimenzót jelentve számottevő mértékben az online térben jelenik meg. Dinamikáját tekintve e kérdéskör - az információs-kommunikációs technológiák fejlődésével, különösen a jelenlegi COVID-19 okozta pandemiás helyzet kapcsán bekövetkezett változások okán – a korábbiakhoz képest jelentősen felgyorsult. A jelenlegi tudományos, műszaki és gazdasági fejlődés szintje, az ún. „state of art” új igényeket és jelenleg még nem ismert kockázatokat, kihívásokat generál.

A konferencia 2020. december 8-án a fent részletezett aktualitásokra figyelemmel a Pécsi Tudományegyetem Állam-és Jogtudományi Kar

Kriminológia és Büntetés-végrehajtási Jogi Tanszéke által került megszervezésre a biztonságpolitika területén folytatott kutatási munka hagyományának további ápolásaként.

Az előadások anyagát jelen kötetünkben az Olvasó szíves figyelmébe ajánljuk.

Prof. Dr.habil. Kőhalmi László

Szerkesztő

Aleksander Wróbel* - Paradox of protective measure in the form of pharmacological therapy in Polish system in comparative perspective

1. Introduction

Polish law knows various types of compulsory measures. The list of compulsory measures is regulated in Article 93 a § 1[1] of the Polish Penal Code (PPC) and is the following:

1) Electronic control of the place of the stay regulated in article 93e
2) Therapy regulated in Article 93f § 1
3) Addiction therapy regulated in Article 93f § 2
4) Psychiatric detention regulated in § 93 g

In this work, the attention would be given only to a singular compulsory measure in the form of therapy and within its frames so-called pharmacological therapy. This institution is relatively new to polish law, still, from the very beginning, it caused a lot of controversies. In its current form, it is one of the examples of systemic paradoxes in the Polish law. Even though the institution is imprinted into law in fact without the cooperation of the culprit. The sole purpose of the measure prescribed in the law is that it should lower the libido of the offender in order to prevent future sexual crimes towards minors. The work aims to answer the question, whether the measure of pharmacological therapy can be labelled as compulsory measure and whether in fact, it has a place in criminal law.

---

* Senior Lecturer LL.M. Uppsala University, University of Czestochowa

[1] § 1. The protective measures are:
1)electronic monitoring of a person's location,
2)therapy,
3)addiction therapy,
4)placement in a psychiatric facility.
§ 2. If a statute provides so, the court may impose the order and prohibitions provided for in art. 39 sections 2-3 as protective measures.

2. Historical background.

Compulsory measure in the form of pharmacological therapy was introduced into polish criminal law in the year 2005 with the adoption of the law from 27th of July 2005 on the amendment of the Criminal Code and Criminal Penitentiary Code[2]. An incentive for such a solution was to prevent the criminal activity of the sexual offenders and to provide a compulsory measure adjusted to the needs of this category of the culprits. Prior to this amendment, the treatment of this category of offenders was possible with simultaneous symptoms of the mental illness enabling imposing the measure of psychiatric detention[3].

At this point, another regulation has numerous flaws among which was the absence of the details concerning the procedure of implementation of the measure, the place where the offender should be treated. Over and above, due to the post-punishment character, heated discussions accompanied the novelty. The worries were whether this measure is violating basic human right principles imprinted into international law and Constitution of Poland from 27th July 2005[4][5].The measure has undergone amendments in the year 2009[6] and in 2015[7], which have shaped the binding form of the institution.

3. Pharmacological therapy – present solution.

Current standpoint adopted in PPC from 1997[8] is imprinted in Article 93f and is called "therapy". As it was mentioned the measure has and had negative cognizance in the

[2] Ustawa z dnia 27 lipca 2005 r. o zmianie ustawy - Kodeks karny, ustawy - Kodeks postępowania karnego i ustawy - Kodeks karny wykonawczy, Dz.U. 2005 nr 163 poz. 1363.
[3] Piotr *Góralski .Środki zabezpieczające w polskim prawie karnym*,(Warsaw 2015), 448.
[4] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz.U. 1997 nr 78 poz. 483
[5] Stanowisko Rządu w sprawie poselskiego projektu ustawy o zmianie ustawy Kodeks karny i kodeks karny wykonawcz (druk nr 2693).
[6] Ustawa z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy Kodeks karny skarbowy oraz niektórych innych ustaw (Dz. U. z 2009 r. Nr 206, poz. 1589).
[7] Ustawa z dnia 20 lutego 2015 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz.U. 2015 poz. 396).
[8] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny., Dz.U. 1997 nr 88 poz. 553.

literature of the subject[9]. It's aimed at the treatment of individuals who are in a state of mental disorder or personality disorders and delinquents suffering from disorders of sexual preferences. It can take the form of in and outpatient treatment[10]. Notwithstanding, starting from the mentioned reform of criminal code of 2015, the wording of Article 93f § 1[11] was changed; as a consequence, an offender must report to a court-designated facility on days designated by a psychiatrist, sexologist or therapist. It purports that an individual can be compelled to undergo out-patient treatment in the form of therapy. Since the locution points to an open form of treatment, this is a configuration which can be executed on an obligatory basis[12]. Nonetheless, in fact, out-patient therapy can arise only voluntarily, and it seems to be the crux of the problem[13].

The self-same is when an offender agrees to undergo pharmacological treatment with the different objective, that of decreasing the libido of the perpetrator[14]. The desired result in the PPC of the therapy measure for the sexual offenders is to eliminate the danger of committing a crime in future, which has its origins in the already-committed crime and the state of the delinquent. Concomitantly, the enactment of therapy consists of therapy for the offender with the aim of protecting society from the future danger of committing crimes alike[15].

---

[9] Ewa Weigend, Joanna Długosz., *Stosowanie środka zabezpieczającego określonego w art. 95a § 1a k.k. w świetle standardów europejskich. Rozważania na tle wyroku ETPC z 17 grudnia 2009 r. w sprawie M. v. Niemcy, (*Czasopismo Prawa karnego i nauk penalnych Rok XIV: 2010, z. 4,) . 54.

[10] Krzysztof Krajewski ,*System Prawa Karnego, T. 7, komentarz do artykułu 93f, pp.* 6-8.(wersja elektroniczna).

[11] *§ 1. The perpetrator with regard to whom therapy has been ordered is obliged to report at a court-designated facility on days designated by a psychiatrists, sexologist or therapist and submit himself to pharmacological therapy aimed at decreasing his libido, psychotherapy or psychoeducation with the purpose of improving his social functioning.*

[12]Małgorzata Pyrcak-Górowska , in: Wróbel Włodzimierz (red.),Zoll Andrzej (red.)., *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 53-116,* (Warsaw 2016), 786-787.

[13] Piotr Zakrzewski, in. Wróbel Włodzimierz (red.), *Nowelizacja prawa karnego 2015. Komentarz.* (Kraków 2015), 705.

[14] Ibidem

[15] Piotr Zakrzewski, in. Wróbel Włodzimierz (red) *Nowelizacja prawa karnego 2015. Komentarz.* (Kraków 2015), 706.

The construction of the therapy is versatile since within it the following treatments can be enacted: psychiatric therapy and pharmacological therapy aimed at decreasing libido[16]. The form of the treatment is determined by the therapist at the execution stage of the measure. This attitude was elucidated by the need for constant adjustment of the treatment to the development of medicine and psychology[17]. The measure aims at preventing the committing of a crime caused by the aberration of sexual preferences through decreasing the libido. Still, there is a certain constraint on situations where pharmacological therapy can't be risked – when pharmacological therapy could lead to danger to the health or life of the offender[18].

One of the first constraints imprinted into the PCC that pertains to this measure is that in order to be admitted to the therapy the perpetrator has to commit one of the crimes enumerated in Art. 93c point 3[19]. As a matter of fact, the measure of therapy is enacted after the sentence of punishment, hence the person has to be sentenced for one of the crimes. To give an example this is a crime of murder, crime of engaging in sexual intercourse or another sexual activity with a minor under 15 years of age etc.

The court, according to Article 93d § 3, develops a prognosis stating whether therapy after discharge will be needed six months before the predicted discharge from the imprisonment facility[20]. This solution has its practical foible since when the court issues a decision to send an individual to therapy after release from prison or the detention facility, the person won't be discharged since his or her state implies the need for continuance of imprisonment or detention. In this state of affairs, the decision

[16]Małgorzata Pyrcak-Górowska , in: Wróbel Włodzimierz (red.),Zoll Andrzej (red.)., *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 53-116,* Warsaw 2016), 789; Igor Zgoliński ., *Komentarz do art. 93 (a) Kodeksu karnego,* stan prawny 2018.08.01, electronic source, Lex.

[17] Piotr Zakrzewski, in. Wróbel Włodzimierz (red.), *Nowelizacja prawa karnego 2015. Komentarz.* (Kraków 2015) 701-702.

[18] Piotr Zakrzewski, in. Wróbel Włodzimierz (red.), *Nowelizacja prawa karnego 2015. Komentarz.* (Kraków 2015), 704.

[19] *3) who has been sentenced for a crime provided for in art. 148, art. 156, art. 197, art. 198, art. 199 § 2 or art. 200 § 1, committed in relation to his aberration of sexual preferences,* … Penal Code Dz.U.2018.1600-translation, lex.

[20]Michał Królikowski,"Środki zabepzieczające" in: ed. Paweł Wiliński *Obrońca i pełnomocnik w procesie karnym po 1 lipca 2015 r. Przewodnik po zmianach*, electronic source, Lex system.

of the court should be null and void[21] and issued again in the period of six months before the release from the facility.

4. Criticism of the compulsory measure of pharmacological therapy.

In the Polish legal realm, the measure from Article 93a point 3 was and is widely deprecated due to the effects of the medicine used in the process of treatment. In reality, the medicine prescribed can have side-effects, such as loss of hairiness, gynecomastia, skin sagging, etc.[22] As a result, it is accepted that the measure cannot be imposed on a delinquent if it can cause danger to the life or health of the individual. Concomitantly, it is hard to imagine a situation in which a doctor would force the patient to take this kind of medication without the latter's approval[23]. Moreover, the therapy can also include a schedule of psychotherapy or psychoeducation. Most opinions propound an outlook that these methods should be amalgamated to be most efficacious[24]. The aforementioned outlook is asserted by the "*Recommendations of the state consultant in the field of sexology concerning the treatment of offenders with sexual preference disorders*"[25]. It implies that the process of therapy consists of various types of action, comprised of the application of drugs leading to a decrease in testosterone, but also work on the mental state of the offender through group meetings and additional exercises.

In the event that a patient is not fulfilling the obligations put upon him or her as a part of the therapy, he or she can be submitted to closed treatment according to Article 93d

[21] Małgorzata Pyrcak-Górowska , in: Wróbel Włodzimierz (red.),Zoll Andrzej (red.)., *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 53-116,* (Warsaw 2016), 775.
[22] Aneta Wilkowska-Płóciennik . in: Ryszard A.Stefański., *Kodeda karny. Komentarz.* 2018, Komentarz do artykułu 95a, electronic source, system Legalis; Marek Mozgawa.M., *Komentarz aktualizowany do art. 93 (f) Kodeksu karnego, stan prawny* 2018.11.15, electronic version, LEX system.
[23] Krzysztof Krajewski , *System Prawa Karnego, T. 7, komentarz do artykułu 93a*,. 113-114.
[24] Krzysztof Krajewski K , *System Prawa Karnego, T. 7, komentarz do artykułu 93a, .* 26.
[25] Zbigniew Lew-Starowicz, Alicja Przyłuska-Fiszer i Jarosław Stusiński , *Normy I kontrowersje etyczne w seksuologii, anex 1,* (Gdańsk, 2015),. 331

§ 6[26]. If the patient would be placed again under one of the measures, the choice of the measure depends on the primal measure. Thus, if the individual is discharged from in-patient psychiatric detention, he or she could be resubmitted to this type of measure. Still, if the measure is embodied in out-patient treatment, the measure to which the person can be placed would be one of the out-patient measures, such as electronic monitoring of a person's location, etc.

The question that arises is whether a delinquent who is placed into in-patient treatment can undergo pharmacological treatment aimed at decreasing libido. The answer should be positive, since the aim of in-patient detention is the treatment of the patient, whereas the goal set by the legislator to pharmacological treatment is to decrease the libido and to protect society from the perpetrator's possible future return to crime by eliminating such factors as depression, *et cetera*. This aim is pursued by eliminating or suppressing the symptoms of the personality disorder that manifests in the unnatural appeasement of sexual urges by the patient[27].

A different interpretation would open the way for a situation in which the measure would be empty, since it would produce offenders with decreased testosterone, but still with a mental ailment and the need to satisfy their urges. At the end of the day, it would ameliorate the frustration and mental problems.

Going further, the concept of pharmacological therapy from Article 93f § 1 is inseparably connected with the consent, of the individual to undergo therapy since the consent of the patient is needed for this to be enacted. Still, without consent the measure becomes an empty shell, because it is enough that the individual comes to the medical facility, stays there for a few minutes, and goes home. Having done that, he or she would meet the conditions of the therapy.

The measure of therapy together with its voluntary basis at the execution stage leads up to the evident conclusion that PPC can abstain from the measure of so-called "chemical castration". The only rationalization for the measure is its sociological

[26]Małgorzata Pyrcak-Górowska , in: Wróbel Włodzimierz (red.),Zoll Andrzej (red.)., *Kodeks karny. Część ogólna. Tom I. Kome tarz do art. 53-116*, (Warsaw 2016), 791.

[27] Adam Strzelec ,"Przymusowe leczenie sprawców czynów zabronionych popełnionych w związku z zaburzeniami preferencji seksualnych," , in: *Konteksty prawa i praw człowieka*.ed. Zyta Maria Dymińska, (Kraków 2012) 59.

aspect: the message to society that the legislator is counteracting the existence of paedophilia.

The special attempts to solve the problem of the need for cooperation on the part of the wrongdoer were furnished by Article 244b § 1[28], which provides criminal liability for failing to fulfil the duties arising from the protective measure imposed by the court on an offender. The role of the article is purely technical, seeing as it wasn't even commented on in the 2015 proposal of amendments[29]. The article was initially criticized, in view of the fact that it is also punishing the individual for not undergoing the therapy. It was put forward in the literature that the mentioned category of patients should not be punished; on the contrary, they need further help[30]. Simultaneously, the issue of voluntariness of treatment was further developed by the Constitutional Tribunal in case OTK-A 2006[31], where the Tribunal adopted the position that dissent from undergoing the therapy is not unlawful behaviour. When combined with the wording of Article 93f § 1, it would be criminally relevant should an occasion arise when an individual did not show up at the place indicated by the court[32], hence Article 244b, from a strictly pragmatic position, does not provide a system of implementation of the therapy.

A different aspect is a serious doubt as to whether Article 244b § 1 is consistent with the basic principles of the Constitution of Poland such as *ne bis in idem* and Article 30 of the Constitution, guaranteeing the respect to the dignity of the human being, and the proportionality principle from Article 31 § 3 of Constitution[33]. Due to the above-

[28] *Whoever fails to comply with statutory duties arising from the protective measure that has been imposed on him, is subject to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty for up to 2 years.*

[29] Witold Zontek ,in: Włodzimierz Wróbel (red) , *Nowelizacja prawa karnego 2015. Komentarz.* (Kraków 2015), . 846.

[30] Witold Zontek., *Kara za brak poddania się terapii? Konsekwencje wprowadzenia art. 244b k.k.*, (Palestra, 7-8/2015), 125.

[31] OTK-A 2006, nr 7, poz. 78, Decision from 4 lipca 2006 r.

[32] Witold Zontek , *Kara za brak poddania się terapii? Konsekwencje wprowadzenia art. 244b k.k.*, (Palestra, 7-8/2015), 129.

[33] Opinia Helsińskiej Fundacji Praw Człowieka o ustawie z dnia 15 stycznia 2015 r. o zmianie ustawy - Kodeks karny oraz niektórych ustaw source: https://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/dokumenty/konsultacje/809/809_hfpc.pdf accessed on the 10.02.2021; Witold Zontek ,in: Włodzimierz Wróbel (red) , *Nowelizacja prawa karnego 2015. Komentarz.* (Kraków 2015), . 853.

mentioned constitutional concerns, the outlook is that the punishment for this crime can be imposed only on the patient who doesn't report to the medical facility on the days designated by the psychiatrist, sexologist or therapist. It is evident that if the patient refuses to undergo therapy, it should not entail meeting the requisites from Article 244b by the act[34].

The mentioned frame of reference leads to the conclusion that the Polish legislature has constructed a system in which pharmacological therapy is in practice unenforceable without the consent of the patient, and it is not pertinent whether it is in the PCC or in other acts.

5. Comparative perspective.

In order to understand what a possible solution to the Polish hardship can be, the Author studied two countries one of which adopted the pharmacological therapy, nevertheless it was annulled and country, which considers adoption of this compulsory measure. The first mentioned legal system is Swedish one and the second is Ukrainian legal system.

The Swedish legal system is a great example of the country, which has an institution of castration and sterilisation in its system for almost 40 years. First law allowing castration and sterilization of particular offenders was adopted on the 1st of January 1935. Based on the Law, the feeble-minded and insane offenders could be sterilized or castrated even without their consent, originating in the decisions of boards consisting of doctors[35]. In 1934 the Law was implemented with the measure of castration and sterilization of the sexual offenders. The new proposal was comprised of a solution according to which compulsory castration or sterilization could be

[34] Maria Szewczyk , Adam Wojtaszczyk , Witold Zontek., in: Włodzimierz Wróbel , Andrzej Zoll., *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 212-277d (cz. 2)*, commentary to article 244b (electronic version, Lex).

[35]Kinberg O., "Criminal Policy in Sweden during the last 50 years*.", Journal of Criminal Law and Criminology*, vol. 24, Art. 21, Issue 1, 1933.

brought into effect to the individuals put down to their "*disrupted mental activity*"; thus, the circle of subjects of sterilisation was quite extensive[36].

Starting from the 1st of July 1944 the new law was adopted, which made also possible to castrate or sterilize sexual offenders. The decision on castration or sterilization was made by the doctors at the first stage and at the second stage by the special board of doctors in order to protect doctors from reapproval from patients or society. Approximately 100 sexual offenders were castrated or sterilized, 13 were castrated because they were sexually aggressive but did not commit a crime, 13 were castrated based on their own will because of their sexual urge[37]. The law was repelled from the Swedish system starting from 1975. During the period of its validity up to 63.000 people were castrated or sterilized[38].

Contemporary Swedish criminal law does not encompass a specialized measure of castration or sterilization. Still, one should answer the question, whether the pharmacological castration can be carried out in the framed of other existing measures. After thorough analysis of Swedish Penal Code 1962[39] (swe. *Brottsbalken*) (BrB), an institution, which at a certain point enables the possibility of treatment of the sexual offenders is an institution of "contract care" (swe. *kontraksvård*). It was implemented into BrB in the year 1988. The idea was to provide an instrument, which will allow court to have more control over the process of [40]. It is regulated within frames of two Chapters, the first of them is Chapter 28 § 1, 4, 6a and 6b and the second - Chapter 30 § 9[41].

---

[36] Roger Qvarsell, *Utan vett och vilja. Om synen på brottslighet och sinnesjukdom.,* (Stockholm 1993) . 311-313.

[37] Roger Qvarsell R., *Utan vett och vilja. Om synen på brottslighet och sinnesjukdom.,* (Stockholm 1993), 315-316.

[38]Steriliseringsfrågan i Sverige 1935 - 1975 Historisk belysning - Kartläggning - Intervjuer (SOU 2000):20,. 16.

[39] The translation adopted after the official translation DS 1999:36.

[40] Anna Gillblom , Karin Kihlberg , *Tvingad av fri vilja Upplevelser av kontraktsvård, motivation och relation ur ett förändringsperspektiv,* (Göteborg 2007), 3. source: https://gupea.ub.gu.se/handle/2077/9419 accesed on 10th of May 2019.

[41] Martin Borgeke , *At bestemma påföljd för brott,* (Stockholm, 2012), 378.

The starting point of sentencing to the contract care is that a court, according to Chapter 30 § 4[42] of BrB would come to closure that the appropriate punishment would be imprisonment up to two years of imprisonment. After this, if the court can analyze the circumstances of the case and decide whether there is a place for contract care[43]. Concomitantly, when constructing the plan of treatment, its conditions ought to correspond, meaning – the period of the treatment, to the period of the initial punishment of imprisonment[44].

As it was already stressed out, the contract care is at its core the measure created for addicts. Nonetheless, it also could be enacted in situations when there was a need for treatment of different mental ailments such as, i.e. exhibitionism or incest. Hence, it could be a mental state, which was not severe, as an outcome an offender could not be sent to the forensic psychiatric care[45].

What is more, contract probation can be combined with the punishment of imprisonment, according to Chapter 30 § 11 of BrB. The punishment of imprisonment ought to be short-term and could last from 14 days to three months[46], intimating that imprisonment can be combined with contract care[47]. The aim of combining both punishments, according to the working papers, was not of any therapeutical character but was rooted in the type of crime committed and previous criminal record of the offender[48]. It intricates that the imprisonment without the protective supervision, would last long, and the term of short imprisonment indicates this fact[49].

---

[42] *In choosing a sanction, the court shall pay special attention to any circumstance or circumstances that argue for the imposition of a less severe punishment than imprisonment. In this connection, the court shall consider such circumstances as are mentioned in Chapter 29, Section 5. Source: DS 1999:36.*

[43] Martin Borgeke , *At bestemma påföljd för brott,* (Stockholm, 2012), 374.

[44] Martin Borgeke., *At bestemma påföljd för brott,* (Stockholm, 2012), 384.

[45] Berggren O., Bäcklund A., Munck J., Victor D., Wersäl F., *Brottsbalken. En kommentar. Kap. 25-38., (*Stockholm, Supplement 5,) July 2014, Chpater 30 § 9, p. 5.

[46] Martin Borgeke, *At bestemma påföljd för brott,* (Stockholm 2012), 395.

[47] Berggren O., Bäcklund A., Munck J., Victor D., Wersäl F., *Brottsbalken. En kommentar. Kap. 25-38., (*Stockholm, Supplement 4), January 2014, Chpater 30 § 11, p. 1.

[48] Ibid.

[49]Berggren O., Bäcklund A., Munck J., Victor D., Wersäl F., *Brottsbalken. En kommentar. Kap. 25-38., (*Stockholm, Supplement 4), January 2014, Chpater 30 § 11, p. 2.

At its core, an offender is entering a contract with the medical facility in order to undergo treatment. The benefit of this situation would be that an individual would be in prison only for some short period. This instrument in fact replaced in the Swedish system a measure of open psychiatric care and is also used in the cases of sexual crimes against minors. As an example of the use of the contract probation, one can name a case before the Supreme Court of Sweden NJA 2006 s. 212.

An offender has committed a crime from Chapter 6 § 4 of BrB, the crime of child pornography and sexual exploitation of a minor[50]. An individual was in need of long-term psychiatric treatment. The court adopted a standpoint according to which in order to reduce the risk of committing a crime in the future, the latter ought to be sentenced to the contract probation. The offender was instructed about the plan and was eager to take part in it[51]. The second case concerned an offender who was 79 year, who was sentenced for sexual exploitation of minors according to Chapter 6 § 4[52]. The court has reached the conclusion that the most fitting punishment for this crime would be contract care combined with open psychiatric care. Making allowance to the character of the crime, the additional punishment was imposed in the form of three months of imprisonment[53].

These two cases are perfect examples of the role of contract probation in cases concerning sexual crimes against minors. What is more, due to its elastic character they can encompass various types of treatments. In fact, one can presume that it can also be a therapy aiming at decreasing libido of the perpetrator.

---

[50] NJA 2006 s. 212.

[51] Ibid.

[52] *A person who engages in a sexual act with someone under eighteen years of age and who is that person's offspring or for whose upbringing he or she is responsible, or for whose care or supervision he or she is responsible by decision of a public authority, shall be sentenced for sexual exploitation of a minor to imprisonment for at most four years. This also applies to a person who, in circumstances other those mentioned previously in this Chapter, engages in a sexual act with a child under fifteen years. If the person who committed the act exhibited particular lack of regard for the minor or if the crime by reason of the minor's young age or otherwise is regarded as gross, imprisonment for at least two and at most eight years shall be imposed for gross sexual exploitation of a minor. (Law 1998:393), source:* DS 1996:36.

[53]NJA 2006 s. 212.

The illustration of contract probation depicts that even though Swedish system does not enumerate special treatment of the sexual offenders in fact it is permissible, and the aims of treatment can be reached.

As per Ukrainian solutions, at this point, there is no compulsory measure of pharmacological castration (oryg. *хімічна кастрація*). The Parliement adopted the law introducing chemical castration into Ukrainian criminal law. Notwithstanding, it was never signed by the President of Ukraine, hence never went into action. The rationale for the project of pharmacological castration were two sexual crimes committed against 13 years old girl by her father in law and the rape of the 11-year-old girl. It was promoted that the sole imprisonment punishment is not effective towards mentioned individuals and as a result, there is a need for a measure in the Ukrainian system[54]. According to the wording of the project, art. 59 – 1 ought to be imprinted into criminal law. According to this article, the punishment of chemical castration consists of the injection of antiandrogen drugs, which consist of chemicals designed to reduce libido and sexual activity of the offender. Still, there was an interesting limitation provided in the art. 59-1 stated that the chemical castration can be enacted only towards offenders who reached the age of 18 years and did not finish 65.

As it was underlined the project was never adopted, since it was vague and unclear. As an example, the drafters omitted detailed regulation of the procedure of the measure. Concurrently the project lacked the *vocatio legis* period, which is more than crucial in this type of cases[55]. It is the Author opinion that the measure of chemical castration will be most certainly under discussion in Ukraine. Regrettably, it would a result of further social unrest caused by one or more cases of sexual crimes against minors and debate concerning place and form of chemical castration remains open.

[54] Проект Закону України 6449 «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за злочини, вчинені щодо малолітньої чи малолітнього, неповнолітньої чи неповнолітнього та особи, яка не досягла статевої зрілості».

[55] Висновок на проект Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за злочини, вчинені щодо малолітньої чи малолітнього, неповнолітньої чи неповнолітнього та особи, яка не досягла статевої зрілості»

6. Summary

It is noticeable that the question of the existence of the institution of pharmacological castration is a very delicate and troublesome query. Each of the presented countries has its unique attitude, still, the thorough analysis depict that the Swedish system can an example of the aptest and most realistic solution. At this point, Swedish experience for Poland is invaluable since it might solve existing problems and its value for the Ukrainian system lie in the fact that adopted measure can be free of both Swedish and Polish mistakes.

The separate regulation of the chemical castration in the criminal law is not looked-for, since it implicates a series of questions from the point of view of human rights regulations. At the same time at each point this measure cannot be called compulsory, since in order to meet its goals in needs to be voluntary. All above that, sole chemical castration has not any effects on the culprit and even though his libido is decreased, the deprived sexual attraction won't disappear. As an outturn, the successful therapy to sexual offenders should be comprised of chemical castration amalgamated with psychiatric therapy and in many cased prescriptions of additional drugs such as i.e. antidepressants etc. Therefore, the best solution for the Polish problem would be to amend the existing law and introduce into polish law the measure of contract therapy, designated no only to this particular category of offenders but as a general reaction to the crime committed also by addicts. The contractual character of the measure will make it possible to underline the voluntary character of the measure. Still, due to the fact that punishment for the sexual crimes against minors are more severe in Poland in Ukraine when juxtaposing to Swedish one, the measure needs to be translated into the legal milieu of those countries. Firstly, the measure ought to have a post penal character and the perpetrator should undergo at least a few years of imprisonment. From the point of view of the effectiveness the imprisonment of such offenders is not reaching any aim of the punishment, hence it should be stressed that placement in prison has a mere symbolic meaning, still from the point of view of the treatment process can enable the treatment process among others through meeting and informational work with an offender.

In the struggle to minimize the rate of the sexual crimes against minors, one most important aspect is massively omitted. The occurrence "paedophilia" and reactions to it at this point has only a form of reaction to already materialized deviation, whereas it is imperative to create preventive mechanisms prior to a crime. It can be done through the introduction of programs providing help and treatment to this group of individuals on everyday basis prior to committing a crime[56]. One of the examples of such endeavours is programme conveyed by the Karolinska Institute in Sweden. It aims at achieving an effect of reducing or excluding the risk of committing a sexual offence against children by the participants of the project. The delineation of the project was "Pedophilia at Risk – Investigations of Treatment and Biomarkers." (PRIOTAB)[57]. The sole aim of the project was to repurpose the drug *Degarelix*. In normal conditions, the drug is prescribed in the course of prostate treatment, as a medicine decreasing testosterone[58]. The treatment was volitional, and only delinquents who have not committed a crime could take part in it. The aim of the project was to prepare the effective treatment and to activate the individuals who have this type of problems, to be able to deal with it[59].

Even though it is important to seek proper instruments of treatment of the individuals who have committed sexual crimes against minors attention should be given to constructing possibilities of receiving help by this category of individuals on the stages preceding committing a crime. Notwithstanding, the therapy employed in response to already committed crime should take into account the character of the

---

[56] https://www.health.harvard.edu/newsletter_article/pessimism-about-pedophilia accessed:

[57] Kastrering testas på pedofiler, Dagens Nyheter 2016, source: https://www.dn.se/nyheter/sverige/kastrering-testas-pa-pedofiler/ accessed May 10, 2019.

[58] Michael Reaves M., "Pedophilia: Prevention or Paternalism?" *Harvard Medical Health Letter*, (July 2010), http://www.voicesinbioethics.net/voices-in-bioethics/2016/11/15/pedophilia-prevention-or-paternalism#_edn3=;
Ferenc G.Rick , Norman L. Block, and Andrew V. Schally. "An update on the use of degarelix in the treatment of advanced hormone-dependent prostate cancer." *Onco Targets and therapy* 6 (2013): 391, soucre: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3633549/ accessed on the 10th of May 2019.

[59] Sally Guyoncourt S, Sweden giving drugs to paedophiles to suppress their sexual urges, 8 May 2016,
Independent, source: https://www.independent.co.uk/news/sweden-begins-drugs-trial-to-prevent-paedophiles-abusing-children-a7019231.html accessed th May 10, 2019.

treatment which, in order to be successful, should take the form of voluntary interaction of patient and specialist.

Balázs Gáti* - Certain privacy related aspects of cybercrime and digital forensics

1. Introduction

The intensive growth of computer technology, the use of different electronic devices, the growing size of storage devices, the enormously expanded field of internet has emerged a new scientific area of Digital Forensic, during the last two decades. Computer forensics, network forensics, forensic data analysis, and mobile device forensics. are special territories of this science. Digital forensic is working on to presenting, documenting, analyzing, preserving, and identifying information from electronic and digital devices while safeguarding the privacy of users.

Digital Forensic Research Workshop has defined digital forensics as "The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." [1]

In this study I am going to present the privacy related aspects of cybercrime, the role of the digital forensic investigations, the digital forensic research and the actual challenges that emerging from rapidly evolving digital technologies and internet platforms.

* PhD Student, University of Pécs, Faculty of Law, Criminology and Penal Execution Law Department

[1] Gary Palmer, "A Road Map for Digital Forensic Research," *Technical Report (DTR-T001-01) for Digital Forensic Research Workshop* (DFRWS), (New York, 2001)

2. General characteristics of privacy and security

The right to privacy is a fundamental human right [2,3]. Several international human rights treaties enshrined the right to privacy, such as Article 8 of the European Convention on Human Rights of 1950'[4]. This includes the right to be left alone, the right to be free from observation, the allowance to keep one's thoughts, beliefs, identity, and behavior secret, and the right to choose and control when, what, why, where, how, and to whom and what extent the information about oneself is revealed [5,6,7,8].

These characteristics of privacy mean anonymity, what might suffer attacks, therefore lead to the scope of information – and data protection.

Anonymity online "provides individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks"[9]

---

[2] Marc-Andre Eissen, *La protection internationale des droits de l'homme dans le cadre Européen*. (Dalloz 1967).

[3] Jan De Meyer, "The Right to Respect for Private and Family Life, Home, and Communications in relations between individuals, and the Resulting Obligations for States Parties to the Convention" In *A. H. Robertson, ed. Privacy and Human Rights.*(Manchester University Press, 1973)

[4] European Convention on Human Rights (1950)

[5] Fried, Charles, *An Anatomy of Values*, (Harvard University Press,1970)

[6] Janis, Mark, Richard Kay, and Anthony Bradley, *European Human Rights Law: Text and Materials*, 2 nd edition.
(Oxford University Press, 2000)

[7] Marie-Helen Maras,. *From Targeted to Mass Surveillance: Is the EU Data Retention Directive a Necessary Measure or an Unjustified Threat to Privacy?* ed. Ben Goold and Daniel Neyland, (New Directions in Surveillance and Privacy, 2009*)* 74-103.

[8] Koops Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, and Maša Galič. "A typology of privacy" *University of Pennsylvania Journal of International Law*, Vol. 38 (2), (2017) 483-575

[9]See: A/HRC/29/32, para. 16 , „Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to "privacy and freedom of expression are interlinked" and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence" and "unlawful attacks on his or her honour and reputation", and provides that

Using anonymity some individuals can be embolden to communicate cruel, discriminatory, racist, hateful, and/or other forms of harmful speech to others. This behavior might mobilize other like-minded individuals to act similarly[10,11] There are several privacy-enhancing technologies which servers that keep online identity and location invisible such as "Tor" and "encryption". This latter blocks third party access to users' information and communications. The need to access encrypted communications and information in order to fight serious crimes, as terrorism, child sexual exploitation is emphasized and demanded by several governments [12,13]. Therefore encrypted messaging services are considered illegal in certain countries[14,15].

Data securitys focused on protecting personal data from any unauthorized third-party access and provides individuals with the freedom to live their lives with personal autonomy. One can live free from fear and coercion, and privacy enables individuals

"everyone has the right to the protection of the law against such interference or attacks". The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8). "

David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" In: *Human Rights Council, Twenty-ninth session* (2015) A/HRC/29/32

[10] Karen M. Douglas, Craig McGarty. "Identifiability and Self-Presentation: Computer-Mediated Communication and Intergroup Interaction." *British Journal of Social Psychology*, Vol. 40(3), (2001) 399-416.

[11] Katja Rost, Lea Stahel, Bruno S. Frey. "*Digital Social Norm Enforcement: Online Firesto*n *Social Media". PLOS One*, Vol. 11(6). (2016)

[12] David Meyer,. "Iran Bans Telegram, an App Used By Half the Country". *Fortune*, (1 May 2018)

[13] István László Gál ,Melána Nagy, "Protection of the Sexual Morality of Children in Hungary" ed: Zoran, Pavlovic . (*Yearbook - Human Rights Protection - Protection of the Rights of the Child : "30 Years After the Adoption of the Convention on the Rights of the Child*)
Újvidék, Szerbia: Institute of Criminological and Sociological Research, (2019) . 567-582. , 16 p

[14] Neil MacFarquhar. "Russian court bans Telegram app after 18-minute hearing".*The New York Times*. (13 April 2018)

[15] David Meyer, "Iran Bans Telegram, an App Used By Half the Country". *Fortune*, (1 May 2018)

"to achieve self-determination and develop their personalities free from coercion"[16]. Protecting the privacy of individuals is integral to protecting data, and securing systems that contain this data and networks through which this data traverses.

2.1. Cybercrime and privacy

Cybercrime consists of criminal acts that are committed online by using electronic communications networks. Cybercrime violates individuals' privacy and the security of their data, particularly hacking, malware, identity theft[17], financial fraud, medical fraud, and certain offences against persons that involve the revealing of personal information, messages, images, and video and audio recordings without individuals' consent or permission.

Data is considered a commodity online and offline by both legal and illegal actors [18]. For this reason, data is a primary target of cybercriminals.[19] Data plays an integral role in the commission of many cybercrimes, primarily because it is not adequately protected. Data breaches are usually gained by lost or stolen encrypted flash drives and other storage devices[20]. Medical, financial, and other personal data could be found on dedicated online carding platforms and darknet sites [21,22]

[16] Marie-Helen Maras. "From Targeted to Mass Surveillance: Is the EU Data Retention Directive a Necessary Measure or an Unjustified Threat to Privacy?" ed. Ben Goold and Daniel Neyland,. *New Directions in Surveillance and Privacy* (2009) 74-103..

[17] Dávid Tóth, "Személyiséglopás az interneten" , *Büntetőjogi Szemle* 9 1 . (2020) 113-119. 7

[18] Marie-Helen Maras, "Cybercriminology". *Oxford University Press*". (2016).

[19] Csaba Fenyvesi*, "*Future Developments *and* Challenges *in* Criminalistics *as* Part *of* Criminal Justice*". Journal* of *Eastern-European Criminal Law (2019)* 2360-4964, 6. 2 72-85.

[20] Andrea Kraut, László Kőhalmi, Dávid Tóth ,"Digital Dangers of Smartphones" *Journal Of Eastern-European Criminal Law* 7 1. 36-49., 14 .

[21] Maras, Marie-Helen"Inside Darknet: The Takedown of Silk Road" *Criminal Justice Matters*, Vol. 98(1), .(2014) 22-23.

[22] Kristin Finklea, Dark Web. *Congressional Research Service*. (2017).

2.2. Cybersecurity and Digital Forensics

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Application of effective cybersecurity measures is particularly challenging today.

Malicious methodologies, tools, and software are implemented and designed every day to pose a threat to public and private networks while simultaneously exploiting data storage, for extracting useful information[23] Digital forensic has gained major attention to counter this emerging threats [24].

Digital forensics is the science of presenting, documenting, analyzing, preserving, and identifying information and evidence from electronic and digital devices while safeguarding the privacy of users. Furthermore, it also makes use of scientific techniques to recreate and explain the sequence of the events. By evaluating, reviewing, and recording these sequences, digital forensics aims at presenting such illegal artefacts as evidence in the court of law.[25]

Cybercrimes significantly contributed in the development of new techniques, tools, and attacks that enable attackers to penetrate even in the well-controlled environment [26].

Digital forensics offers scientific methods for identification, validation, interpretation, and documentation on digital devices like RAM, phones, memory cards, floppy disks,

[23] Asou Aminnezhad, Ali Dehghantanha, "A survey on privacy issues in digital forensics," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 3, no. 4, (2014).183-199,

[24] Farhood N. Dezfouli , Ali Dehghantanha, "Digital forensics trends and future," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 3, no. 4, (2014). 183-199,

[25] Csongor Herke, „ A digitalizáció szerepe a büntetőeljárásban" ed. Mezei, Kitti *A bűnügyi tudományok és az informatika* (Pécs, Magyarország, Budapest, Magyarország: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont 2019) 204, . 104-124. , 21

[26] Bhoopesh K.Sharma, M. A. Joseph, B. Jacob and L. C. B. Miranda, "Emerging trends in Digital Forensic and Cyber security-An Overview," In *2019 Sixth HCT Information Technology Trends (ITT*),(2019), 309-313,

and flash drives to collect digital evidence.[27] Parallel to advancement in digital forensics techniques, hackers are equally exploiting anti-forensics technology [28].

3. Digital Forensic Investigation

Digital forensic investigation (DFI) has become a recognized profession and research field [29] . Whilst the field of digital forensics is now well established, its research community can be considered relatively emerging in comparison to the associated areas of traditional forensic and computer sciences [30].

DFI processes, including identification, preservation, analyses, documentation and presentation of digital evidence[31] must be conducted in a robust and legally accepted manner in order to stand the test of legal scrutiny in the courts of law. Many institutions are relying on digital media for the storage of information [32]. NIST (National Institute of Standards and Technology) defines *digital forensics* as "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain

[27] Zoltán András Nagy "A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén" *Belügyi Szemle: A Belügyminisztérium Szakmai Tudományos Folyóirata* (2018) 66:10, 36-55 20

[28] Mohammad Wazid, Avita Katal, Rayan H. Goudar and Sreenivas Rao, "Hacktivism trends, "Hacktivism trends, digital forensic tools and challenges: A survey" *2013 IEEE Conference on Information & Communication Technologies*, . (April 2013), 138-144,

[29]Act 29, "Criminal offenses act 1960", https://www.wipo.int/edocs/lexdocs/laws/en/gh/gh010en.pdf (1960),Accessed: 7 Oct 2020,GoogleScholar

[30] Act 30, "Criminal procedure Code (Act 30)" https://www.wipo.int/edocs/lexdocs/laws/en/gh/gh011en.pdf (1960),Accessed: 6 Jun 2020, Google Scholar

[31] Act 526, "The security and intelligence agencies act 1996" https://acts.ghanajustice.com/actsofparliament/security-and-intelligence-agencies-act-1996-act-526/ (1996),Accessed: 7 Oct 2020, Google Scholar

[32] Act 772, "Electronic transaction act 2008" https://moc.gov.gh/sites/default/files/downloads/Electronic%20Transactions%20Act%20772.pdf (2008),Accessed: 7 Oct 2020 , Google Scholar

of custody for the data"[33]. As the use of digital media for information storage expands rapidly, there is a corresponding growth in computer crimes and cyber fraud [34]

DFI is defined as the use of scientifically proven methods to obtain digital evidence from digital media sources which can be used by the court of law[35]. DFI is not limited to personal computers but other digital devices such as cell phones, Personal Digital Assistants (PDAs), network traffics, among many others. The various types of digital forensics include disk forensics, network forensics, wireless forensics, server forensics, database forensics, malware forensics, email forensics, memory forensics, mobile phone forensics [36] and more recently dashboard camera (dashcam) forensics[37]. Digital forensics aims to establish comprehensive knowledge and develop appropriate methodologies that can be adopted to defeat digital criminals and cyber fraudsters. [38]. The proper personal data processing is a very important element of the digital forensic investigations, as enshrined in the Directive (EU) 2016/680 of the European Parliament and of the Council [39]. One of the most important provisions of the directive is set out in Article 4 [40],

---

[33]Karen Kent Suzanne, Chevalier Tim Grance, Hung Dang, „Guide to integrating forensic techniques into incident response." (2006).https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response, Accessed: 20 Oct.2020

[34] Act 775, "Electronic communication act 2008" https://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf (2008),Accessed: 7 " Oct 2020, Google Scholar

[35] Act 804, "Economic and organized crime act 2010" http://www.eoco.org.gh/wp-content/uploads/2015/03/Economic-and-organized-crime-Ac.pdf (2010),Accessed: 7 Oct 2020, Google Scholar

[36] Act 807,"Mutual legal assistance act 2010" https://www.unodc.org/res/cld/document/gha/2010/mutual-legal-assistance-act_html/Mutual_Legal_Assistance_Act.pdf (2010), Accessed: 7 Oct 2020, Google Scholar

[37] Act 843", Data protection act 2012" https://www.dataprotection.org.gh/index.php/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843 (2012) Accessed: 7 Oct 2020,Google Scholar

[38] See also: Act 843, „Data protection act 2012"

[39] EC, EP, 2016a. "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing" *Council Framework Decision 2008/977/JHA. ELI.* http://data.europa. eu/eli/dir/2016/680/2016-05-04 , Accessed: 10.Feb.2021

[40] EUR-Lex, 2017. "Protecting personal data when being used by police and criminal justice authorities (from 2018)" https://eur lex.europa.eu/legal-content/EN/TXT/ ?uri=LEGISSUM:310401_3.Accessed: 18 Dec 2020

which states that personal data of natural persons must be: a) processed lawfully and fairly; b) collected for specified, explicit and legitimate purposes and processed only in line with these purposes; c) adequate, relevant and not excessive in relation to the purpose in which they are processed; d) accurate and updated where necessary; e) kept in a form which allows identification of the individual for no longer than is necessary for the purpose of the processing; f) appropriately secured, including protection against unauthorized or unlawful processing.

A further challenge for the low enforcement authorities that data they need is often stored abroad or by a foreign service provider. This results in the need to resort to mutual legal assistance and, at the EU level, to the European Investigation Order (EIO), which procedure is too slow because relevant data can be lost in the meantime. In April 2018, the European Commission proposed new rules enabling police and judicial authorities to obtain electronic evidence more quickly and more easily. They were included in the "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters" and the accompanying "Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings"[41]. The European Commission stressed the growing importance of electronic evidence for criminal proceedings, the fact that cross-border requests for such evidence currently predominate in criminal investigations. Authorities need to be equipped with 21st century techniques, given that approximately two thirds of electronic evidence are located in another State, a fact that hinders both the investigation and the prosecution[42].

The European production order (EPdO) and the European preservation order (EPsO) allow the judicial authority of a Member State, the issuing State, to directly order a provider offering the service in the EU to hand over or store the electronic evidence.

[41] COM (2018) 225 final and COM (2018) 226 final." For an analysis of the proposals", see also S. Tosza, "The European Commissions's Proposal on Cross-Border Access to E-Evidence" (2018) eucrim, 212–219

[42] Ángel Tinoco-Pastrana The Proposal on Electronic Evidence in the European Union, Eucrim," 2020, https://doi.org/10.30709/eucrim-2020-004 ,Accessed:21 Feb 2021

The EPdO implies an extraordinary simplification of the procedure, with a significant reduction in deadlines for delivery of the evidence (i.e. ten days or – in emergency situations – six hours (Art. 9(1) and (2) of the text in the version of the Council's general approach.)[43,44].

Reconciliation between security and justice is also a premise at the Council of Europe level. When interpreting the European Convention on Human Rights (ECtHR) as regards access to data and the exchange of information between Member States for the purpose of combating transnational crime and terrorism, the ECtHR, on the one hand, recognizes such access and exchanges as essential, due to the sophisticated methods of data evasion by criminal networks. On the other hand, the ECtHR defines the limits and proportionality of electronic surveillance and transfer of data must respect the principle of proportionality. [45]

As part of the package of proposals from the European Council the purpose of Directive is to decide on the right of legal representatives. According to this oblige service providers to appoint a legal representative within the Union to ensure that the same obligations apply to all provider of services within the European Union, even then also if they are established in a third country. The legal the representative must be present in one of the Member States where the service provider is established or provides services.[46]

[43] "Cf. Council doc. 15292/18/19 of 12 December 2018; a version of the general approach of December 2018 supplemented by respective annexes "was published on 11 June 2019, Council doc. 10206/19.

[44]" Factsheet e-evidence", https://europa.eu/rapid/press-release_MEMO-18-3345_en.htm, (2006),Accessed:21 Feb 2021

[45] ECtHR, 13 September 2018, *Big Brother Watch and others v. the United Kingdom*, Application. nos. 58170/13, 62322/14 and 24960/15, http://hudoc.echr.coe.int/fre?i=001-140713,Accessed: 21 Feb 2021

[46] "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" COM/2018/226 final - 2018/0107 (COD)
EUR-Lex, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018PC0226,Accessed: 20 Feb 2021

4. Fast growing digital platforms and digital forensic

Data plays an integral role in the commission of many cybercrimes and vulnerabilities to cybercrime. The privacy has recently been extensively threatened by some fast growing digital platforms as cloud-, social- and internet of thing (IoT) platforms, therefore special attention is required from the digital forensic research and privacy-related activities in these areas.

4.1 Cloud storage

The increased use of cloud storage has been rising by 11-16% over the last few years[47]. The majority of Digital Forensic Unit work is complex, therefore managing the demand is also complex.[48]

Cloud computing offers massive resource pool, dynamicity, and wide access for storage. Private, public and hybrid models of cloud computing exists, in addition to multiple services, such as security-, database -, integration -, and software as service[49]. Cloud computing has been widely accepted in multiple governments and private companies. Communication Service Providers also have established data centers worldwide that provide cloud services for ensuring value-effectiveness and service availability [50].

However, cybercrimes and security in the cloud environment are the major hurdles for organizations to transfer their systems to this platform, therefore, cloud forensics has gained major attention by forensics investigators. Cloud forensics is a special

[47] „Cloud computing - statistics on the use by enterprises", eurostat, explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Cloud_computing_as_a_service_model_for_meeting_enterprises.E2.80.99_ICT_needs,Accessed: 20 Feb 2021

[48] Malek Harbawi , Asaf Varo, „The Role of Digital Forensics in Combating Cybercrimes," https://www.researchgate.net/publication/303393656_The_role_of_digital_forensics_in_combating_cybercrimes,Accessed: 2 Dec .2020

[49] See also: M. Wazid, A. Katal, R. H. Goudar and S. Rao, "Hacktivism trends digital forensic tools and challenges: A survey."

[50] See also: B. K. Sharma, M. A. Joseph, B. Jacob and L. C. B. Miranda, "Emerging trends in Digital Forensic and Cyber security-An Overview,"

application of digital forensics in a cloud-based environment [51]. This field utilizes scientific principles, proven methods, and technological practices to process events in cloud environment via reporting, examination, preservation, collection, and identification of digital data, so that events can be reconstructed.[52] The default characteristics of cloud computing, which includes a high degree of virtualization, data duplication, jurisdiction, and multi-tenancy add various complexity layers in cloud forensics.[53] Besides, the procedures involved in cloud forensics depends on the deployment and service model of cloud computing [54].

One of the main challenges with cloud storage and computing, which is widely used in many countries and regions, is that data can reside and be transmitted on computers and networks in different jurisdictions, where data security and privacy laws and regulations may be very different[55]. Cloud forensics is categorized as legal, organizational, and technical [56]. The legal dimension takes care of the development of agreements and regulations to ascertain that digital forensics methods do not breach regulations and laws. On the contrary, the organizational dimension encompasses organizational factors of the digital forensics [57]. The technical dimension covers the

[51] Haider TH. Alrikabi, Abdul Hadi M. Alaidi, Ahmad Shaker Abdalrada, Faisal Theyab Abed, "Analysis the Efficient Energy Prediction for 5G Wireless Communication Technologies, *International Journal of Emerging Technologies in Learning (iJET)*s," vol. 14, no. 08, (2019) 23-37,https://online-journals.org/index.php/i-jet/article/view/10485,Accessed: 20 Feb 2021

[52] Zsolt Gáspár, „A digitális adat felhasználása a büntetőeljárásban"
In: Barna, Boglárka Johanna; Kovács, Petra; Molnár, Dóra; Pató, Viktória Lilla (szerk.) XXIII. Tavaszi Szél Konferencia Absztrakt Kötet, "*Mi és a tudomány jövője"* (Budapest, Magyarország, Doktoranduszok Országos Szövetsége (DOSZ) 2020) 550 . 70 , 1 p

[53] Lei Chen, Nhien-An Le-Khac, Sebastian Schlepphorst, Lanchuan Xu, "Cloud Forensics: Model, Challenges and Approaches" ed. Lei Chen, Hassan Takabi, Nhien-An Le-Khac*: Security, Privacy, and Digital Forensics in the Cloud,2019.* (2019 Higher Education Press) 201-216

[54] Shams Zawoad, Ragib Hasan, "Cloud forensics: a meta-study of challenges, approaches, and open problems," arXiv preprint arXiv, p. 1302.6312 [cs.DC] (2013), https://arxiv.org/abs/1302.6312,Accessed: 20 Feb 2021

[55] Lei Chen, G., Du, Y., Du, J., Li, N. „ Research of digital forensics under cloud computing environment." *Netinfo Security* 2013 (8): 87–90.

[56] Israa Al_Barazanchi, Shihab A. Shawkat, Moayed H. Hameed, Khalid Saeed Lateef Al-badri "Modified RSA-based algorithm: A double secure approach," *Telkomnika* vol. 17, no. 6, (2019) pp. 2818–2825, https://core.ac.uk/download/pdf/324199364.pdf, https://core.ac.uk/download/pdf/324199364.pdf

[57] Keyun Ruan; Joe Carthy; Tahar Kechadi; Mark Crosbie "Cloud forensics," In: *IFIP International Conference on Digital Forensics.* (Springer, Berlin, Heidelberg ,2011) , 35-46,

procedures and tools that are essential to execute forensic investigation in a cloud computing domain.

4.2 Social Media

The social media platforms have become a primary source of socialization. This offers a possibility for hackers to exploit user's account[58].

Different social media applications like LinkedIn, Instagram, Facebook, and Twitter have been exposed to multiple cyber threats and malware. Attacks on social media platforms can take place outside the system/network or within the network. Outside systems attack usually include DDoS, (distributed denial-of-service attack) or DoS, (denial-of-service attack) while attacks within the network include retrieving cookies data[59]. Besides, it is established that the database of these social media applications is most vulnerable to such attacks. Digital investigators have paid a major interest towards the social media forensics. Social media platforms are a big source of information regarding potential offenders, suspects, and witnesses[60].

Combining social media with digital forensics, investigators can gain access to a modern and diverse subset of sources of data, including demographic location, photographs, contact lists, geo-location, and text messages. This network data, combined with the metadata, has the potential to assist digital forensics

[58] See also: M. Wazid, A. Katal, R. H. Goudar and S. Rao, "Hacktivism trends, digital forensic tools and challenges: A survey"

[59] See also: B. K. Sharma, M. A. Joseph, B. Jacob and L. C. B. Miranda, "Emerging trends in Digital Forensic and Cyber security-An Overview,"

[60] Anderson E. A. Rocha, "Authorship attribution for social media forensics" *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, (2016).. 5-33

investigations[61,62]. The social media forensics is a rising trend in the digital forensics' domain due to its ability to efficiently providing adequate digital evidence.[63]

4.3 Internet of Things

The connection of different electronic devices through the internet to execute tasks is a fast growing technology defined as internet of things (IoT)[64]. Three areas are involved in the science of IoT forensics, as IoT device -, network - and cloud platforms. The IoT systems offer smart and intelligent way of communication in the private area as well as in business applications [65].

IoT devices exchange data with millions of other devices around the globe. Such type of open large-scale communication makes them especially inviting for users with illegal intentions. Only in 2017 there was 600 percent increase in attacks against IoT devices [66]. In many cases, the intruders are not directly targeting the IoT device, but using it as a weapon to attack other websites[67]. As a result, cybercrime has become

[61] Mohammed I. Alghamdi, „Digital forensics in cyber security - recent trends, threats, and opportunities" *Periodicals of Engineering and Natural Sciences*, Vol. 8, No. 3, (July 2020), 1321-1330

[62] Matthew Andreotta , Robertus Nugroho , Mark J Hurlstone , Fabio Boschetti „Analyzing social media data: A mixed-methods framework combining computational and qualitative text analysis" *Behav Res* 51**,** (2019). 1766–1781 https://doi.org/10.3758/s13428-019-01202-8,Accessed: :21 Feb 2021

[63]Kathryn C. Seigfried-Spellar, Sean C. Leshney, "The intersection between social media, crime, and digital forensics: Who Dun It?" In: *Digital Forensics,Threatscape and Best Practices* (2016) 59-67

[64] Naseer Ali Hussien, Iman Kadhim Ajlan, Mohamed Fazil Mohamed Firdhous, Haider TH. Salim Alrikabi "Smart Shopping System with RFID Technology Based on Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM*) , Vol 14, No 04 (2020)

[65] Mohammed I. Alghamd, „Digital forensics in cyber security - recent trends, threats, and opportunities" ,*Periodicals, Enineering and Natural Sciences,* Vol 8, No. 3 (2020) en.ius.edu.ba/index.php/pen/article/view/1463m Accessed:21 Feb.2021

[66]„Internet Security Threat Report" (ISTR): Symantec. (2018). Volume 23, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23- 2018-en.pdf ,Accessed: 21 Feb.2021

[67] Saad Alabdulsalam, Kevin. Schaefer, Tahar Kechadi, and Nhien A. Le-Khac "Internet of Things forensics—Challenges and a case study," In *Proc. IFIP Adv. Inf. Commun. Technol*., vol. 532, (2018) 35–48

the second most reported crime worldwide [68]. IoT systems seem to be easy targets for attackers, mostly due to the fact that when building an IoT device, manufacturers often place great emphasis on cost, size and usability, while security and forensics aspects tend to be neglected. Lally and Sgandurra[69] outline that some producers implement security practices mainly because an eventual exploitation of one of their IoT products will damage the company's image.

The digital forensic experts have developed an interest in IoT forensics to carry out the digital investigation. The rise of IoT forensics trend is due to the fact that IoT systems present multiple complex and unique challenges in the digital forensics field [70]. IoT-based applications contain a huge number of resources and distinct devices that generates a tremendous amount of data, which is known as Big IoT data. This data, combined with digital forensics tools and techniques, provide investigators with an opportunity to trace cybercrimes that further help them in preventing cyber-attacks [71,72].

Forensic investigators are forced to face additional analytics, security, and capacity challenges. Regardless of several limitations, IoT forensics offers a richer and authentic source of evidence, as compared to conventional computer systems[73]. IoT forensics react to the requirements of users without requiring users' conscious interaction. As a result, the IoT forensics environment provides contextual evidence

[68]" Global Economic Crime and Fraud Survey 2018." PwC. (2018)." https://www.pwc.com/gx/ en/forensics/global-economic-crime-and-fraud-survey-2018.pdf, Accessed: 21 Feb.2021

[69]Gurjan Lally, Daniele Sgandurra, *Towards a Framework for Testing the Security of IoT Devices Consistently*. Cham, Switzerland: (Springer, 2018,) 88–102.

[70]Tharmini Janarthanan, Maryam Bagheri, Shahrzad Zargari, IoT Forensics: "An Overview of the Current Issues and Challenges," In book: *Digital Forensic Investigation of Internet of Things (IoT) Devices* (Springer, January 2021)) 223-254

[71]Darren Quick and K.-K. R. Choo, "IoT device forensics and data reduction," *IEEE Access,* vol. 6, (2018). 47566–47574

[72]Temilola Aderibigbe, Bobby C. Granville "A framework for IoT data acquisition and forensics analysis," In *Proc. IEEE Int. Conf. Big Data*,(2019) 5142–5146

[73] Robert. Hegarty David. J. Lamb , Andrew. Attwood, "Digital Evidence Challenges in the Internet of Things," In*:INC,* (2014). 163-172

that helps digital forensic investigators to analyze physical world events therefore, IoT forensics is one of the prominent trends of digital forensics domain[74].

The Health System one of the most sensitive area of the IoT platform, defined as Internet of Medical Things (IoMT) Forensics. Increase of cyberattacks towards the medical sector by hackers targeting the Electronic Health Records has been observed during the last few years. DiGiacomo presented about 115 cyber-attacks in January 2018, East RHF [75]. A healthcare organisation that manages hospitals in Norway with a possibility that over 2.9 million users are potentially affected by the breach[76].

The research from Catarinucci and co-workers demonstrated that Personal Health Information is processed and transmitted via IoT-based devices used for medical purposes supporting the work of General Practitioners to avoid unnecessary medical appointments with patients[77]. Mittal[78] predicted an estimated amount of 163.2 million IoT devices aimed to healthcare purposes.

Considering that most of devices are unlikely to show or contain the necessary consent from users[79], to define a comprehensive and holistic forensic investigation model that ensures data privacy and compliance maintaining most discretion during an investigation in order to protect people during and after a security breach is now required.

---

[74]Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis, „A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys & Tutorials*, VOL. 22, NO. 2, second quarter (2020,) https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8950109,Accessed: 22 Feb 2021

[75] John J. DiGiacomo, (2018) "Data Beach Statistics For 2018 Plus Totals From 2017." Revision Legal, https://revisionlegal.com/internet-law/data-breach/2018-statistics/,Accessed:22 Feb 2021

[76] "Louis Columbus (2019). "2018 Roundup Of Internet Of Things Forecasts And Market Estimates." 8/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/?sh=686f28e47d83,Accessed: 22 Feb 2021

[77] Luca Catarinucci, Danilo de Donno, Luca Mainetti, Luca Palano et al. "An IoT-aware architecture for smart healthcare systems". *IEEE* 6: (2015) 515-526.

[78] " IoT Ecosystem: How the IoT Market will Explode by 2020." Mittal S (2019),

[79] Yvonne O'Connor, Wendy Rowan, Laura Lynch, Ciara Heavina "Privacy by Design: Informed Consent and Internet of Things for Smart Health" *Procedia Computer Science* 113: (2017) 653-658.

5. Challenges in the Digital Forensics

5.1 General aspects of challenges

Digital forensics has been defined as the use of scientifically derived and proven methods towards the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derivative from digital sources to facilitate the reconstruction of events found to be criminal[80,81]. But these digital forensics investigation methods face some major challenges at the time of practical implementation. Digital forensic challenges are categorized into three major heads [82]. These are technical challenges, resource challenges and legal challenges.

5.1.1 Technical challenges

The advancement in digital technology has opened doors to various opportunities; however, it has also caused the digital forensics domain to face various challenges. Although different digital forensic experts and researchers have been analyzing and studying numerous known digital forensic issues, there is still a requirement to classify these challenges[83]. In this account, it has been discovered that digital forensic systems are exposed to technical challenges that threaten the integrity of these systems. Technical challenges are those potential threats that can be addressed using existing operations, protocols, and expertise. Understanding that digital forensics demands an optimum combination of ethical conduct and technical skills.

---

[80] Vishal R. Ambhire, B.B Meshram, "Digital Forensic Tools," *IOSR Journal of Engineering*,(March.2012), Vol. 2(3) 392-398, ISSN: 2250-3021.

[81] Csaba Fenyvesi, József Orbán, „Az Elektronikus Adat Mint a 7-5-1-Es Kriminalisztikai Piramismodell építőköve", *Belügyi Szemle* 67 (2), (2019) 45-55. https://doi.org/10.38146/BSZ.2019.2.3.Accessed: 22 Feb 2021

[82]"An Introduction To Challenges In Digital Forensics" https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics/Accessed: 21 February 2021

[83] Ahmed Raisan Hussein," Intelligent control methods of variable speed wind turbine generator" http://dx.doi.org/10.21533/pen.v8i3.1529.g631 Accessed: 21 February 2021

Some of the major technical challenges, associated with digital forensics are encryption, a huge volume of data, and incompatibility among diverse forensic tools[84]. The advancement in communication technology has made sophisticated encryption products and services easy and widely accessible. Due to this, encryption algorithms and standards are becoming more complex, which further increases the time and difficulty of conducting cryptanalysis. This technique joins encrypted files together to extract meaningful information.[85] In addition, encryption makes electronic data unreadable, which further enable criminals to camouflage their criminal activities[86]. For a digital forensic officer, this can negatively affect their investigation process. It has been discovered that around 60% of cases - involving some type of encryption - goes unprocessed because it significantly limits the ability of the investigator to extract information from the evidence[87]. Thus, the easy implementation, low cost, and the availability of encryption tools greatly pose a threat to the integrity and credibility of the digital forensics process. In addition to encryption, huge volumes of data that exist within numerous applications- like enterprise resource planning-also poses a great threat to digital forensic operations.

The substantial increase in data volumes significantly reduces the capability of legal systems and forensic investigators to keep up with the digital threats[88]. Likewise, with the introduction of cloud computing, much IT-related hardware, such as network switches, racks, and servers have been replaced with remote-on-demand, virtualized software that are configured according to business needs. Besides, these services and data can be managed and hosted by a third-party or the user from any place. Thus, the

[84] Nixon M. Karie, Hein S. Venter, "Taxonomy of challenges for digital forensics" *Journal of Forensic Sciences,* vol. 60, no. 4, (2015). 885-893,

[85] Dávid Tóth, "Digitalization trends in the Hungarian Criminal Procedure"
ed Belaj, Ivan; Vajda, Halak Željka; Slobodan, Stojanović *10. Međunarodna Konferencija Razvoj Javne Uprave,* Vukovar, Horvátország :Veleučilište Lavoslav Ružička u Vukovaru (2020) pp. 309-316. , 8 p

[86] Adedayo M. Balogun, Shao Ying Zhu "Privacy impacts of data encryption on the efficiency of digital forensics technology" arXiv preprint arXiv:1312.3183., (2013)

[87] Eva A. Vincze, "Challenges in digital forensics. *Police Practice and Research*," vol. 17, no. 2, (2016),. 183-194

[88] Sriram Raghavan, "Digital forensic research: current state of the art" *CSI Transactions on ICT*, vol. 1, no. 1, (2013): 91-114

data and software have the possibility that it is stored physically across multiple geographic locations[89]. This distributive nature of data substantially lowers the control and visibility of forensic experts over digital forensic artefacts. Similarly, digital forensic tools and techniques commonly differ in cost, complexity, and functionality. Due to this, most of the digital forensic tools contain heterogeneous parts or elements, which increases their incompatibility to work together[90]. Moreover, some forensic tools are not able to handle the ever-increasing storage capacity of target devices. This means that vast targets constitute a major technical challenge to digital forensic operations because they demand more complex analysis techniques.[91]

It is affirmed that different technical challenges pose a great threat to the performance and integrity of digital forensic operations. For instance, in case of encrypted devices or data sets their content is not always known to the investigating authorities, so they cannot be used in proof either. This is due to the fact that in most countries,- also in Hungary- the success of an investigation often depends on the co-operation of the *accused person* and the means of evidence found and obtained on the spot, as *the prohibition of self-incrimination prevails* in criminal proceedings[92].

However, there is a counterexample to this, because a few countries allow the obligation to decrypt, so the French Penal Code threatens to imprison for up to three years or, in qualified cases, five years for anyone who refuses to provide the password and code.In the United Kingdom for two years[93]. In Belgium, one this is punishable by up to one year in prison.[94]In this close context, it is worth mentioning cases when the user uses an encryption that is not a password or code, but biometric data (e.g.

---

[89] See also: E. A. Vincze, "Challenges in digital forensics" *Police Practice and Research*," vol. 17, no. 2, (2016), 183-194

[90] Nickson. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics" *Journal of forensic sciences*, vol. 60, no. 4, (2015). 885-893

[91]Csaba Fenyvesi," Kriminalisztikai világtendenciák – különös tekintettel a digitális felderítésre". In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. (PTE ÁJK-MTA Társadalomtudományi Kutatóközpont, Budapest-Pécs, 2019). 64-82.

[92] See also: Dávid Tóth, "Digitalization trends in the Hungarian Criminal Procedure"

[93] Bert-Jaap Koops, Eleni Kosta," Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". *Computer Law & Security Review*, 4, . (2018) 890-900.

[94] László Dornfeld, "Az elektronikus bizonyítékszerzés egyes kérdései" *Kriminológiai Közlemények*, 77, (2017) 241-256

fingerprint, facial recognition, iris), which is particularly may complicate the situation of the investigating authorities and the conduct of the proceedings, because this form of digital identification is appearing in more and more[95].

5.1.2 Resource challenges

Personnel related challenges may endanger the integrity of digital evidence. Among various personnel-related challenges, lack of well-trained forensic staff is the most prominent one [96]. Despite the overwhelming significance of the digital forensics field because of cyber-crimes, the lack of qualified forensic officers threatens the process of digital forensics. The shortage of well-trained forensic investigators is due to the fierce competition in law enforcement as well as high requirements since digital forensics require technically proficient personnel that are certified and trained to deliver scientifically valid evidence [97]. Likewise, it cannot be denied that digital forensics has gained major importance among forensic practitioners, law enforcement agencies, and computer professionals. *Unfortunately, the advancement in this field has encouraged an environment that is threatened by semantic disparities*. Another potential personnel-related challenge is a chain of custody.

Chain of custody refers to the location log that defines the collection point of the evidence. In digital forensic analysis, it is one of the most crucial issues because it requires physical control of the evidence that is not possible in a digital environment [98] In addition, due to proprietary technology, procedures, and multi-jurisdictional laws, effectively managing the chain of custody is a major challenge that is faced by

[95]„Joint Project on Regional Cooperation against Cybercrime, Electronic evidence guide - A basic guide for police officers, prosecutors and judges, Version 1.0", Authors: Jones, N., George, E., Insa Mérida, F., Rasmussen, U., Völzow, V., http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp , Accessed:21 Feb 2021

[96] See also: N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics."

[97] See also: Eva A. Vincze, "Challenges in digital forensics. Police Practice and Research"

[98] Shams Zawoad , Ragib Hasan "Cloud forensics: a meta-study of challenges, approaches, and open problems," arXiv preprint arXiv, (2013), 1302, 6312

digital forensics. *Hence, it can be established that personnel-related challenges pose a great challenge to traditional forensic operations*.

In addition to the discussed challenges, it is undeniable that digital forensics l*ack a unified formal representation of standardized procedures and knowledge* for analyzing and gathering digital artefacts. This inevitably causes incompatibility and conflict within various digital forensics tools[99].

Errors in the interpretation and analysis of digital artefacts occur when the standardized or formalized procedure for analyzing, preserving, and collecting digital evidence is absent. Likewise, when forensic experts manage a vast amount of data while simultaneously performing forensic investigation, they utilize specialized skills and digital technologies. However, these experts often fail to record their work, which further hampers training and external reviews [100].

Modern digital forensics is a multidisciplinary effort that embraces several fields, including law, computer science, finance, networking, data mining, and criminal justice. Professionals will increasingly face a mixed set of challenges and issues regarding the efficiency of digital evidence processing and related forensic procedures[101].

Analysts will require externally certificated training to provide them with the confidence to use the forensics tools and the credibility to deliver reliable evidence in a court. Consideration may be to issuing each staff member with a Personal Development Portfolio (PDP), which will contain ongoing record of their training and qualifications, as well as milestones achieved in their work mentored activities. Managers may use PDP's to set targets for individuals that will within the team create a more balanced and effective capacity.

---

[99]Nordiana Rahim, Wahid Abdul Wahab, Yamani Idna Idris, Laiha Mat Kiah "Digital Forensics: An Overview of the Current Trends" *International Journal of Cryptology Research* 4, (2014) https://scholar.google.com/citations?user=gD7XfW8AAAAJ&hl=en, Accessed: 22 Feb 2021

See also :[100] Eva A. Vincze, "Challenges in digital forensics. Police Practice and Research,"

[101] Wojciech Mazurczyk, Luca Caviglione; Steffen Wendzel, „ Recent Advancements in Digital Forensics" *IEEE Security & Privacy*, vol. 15, no. 6, (November/December 2017) 10-11

Management will also need to set aside some time for these analysts to undertake research and development. As new tools and applications come onto the market – the analysts should evaluate them to identify artifacts of value to the digital forensic laboratory.

Staff retention will be key to managing a successful digital forensic laboratory. A great deal of time and money will be spent on training of staff, and it is vital they are retained, especially once they are trained and begin to become more experienced. Having robust personal development plans for each member of staff will give them objectives and a better understanding of their career path and future opportunities[102].

5.1.3 Legal challenges

Legal Desire (2020. May) also points to the main challenging areas, as challenges on the field of technology and on the field of handling with the digital volume increase[103]. See the next section for legal regulations and challenges.

6. Legislation and privacy impact assessment

Personal data is protected under the right to privacy in international human rights instruments, European Court of Human Rights has held that telephone data, emails, and Internet use, and data stored on computer servers [104] fall within the scope of protection of Article 8 (1) of the European Convention on Human Rights. The mere storage of personal data can violate a user's right to privacy. The violation depends on

[102] Sanja Jelisavac Trosic, „Digital forensic procedures of European Anti-fraud Office and protection of personal data",https://www.academia.edu/33670673/DIGITAL_FORENSIC_PROCEDURES_OF_EUROPEAN_ANTI_FRAUD_OFFICE_AND_PROTECTION_OF_PERSONAL_DATA,Accessed:22 Feb 2021

[103] „Challenges faced by Digital Forensics, Legal Desire," https://legaldesire.com/challenges-faced-by-digital-forensics/,Accessed: 22 Feb 2021

[104] "Case of Wieser and Bicos Beteiligungen GmbH v Austria" (App no. 74336/01) [2007] ECHR 815., JUDGMENT STRASBOURG, https://www.legal-tools.org/doc/502dd6/pdf/ ,Accessed: 22 Feb 2021

the context in which the data was collected, the way it was collected, processed, and used, and the outcome of this processing[105].

6.1 General data protection regulation (GDPR)

The cross-border nature of the Internet requires transnational data protection regulation that extend beyond national frameworks and law. Examples include the African Union Convention on Cyber Security and Personal Data Protection of 2014 and the Economic Community of West African States (ECOWAS)[106]. These regional laws and frameworks were influenced by the EU Data Protection Directive[107] what later on was replaced by the EU General Data Protection Regulation (GDPR) on 25 May 2018[108] . This single data protection law governs data processing, storage, use, and exchange of data in EU Member States and other countries, agencies, and private organizations outside of the EU that provide goods and services to the EU, and process data of EU residents. The GDPR seeks to harmonize the secure data processing, storage, use and exchange of personal information.

This law minimizes the digital footprint of users and the way apps, technology, and Internet services and platforms exploit this footprint. The GDPR strengthens the privacy rights of individuals and enhances the free flow of personal data across borders by harmonizing data protection practices. The GDPR provided clarity on what constitutes personal data, set rules for the handling of data, delineated roles and

[105] "Case of S and Marper v United Kingdom" (App nos. 30562/04 and 30566/04) [2008] ECHR 1581., JUDGMENT STRASBOURG, https://rm.coe.int/168067d216 ,Accessed: 22 Feb 2021

[106] Economic Community of West African States (ECOWAS). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf,Accessed: 22 Feb 2021

[107] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" Document 31995L0046, EUR -Lex

[108] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" General Data Protection Regulation (GDPR), Document 32016R067, EUR -Lex

responsibilities of those who control and process personal data, created greater penalties for noncompliance, and compelled notification of data breach within 72 hours of the incident.

This regulation mandates new obligations for data controllers (i.e. the entity that determines the reasons for data processing and the methods used to process data), and data processors. The GDPR regulates data access, rectification, erasure, transparency of data processors and controllers; provides a right to object to profiling practices; imposes data security obligations on companies that process data; and provides increased powers to data protection authorities and facilitates the coordination and cooperation in data processing and protection.

The GDPR applies to EU establishments, which has been broadly interpreted by the European Court of Justice as an organization that processes data in the context of its activities, even if these activities are minimal[109].

The GDPR does not apply to the processing of personal data for national security reasons and pursuant to the EU's common foreign and security policy. The GDPR also does not apply to data processed by EU institutions "on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data"[110]. The GDPR also does not apply to data processed by public authorities in the course of the prevention, detection, investigation, and prosecution of crime, "on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of

[109] "Weltimmo v. Hungarian Data Protection Authority" Case C-230/14 [ECR, 30 October 2015, Judgment of the Court, *Official Journal of the European Union*, C 381/6

[110] "Regulation (EC) no 45/2001 of the of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data" , Document 32001R0045, EUR-Lex

the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data"[111,112].

6.2 Police Directive

The personal data processing of large-scale digital evidence in criminal investigations falls within the scope of Directive (EU) 2016/680 of the European Parliament and of the Council[113](the so-called Police Directive). This directive protects individuals, and at the same time ensures a high level of public security. Member States were expected to transpose the directive into national law from May 2016 to May 2018 (EC & EP, 2016a)[114].

One of the most important provisions of the directive is set out in Article 4(1)[115] which were previously appeared in this work, stipulating that Member States shall ensure that the processing is in accordance with the principles of necessity and proportionality.[116]

---

[111] "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data." Document 32016L0680, EUR-Lex

[112] László Kőhalmi, "Szubjektív gondolatfoszlányok a jogállami büntetőeljárásról" *Miskolci Jogi Szemle: A Miskolci Egyetem Állam- és Jogtudományi Karának folyóirata* XIV : .2.Különszám 2.kötet, (2019), 58-67. 10

[113] „Directive (Eu) 2016/680 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing" Council Framework Decision 2008/977/JHA, *Official Journal of the European Union*, L 119/89

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

[115] "Protecting personal data when being used by police and criminal justice authorities (from 2018) ",EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A310401_3,Accessed: 23 Feb 2021

[116] See also: "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

The Police Directive contains many novel provisions of the Framework Decision[117]. Data protection by design and by default are introduced in Article 20 as two of the obligations of the controller. The competent authorities must take into account these two principles *both at the time of the determination of the means for processing and at the time of the processing itself*.

It is also a novelty that notification of a personal data breach to the supervisory authority as stipulated in Article 30. Moreover, designation of a data protection officer is introduced in Article 32 as a new obligation for the controller. This directive provides new rights to data subjects which include right to receive information by the data subject (Article 13), right of access by the data subject (Article 14), and right to rectification or erasure of personal data (Article 16)[118].

Despite much controversies it was concluded that the directive is a positive improvement towards a comprehensive data protection in EU[119]. Another interesting debate is that the right to data protection and public security seem to be as competing interests (Europol, 2018)[120]. The right to data protection and the right to security can be balanced within a society where the police may seemingly give priority to the obligation to keep society safe over privacy and data protection. As underlined by the European Court of Human Rights' case law [121] the right to the protection of personal

---

by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing "Council Framework Decision 2008/977/JHA

[117] Paul de Hert, Vagelis Papakonstantinou, "The new police and criminal justice data protection directive: a first analysis"*New J. Eur. Criminal Law*, 7 (2016), 7-19

[118]Mark Leiser, Bart Custers " The law enforcement directive: conceptual challenges of EU directive 2016/680"*European Data Protection Law Review*, 5, (2016) 367–378

[119] "Opinion 6/2015 - a further step towards comprehensive EU data protection: EDPS recommendations for the police and justice sector" EDPS, https://edps.europa.eu/press-publications/press-news/press-releases/2015/further-step-towards-comprehensive-eu-data_en,Accessed: 6 Feb 2021

[120] "Freedom and security - EDEN conference report" Europol, https://www.europol.europa.eu/events/freedom-and-security,Accessed: 6 Feb 2021

[121] "Judgment of the Court (Grand Chamber) of 9 November 2010. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. References for a preliminary ruling: Verwaltungsgericht Wiesbaden - Germany. Protection of natural persons with regard to the processing of personal data - Publication of information on beneficiaries of agricultural aid - Validity of the provisions of European Union law providing for that publication and laying down detailed rules for such publication „- Charter of Fundamental Rights of the European Union - Articles 7 and 8 - Directive 95/46/EC - Interpretation of

data is not an absolute right, this right may be limited to ensure that other rights are protected, as protecting society from crime and terrorism.

6.3 Data Protection/Privacy Impact Assessment

The guidelines on how to successfully implement appropriate safeguards for compliance is missing from the Police Directive[122]. One of the provisions requires data controller to carry out a Data Protection Impact Assessment (DPIA) as addressed in Article 27. DPIAs (previously known as privacy impact assessments (PIAs)) are tools to evaluate the origin, nature, particularity and severity of risks to the rights and freedoms of natural persons and to determine the appropriate measures[123].

How member states determine whether a PIA has to be carried out is provided in Article 27(1) as follows: *Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.* Furthermore, Article 27(2) provides a minimum standard for conducting a PIA: *The assessment referred to in paragraph* 1 shall *contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this*

Articles 18 and 20.
Joined cases C-92/09 and C-93/09., Document 62009CJ0092,EUR-Lex

[122] Thomas Marquenie," The police and criminal justice authorities directive: data protection standards and impact on the legal framework", *Comput. Law Secur. Rep*., 33 (2017), 324-340 https://doi.org/10.1016/j.clsr.2017.03.009

[123] See also: "EC, EP Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) "

Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned (EC & EP, 2016a)[124].

PIAs have been studied in detail since 1990s [125]. There are plenty of PIA methods which are proposed by researchers, governments, Data Protection Authorities (DPAs) and standards bodies, and more industry/technology-oriented PIA methods are developed, such as the RFID PIA[126]and Smart Grid DPIA template[127].

Bas Seyyar and Geradts compared several privacy impact assessment (PIA) methods and emphasized the importance of PIA methods and the collaboration between the investigators and PIA practitioners[128].

---

[124] See also: "EC, EP,Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing"

[125] Kush Wadhwa, Rowena Rodrigues, "Evaluating privacy impact assessments". *Innovation Eur. J. Soc. Sci. Res*., 26 (2013), 161-180

[126] Sarah Spiekermann, "The RFID PIA – developed by industry, endorsed by regulators" D. Wright, P.De Hert (Eds.), *Privacy Impact Assessment, Springer Netherlands*, (Dordrecht,2012). 323-346, https://doi.org/10.1007/978-94-007-2543-0_15,Accessed: 23 Feb 2021

[127] "Data protection impact assessment template for Smart grid and Smart metering systems" Smart Grid Task Force 2012–14 Expert 2,https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf,Accessed: 23 Feb 2021

[128] Bas Seyyar and Geradts compared several privacy impact assessment (PIA) methods and selected three that best suit the requirements. Today, do not exists a PIA methodology that is in conformity with the Police Directive with a focus on law enforcement activities. The study demonstrates firstly the importance of conducting a PIA for all forensic platforms. Seized digital material may contain large amounts of common and sensitive personal data of everyone involved in a crime. Hence, the processing for forensic purposes is more likely to result in an interference in the fundamental rights of data subjects. PIAs may be of benefit to minimize this interference. Secondly, the findings from this study strengthen the position that privacy correlates with security. Necessary measures should also be taken to ensure the security of such forensic platforms. This case study reveals that threats in police sector that can lead to privacy risks are rather different from those in other sectors. Collaboration between the investigators and PIA practitioners is crucial in precisely specifying these threats. The implementation of a PIA encourages privacy awareness within the investigators and the developers of a big data forensic platform. It is worth noting that PIAs should be carried out before the development of such platforms. Merve Bas Seyyar, Zeno .J.M.H.Geradts, „Privacy impact assessment in large-scale digital forensic investigations"
Digital Investigation, Volume 33, (June 2020) 200906, https://www.sciencedirect.com/science/article/pii/S2666281720300263#bib1, Accessed: 23 Feb 2021

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is a legally binding international data protection treaty[129]. A further protocol (CETS No. 223) amended and updated the 1981 Convention (i.e. the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 2018). According to the Council of Europe (n.d.), the modernization of the Convention "pursued two main objectives: to deal with challenges resulting from the use of new information and communication technologies and to strengthen the Convention's effective implementation".

In addition to national, regional, and international data protection laws, there are guidelines and principles that have been created by countries and intergovernmental organizations and implemented by public and private sectors around the globe, such as the Organization for Economic Co-operation and Development (OECD)Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (1980; 2013)[130]The EU is taking steps to improve cross-border access to e-evidence by creating a legal framework which will enable judicial orders to be addressed directly to service providers based in another member state.

The regulation seeks to introduce an alternative mechanism to the existing tools of international cooperation and mutual legal assistance. It specifically addresses the problems stemming from the volatile nature of e-evidence and the "loss of location" aspect by setting new procedures for quick, efficient and effective cross-border access.[131]

---

[129] "Council of Europe Convention No. 108 on data protection**"**
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en,Accessed: 22 Feb 2021

[130] „Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" OECD,2013, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, Accessed: 22 Feb 2021

[131] „Regulation on cross border access to e-evidence : Council agrees its position," Council of the EU,2018, https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/,Accessed: 22 Feb 2021

6.4 Future challenges

According to Reza Montasari and colleagues[132] the future challenges could be outlined on three territories, as standardization, automation and providing digital forensic (DF) services at the point of need.

Standardization will enable all subsequent improvements. We cannot standardize all DF processes, so working with forces transforming forensic (TF) will identify the most common high volume processes where standardization is possible.

After standardization has been done, we can automate a process, and where this process is high-volume with low variability, there is the potential to make significant efficiency gains.

Providing DF services at the point of need, a tiered model. Most forces have already moved towards providing DF capability at the front line through self-service kiosks which enable trained officers to extract data from mobile device as by following a locked-down workflow.

7. Summary

In recent years, Information and Communications Technology (ICT) has rapidly advanced, bringing numerous benefits to the lives of many individuals and organizations. Technologies such as Internet of Things (loT) solutions, Cloud-Based Services (CBSs), Cyber-Physical Systems (CPSs) and mobile devices have brought many benefits to technologically-advanced societies. As a result, commercial transactions and governmental services have rapidly grown, revolutionizing the life styles of many individuals living in these societies.

While technological advancements present many advantages, at the same time they pose new security threats. As a result, the number of cases that necessitate Digital Forensic Investigations (DFIs) are on the rise, culminating in the creation of a backlog

[132] Reza Montasari, Richard Hill, "Next-Generation Digital Forensics: Challenges and Future Paradigms," *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, (London, UK, 2019) 205-212

of cases for law enforcement agencies (LEAs) worldwide. Therefore, it is of paramount importance that new research approaches be adopted to deal with these security threats.

The digital forensics is a multidisciplinary research field, involving law, computer science, finance, networking, data mining, and criminal justice. Professionals increasingly faces a mixed set of challenges and issues regarding the efficiency of digital evidence processing and related forensic procedures.

The General Data Protection Regulation (GDPR) is working on to harmonize the secure data processing, storage, use and exchange of personal information.

The Directive (EU) 2016/680 of the European Parliament and of the Council (Police Directive) protects individuals, and at the same time ensures a high level of public security.

The advancement in digital technology continuously opens various new opportunities for the criminals as well as for the law enforcement agencies, which necessitates a fast intensive growth in the digital forensic research and development. A regular follow up the legislation should also accompany these changes in particular the privacy.

Final thoughts: the right to personal data protection is a fundamental right. Victims and witnesses, but also suspects of crimes have the right to have their data duly protected in the context of a criminal investigation or a law enforcement action at the same time, furthermore harmonized laws will make it easier for police or prosecutors to work together in cross-border investigations and to combat crime and terrorism more effectively worldwide.

Bujtár Zsolt[*] - Central bank-issued digital currencies and their characteristics in light of security

1. Introduction

The aim of the study is to highlight the causes of urgent development of Central Bank-Issued Digital Currency (CBDC). The research describes the potential features of CBDC relative to fiat money and a broad view of the roots and predecessors thereof it. The study reviews the potential types and characteristics of CBDC. Finally, yet importantly, the study takes into account the potential security issue of the CBDC and the current solutions providing answers for security concerns.

2. CDBC and fiat money – a comparative analysis

There are four characteristics necessary for a thing to become money. These are certain durability, divisibility, portability, homogeneity, and scarcity. The basic money functions are the medium of exchange, the unit of account, the store of value, and the credit function. The first two functions are already valid for the crypto asset, bitcoin. For the store of value and credit function however there is a need for a more stable environment in terms of the economic and legal framework as well. The most important issue for achieving these latter two characteristics for a money-like instrument is the need for public trust; this trust can be earned or guaranteed by legal actions too.[1]

In the gold standard monetary system, trust in gold or silver provided enough social capital for accepting money issued by commercial banks without deposit-insurance schemes. This public trust was betrayed several times by bankruptcies of bank clients

[*] Senior Lecturer, University of Pécs, Faculty of Law Financial and Business Law Department

[1] This public trust was missing at the issue of first CBDC in Ecuador in 2014 and this lack of trust has lead to the failure of this CBDC experiment. See Lawerence, H. White: "The World's First Central Bank Electronic Money Has Come – And Gone: Ecuador, 2014–2018" accessed January 16, 2021, https://www.cato.org/blog/worlds-first-central-bank-electronic-money-has-come-gone-ecuador-2014-2018

because of bank runs. The process of bank runs in every decade in the late XIX early XX century led to the creation of deposit insurance systems all over the world. After the Great Depression of 1929-33, the gold standard monetary systems ceased to exist. That provided the basis for the widespread emergence of fiat currencies. The issuer country and its economic power legally back these monies. Even in the case of the issuing state's bankruptcy, the legal biding power ensures the money functions of the given state's official fiat currency. As opposed to it, private money let it be a digital one is not backed by any state, only - if at all - by its issuer. In the case of bitcoin since its issuer/developer unknown, even this guarantee is not even available.

Fiat money has the four above-mentioned characteristics, but even with the legal binding behind it, an evaporating public trust can erode its purchasing power. It is so because its purchasing power diminishing due to inflationary periods and to the fact, that decreasing number of available monetary tools are available to keep fiat currency's inflation under control. In the meantime cashless societies, as thereof Sweden presses for digital money, which can be implemented on new technological devices like mobile phones and palmtops, laptops.

CBDCs born to reinvent fiat money to satisfy the needs of the XXI century. This statement can be the distilled summary of the history of CBDC. The fourth technological revolution makes several analog devices obsolete. It is not true in the case of money, but the need for faster money transfer and more mobile money transfer solutions are definitely challenge financial institutions as money transfer intermediaries face in this century.

Fiat currencies have printed form, paper money, and coins as well, but also account type is available in fiat currencies, as one keeps her/his savings in a bank account, which amount, is available for transfer or withdrawal in a paper money form. If digital money would be available only on computer devices, with the opportunity to transfer it to fiat currency. This is a dual money system where fiat money and digital money coexist. This coexistence is already in practice for crypto-assets when a special digital account holder device, called crypto wallet keeps track of the crypto-assets thereof its owner. Crypto-assets transferred into the wallet are bought for fiat money and vice

versa. This is also a pivotal point for taxation,[2] since until investment in crypto-assets does not leave the crypto-assets' world not taxable, but from that point, any gain on it would become taxable income either as investment income,[3] or other income as stipulated by the personal income tax law for the Hungarian taxpayers.[4]

CBDC as digital money issued by solely a central bank has the full faith of the central bank similar to fiat money. This fact though not makes CBDC widely accepted for daily use. The spread of usage also depends on the money usage traditions of the given country. In Sweden people and entrepreneurs support digital money because they use less and less paper or coin as fiat money.[5] In Hungary it is just the opposite, the high cash usage rate was elevated by 10 % during Covid-2019 Pandemic.[6]

As a summary of the comparison between fiat currencies and CBDC, it can be concluded that public trust and money usage customs also needed for the successful CBDC introduction even in the dual money system. An exclusive CBDC money system, however, even in countries with a high number of financial outcasts not a relevant option yet.

[2] Alexander Roland Szívós, "The issues of wealth taxation – the case of Hungary" in *9th Interdisciplinary Doctoral Conference Conference Book,* ed. Beáta Csiszár, Csilla Hankó, , Fanni Luca Kajos, Emerencia Mező, (Pécs, Magyarország: Pécsi Tudományegyetem Doktorandusz Önkormányzat, 2020), 490-498.

[3] Csaba Szilovics, : "Gondolatok a hatékony adórendszer néhány eleméről *JURA* 25, no. 1. (2019): 138-159. and Szilovics, Csaba: Az adótervezéstől az adócsalásig" *Magyar Jog* 60, no. 7, (2013): 407-415.

[4] Alexander Roland Szívós, "Az adórendszer és a pénzügyi kultúra összefüggései" in *Business And Economy In the 21st Century II. – Conference Proceedings,* ed. Csaba Szilovics, Zsolt Bujtár, Barnabás Ferencz, Botond Breszkovics, Alexander Roland Szívós (Pécs, Magyarország: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2020), 56-57.

[5]https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf accessed January 12, 2021

[6]https://www.portfolio.hu/bank/20210115/mnb-10-szazalekkal-tobb-keszpenzt-hasznalunk-mint-egy-evvel-ezelott-465470 accessed January 17, 2021

3. Predecessors and the roots of CBDC

3.1. The predecessors of CBDC

This chapter provides a broad picture of the early predecessors of CBDC, namely the first digital money Cyberbucks, the blockchain technology, and a digital settlement system between financial institutions called RTG. The chapter also provides an overview of the financial needs of the society, which lead to the necessary invention of different digital monies. Finally, it is worth mentioning that the macroeconomic policy especially within it with the monetary policy makes digital money vital for the future.[7]

The first electronic money dates back as early as 1983. *David Chaum*, the researcher of University Berkeley, San Francisco has invented it. His goal was to provide a blind signature for untraceable payments. The system already used the double coding system similar to the one used by the blockchain technology. It consisted of a public code and a private code, both of them needed for a transfer that could be executed by the financial institution. This financial institution issued 1 million pieces of tokens named *Cyberbucks*, which could be accessed by fiat money transfer and could be stored on a PC's hard drive. The financial institution could validate the transfer without actually knowing its identity with the help of a digital envelope in which the codes could be matched. The experiment failed since merchants complained about not having enough users to operate the system while users complained about not having enough merchants to use it at a typical chicken or egg problem.

By 2009, a new more powerful digital money came to life. Bitcoin was the first one of several thousands of crypto-assets, but definitely the most known with certain money characteristics as being a tool of money transfer among private persons and legal entities. Also, it has public and private codes similar to *Cyberbucks* but differs

[7] Zsolt Bujtár, "Central Bank issued digital currency – digital dollar US CBDC" in *Gazdasági kihívások a XXI. században : Konferenciakötet* ed. Csaba Szilovics, Zsolt Bujtár, Barnabás Ferencz, Roland Alexander Szívós, Botond Breszkovics, Zsolt Gáspár, (Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Pénzügyi Jogi és Gazdasági Jogi Tanszék, 2021) 104., 13-22., 10.

from the latter, that it can be held either in a special crypto wallet or a crypto trading platform. This second generation of digital cash came slowly into the limelight and spread gradually to almost all countries of the world. The *distributed ledger technology (DLT)* was the technology platform, which has made it available, not only on a high-performance computer but also on mobile phones too. All crypto-assets like bitcoin, ether, or ripple are based on DLT, but not all digital monies held on the DLT platform.[8] If a person holds savings in crypto-assets, he risks losing the value of his savings, because of the high volatility of crypto-assets relative to fiat money. In the case of fiat money, this volatility is much lower, but in the case of fiat money inflation can erode the value of fiat money as well. This case especially valid for countries, which have hyperinflation like Venezuela in 2019 or Zimbabwe in 2008. The crypto-assets' major advantage relative to fiat currencies is their ability to provide global payment tools to the public within minutes while this process can take days in the case of fiat currencies. Because of this global role, these crypto-assets can serve as a tool for payments all over the world. This fact could result in the global, widespread use of bitcoin, ether, or ripple at a fast pace. That is not happened yet, due to the fact, that these crypto-assets have high volatility, but also because of lack of global legal regulation for crypto-assets.[9] One possible solution for stabilizing these payment tools is to follow what stable coins already do. Stable coins achieve low volatility - similarly to the gold standard monetary system - by holding as many precious metals or fiat currency or basket of fiat currencies as the value of issued stable coins. Among stable coins, Thether[10] is the largest in value and volume and Libra (renamed as Deim) is the

[8] Róbert Szuchy, "A Blockchain technológia alkalmazása a kötelmi jogban" in *Az önvezető járművek és a kontraktuális felelősség. Jogértelmezési nehézségek a személyszállítási szolgáltatási és a bérleti szerződések körében,* ed. Béla Csitei, - Dr. Mário Certicky (Miskolc, Magyarország: Magánjogot Oktatók Egyesülete, 2020), 75-83.

[9] Gábor Szalay, „A kriptovaluták nemzetközi szabályozási trendjei Kriptotőzsdék és ICO-K értékpapírjogi perspektívából" *Jogtudományi Közlöny*, 74. no. 3. (2019): 132-133.

[10] Tether real full USD backing was questioned several times https://www.coindesk.com/tether-lawyer-confirms-stablecoin-74-percent-backed-by-cash-and-equivalents accessed November 10, 2020

most famous. Although the latter one is not operating yet and a new deadline is set in 2020 for starting its operation by the end of 2021.[11]

3.2. The roots of CBDC

Fiat monies are significant and almost sole players in the monetary system. Fiat money systems however face many challenges after the Global Financial Crisis of 2007-2009. Monetary policies made zero-interest policy (ZIRP) a normal and not an exception.[12] Most of the economies could not have the chance to leave the ZIRP behind when COVID-19 Pandemic hit again the world economy with another economic crisis. Bank of Japan and the European Central Bank could not raise their close-to-zero central bank rates, because of the slow recovery of the respected economies, in March 2020 the Federal Reserve also reduced its central bank rate to zero due to the aftermaths of Covid-19 Pandemic. This process made the monetary policies in several countries implementers of Modern Monetary Theory[13]. The increased corporate and consumer indebtedness and the potential inflationary pressure of quantitative[14] and qualitative easing[15] altogether resulted in a decreasing faith in current fiat currencies by 2020. [16]

[11]At the time of renaming, the reserve of basket currency was also changed to only USD pegged one private stable coin. https://www.coindesk.com/libra-diem-rebrand accessed January 10, 2021

[12] Zoltan Zéman,– Peter Kalmár, - Csaba Lentner,:" Evolution Of Post-Crisis Bank Regulations And Controlling Tools: A Systematic Review From A Historical Aspect *Banks and Bank Systems*, 13. no. 2. (2018), 138-140

[13] According to Modern Monetary Theory governments can spend freely to the level where demand meets supply at that point at full employment could make inflation grow, but it could be hold under control by levying higher taxes. https://www.businessinsider.com/modern-monetary-theory-mmt-explained-aoc-2019-3 accessed November 12, 2020

[14] During a quantitative easing program a central bank increases its portfolio of assets from the same asset class for example by increasing the volume of high quality corporate bonds which held already by the monetary authority.

[15] During a qualitative easing program a central bank increases the volume of its asset portfolio by adding new, riskier assets to its portfolio relative to what it has already had. If it is like the monetary authority has bought only bonds and from now on, it would buy shares of listed companies on stock exchanges through ETFs as Bank of Japan did.

[16] Bujtár, "Central Bank issued digital currency – digital dollar US CBDC",

There is another reason to introduce e-money or become a cashless society: it is the relatively high cost of keeping cash type money in circulation as is true in the case of banknotes and coins. In Hungary, this cost can reach as high as about HUF 400-450 billion yearly basis.[17]

Finally yet importantly, one more important that makes digital money of potentially great use for society can be summed up as giving access to financial services to people who are currently financially deprived. This number can reach hundreds of millions of people when taking into account all financial outcasts – hundred of millions of people globally. Digital money also can be very useful when helicopter money[18] or basic income come into fashion during a crisis management[19] of the governments, as was the case in Hong Kong and the United States during Covid-19 Pandemic in March of 2020.[20] This fact is also relevant in the case of Deim. Deim claims its goal, that its cryptocurrency can solve the problems of hundreds of millions of people by providing a cheap and fast payment system for the ones who are most in need and have no access to commercial banks. Deim is a private stablecoin, which means, that issued by a private entity, and all money created is backed by a basket of fiat currencies of a single fiat currency or gold. The tide of stablecoins and among them a potential global player Deim explains the start of a global race for implementing the first CBDC. This competition especially relevant for the United States for two reasons: the first is Facebook's more than 2.2 billion users, who are all potential clients of Deim payment methods, while the second one is that if it succeeds it can pose a danger for the current role of the US dollar as a world reserve currency. This is why almost all major

[17]https://www.napi.hu/magyar_gazdasag/https://www.napi.hu/magyar_gazdasag/penzugyminiszterium-keszpenz-pm-bankkartya.686466.html.686466.html accessed October 101, 2020.

[18] Helicopter money's definition was introduced by Milton Friedman in 1969, but was popularized by former FED Chairman Ben Bernanke in 2002. According to theory, central bank can inject money into the economy to exert inflation or increase GDP. It can be a one-time or a permanent policy action as well. Belke, Ansgar : After the bazooka a bonanza from heaven: "Helicopter money" now?, accessed November 1, 2020, Rome Discussion Paper Series, No. 18-02, Research On Money in the Economy (ROME), 2018

[19] Csaba Lentner,– Zoltán Zéman,: Handling Crisis – Role in the Economy, *Moderni Veda*, no 3. (2016): 45-58.

[20] It would be useful in cases when a government like Biden Administration intends to provide a pay check of USD 1400 for almost all Americans except for the ones in highest income bracket.

financial authorities have raised first their concerns against the fast introduction of Libra. Major criticism came also from traditional commercial banks, being afraid of losing payment revenues and receiving a new competitor having completely different rules with respect to know your customer (KYC) rules and implementing the rules of anti-money laundering (AML).[21]

The roots of CBDC came from two major sources: one is the computer network system and the other one is DLT. Digital or e-money consists of a series of data, which can be retrieved at any time or place without compromise with the relevant code. The duality of digital money vs traditional money is similar to creating securities in our world. The issuer can issue a prescribed amount of stock or bond via printing as a document of proof or as a dematerialized security in the form of series of data.[22] All public companies in Hungary exclusively issues the latter type of security since it is stipulated for the listed legal entities by the law. CBDCs will come to existence in a digital form as dematerialized securities. The person of the issuer was a question, whether it would be issued by the central bank or a separate legal entity. This question seems to be answered for now, as low public trust in privately controlled digital currencies like Diem would make hardly enough trust for its success, after such scandals as Facebook's Oxford Analytica.[23]

4. Potential types and characteristics of the CBDC

CBDC main roots are crypto-assets and digital money. The crypto-assets implemented on the DLT platform - their first type, bitcoin - were born together with DLT. This

[21] Mezei, Kitti,; A kriptovaluták kihívásai a büntető anyagi és eljárási jogban *Pro Futuro - A Jövő Nemzedékek Joga* 9. no. 1. (2019) 87-88.

[22] Botond Breszkovics, "Kriptoszabályozás Wyomingban" in *Business And Economy In The 21st Century II. – Conference Proceedings,* ed. Csaba Szilovics, Zsolt Bujtár, Barnabás Ferencz, Botond Breszkovics, Roland Alexander Szívós (Pécs, Magyarország: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2020), 107.

[23] https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html accessed January 11, 2021.

technology provides the opportunity to issue, store, and retrieve CBDC with high security.[24]

There are two potential flaws of DLT-based crypto-assets: one is the case of control of more than 50 % of nodes[25] and the other is the speed of quantum computers.[26] These problems are not valid for a centralized DLT system, since its owner can control 100 % of the nodes, while the second issue is already addressed, but not solved yet.

Although DLT technology is very attractive, the safety thereof is not a proven 100 %. This is the underlying reason why the author agrees with professor Berentsen and his fellow researcher Fabian Scähr on not risking central banks' reputation by using a DLT technology for a CBDC without the necessary precautions.[27] This technology has not proved its security at the highest level, but rather one can consider it as one possible solution, which has high security, scalability opportunities.

The difference between central bank-issued centralized CBDC and decentralized CBDC is that, who operates the technology that creates the CBDC. In the case of centralized CBDC, creation and operation are fully controlled by either the central bank or its designated affiliate. However, in the case of decentralized CBDC, a central bank gives up its full control of creating money by giving the right to a third party – let it be a private or public, or non-profit entity – to mine or create in any other way the CBDC. That latter fact is a very relevant problem, since issuing money is the monopoly of central banks, as control of the money supply is also an integral part of its monetary policy. Because of this, no central banks yet inclined to support the idea of issuing such money, which is uncontrolled in its quantity by the given central bank

[24] Róbert Szuchy, . "Az új technológiák hatása az energiajogra" in *Technológiai kihívások az egyes jogterületeken*, ed. Árpád Homicskó (Budapest, Magyarország: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2018), 203-216.

[25] It happened with the second largest capitalization crypto-asset, Tether in 2019 https://qz.com/1516994/ethereum-classic-got-hit-by-a-51-attack/ Accessed February 12, 2021

[26] Zsolt Gáspár, "Scamming Investors: Ponzi scheme in the cyberspace", in *Business And Economy In the 21st Century II. – Conference Proceedings* ed. Csaba Szilovics, Zsolt Bujtár, Barnabás Ferencz, Botond Breszkovics, Roland Alexander Szívós (Pécs, Magyarország: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2020), 82.

[27] Aleksander Berentsen, Fabian Schar. *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*, Review, Federal Reserve Bank of St. Louis, 100. no. 2. (2018): 97-106.

without having controlling power over the whole process. One has to mention that in the case of private CBDC the seigniorage[28] income would be given to the issuer of private CBDC by the central bank.

4.1 Wholesale and retail types of the CBDC

There is a very important distinction between two types of CBDCs the wholesale and the retail one. Retail CBDC is the one, which is available for households and non-financial institutions in its widest circle. If only the wholesale financial actors could use the CBDC as it is in the case of wholesale CBDC, then it would not be a completely new digital money, but only the acknowledgment of the status quo, which is one with already in-use for digital settlement, the RTSG.[29] In the following part, the author examines the possible advantages of the two, above-mentioned types of CBDC. From the users' point of view, it is a question, who will be eligible to use CBDC as money, since it has a different circle of eligible users in the case of retail or wholesale type.

Both wholesale and retail CBDCs can be part of a time journey in terms of going back to the one-tiered banking system, in which all economic actors except for households could have an account at the central bank. This would be the case when the CBDC would be implemented without the involvement of financial intermediaries. It is interesting to note, that in Hungary, the one-tiered banking system ceased to exist already in 1987.

According to the current information available from the Chinese, the Swedish, the United States', the European Union's CBDC, although there is no final decision on which technology to apply DLT or not DLT, the decisions are tilted towards DLT type

[28] *Seigniorage is the government's revenue from the provision of the national currency*. *Jens Reich Seigniorage On the Revenue of Creation of Money* (Hamburg, Springer International Publishing AG 2017) 4.

[29] A good example is the Real Time Gross Settlement System (RTSG) see Kumhof, Michael - Noon Clare: Central Bank digital currencies – design principals and balance sheet implications *Bank of England Staff Working paper* (2018) No. 725. 3.

one. Most of the major central banks are in favor of retail CBDC in opposite to the wholesale one.

5. Security issues of the CBDC

Cybersecurity is naturally the most relevant issue for digital money, which is created, transferred and even in most cases held mainly on computer tools connected to or via the internet. This problem should be treated from two different points of views.[30]
One is the DLT system as a whole, whether it can be compromised so closed enough system not to be broken. A system that cannot be closed, cannot be trusted and the user does not accept the payments because of the fear of a double spend.[31] The DLT system can prevent these events, however, when 50 % of nodes acquired by an outside group of users this problem in theory still can occur. The CBDC can solve the problem by using a sole wallet service provider or by using state-controlled wallet service providers or their services have to meet high quality and security standards.
The other circle of targets is the users of the CBDC. Households and legal entities during the use of the CBDC can be an easy target of a cyberattack if they are not cautious to use digital tools for payment carefully. A double identification system can help a lot, but still, there are loopholes with which one's identity and mobile phone can get into the hands of criminals. It means that a safety net for the average user is an important issue to be addressed by the designers of any CBDC.
CBDC similarly to paper money can be a tool for money laundering or even terrorist financing if with anonymity its real users can be hidden from the authorities or service providers. That is the key when this issue can be detected from the start even to prevent criminals to use it as a tool for money laundering on a large scale. Digital currencies if they are DLT-based have dual identification: public and private code. The authorities have the power to use the entry and exit points when fiat money transferred

[30] Flóra, Józan ; László, Kőhalmi Rule of Law and Criminal Law: Thoughts about the criminal justice of the Millennium Era *Journal Of Eastern-European Criminal Law* 4 no. 1 (2017): 214
[31] Gál, István László; Tóth, Dávid, Risk analysis of counterfeiting: money in Hungary and in the EU *Journal of Criminology and Criminal Law / Revija Za Kriminologiju I Krivicno Pravo* 56. no. 3. (2018): 15-17

to become a digital asset at vice versa. This transaction takes place with the use of either wallets or crypto exchanges.[32] Once these service providers' activities controlled by the same anti-money laundering regulation identification processes and criminal punishments with regular control can reach the same effectivity as thereof the traditional banking system.[33] This goal is not too ambitious but as scandals like HBSC's proves it is not over-ambitious either. As to summarize, anonymity should be left only to users not hindering the operation of potential new money but by using the digital money with the necessary anti-money-laundering activities of their service providers as in fiat money systems.

The competition between countries of significant economic power like the USA and China can lead to the digital trade war, which can easily accelerate into a cyber cold war. The actual channel for these cyber cold war activities - among others is - definitely the CBDC as making it not enough trustworthy for being a national currency.

In a broad term using CBDC as a part of the money system can have security issues too. When a CBDC is used either alone or as part of a dual money system it can lead to a collapse of a bank (the bank run) or a banking system of a country (forcing to devaluate its currency without real monetary policy mistakes). It has to be noted, that CBDC would be part of the economic policy and can be a research topic of another study due to constraints of this study's length.

6. Conclusion

The research describes the potential features the CBDC relative to fiat money and a broad view of the roots and predecessors thereof it. The study reviews potential types

[32] For listing of a crypto-asset on a crypto exchange, there is not a prerequisite of an IPO as opposed to the regulated stock exchange. See Kecskés András, Halász Vendel, "A 2003/71/EK irányelv (prospektus irányelv) szabályozási rendszere és a kibocsátási tájékoztatók új szabályozása" *Európai Jog* 19. no. 4. (2019): 10-11 and
András Kecskés , Vendel Halász, "A kezdeti nyilvános részvénykibocsátás kapcsán jelentkező prospektusfelelősség és kezelése" *Európai Jog*, 12. no. 4. (2012): 17-19.

[33] László István Gál, *A tőkepiac büntetőjog védelme Magyarországon* (Pécs: Kódex Nyomda Kft., 2019), 123-129.

and characteristic of CBDC. Last but not least, the study takes into account the potential security issue of the CBDC and the current solutions providing answers for security concerns. It can be concluded, that most of the security issues stem from using DLT. It is also important to note that DLT can provide programming solutions for most of these problems too. The AML problems can be prevented with a well-orchestrated AML regulation for all service providers at which CBDC and fiat currencies change hands. Finally, the dual system with CBDC and fiat money can alleviate the security problems when the introduction of the new money (CBDC) is not in a hurry but designed and introduced with great caution and care.

Dávid Tóth* - The Criminology of Identity theft

1. Introduction

The original form of identity theft was the impersonation of another person with fraudulent intent. An example of a crime can be found in the Bible in the history of Jacob and Esau, where Isaac's firstborn son Esau relinquished his prerogatives for a bowl of lentils in favor of Jacob, but their father was unaware of this. (Genesis 25: 19-34) Later, Jacob went to his already blind father to receive the blessing of the inheritance. He did this in the clothes of Esau and in goatskin so that Isaac would not notice the deception. Among the historical examples we could highlight the case of John Ylmer. Aylmer was practicing medicine in the middle of the 15th century, and in 1449 he escaped to France because he was charged with a murder committed against his wife. Around one year later he went back to England with the Jack Cade pseudonym. He began to organize an army of dissidents against King Henry. He then claimed to be John Mortimer, a relative of Prince Richard of York. Aylmer's army defeated the royal soldiers at Kent. Despite initial success, his army later disintegrated, and Aylmer was killed by Kent Sheriff.[1]

In the modern age, identity theft is an increasing worldwide phenomenon due to the development of information technology. The growth has several reasons. On one hand, more personal information is available on the Internet as people voluntarily share information about themselves on social networks. On the other hand, government, and business agencies store huge amount personal data in large databases. Third, perpetrators constantly attack accessible or hackable sites, cloud services, computers with various techniques (such as hacking, sending viruses) to gain access to this personal information. In addition to cybercrime, we must not forget the

* Senior Lecturer, University of Pécs, Faculty of Law, Department of Criminology and Penal Execution Law

[1] Sandra K. Hoffman and Tracy G. McGinley, *Identity Theft: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO, 2010), 5-7.

physical crimes (theft, fraud), which also increase the scale of this special form of crime.

The aim of the study is to explore the criminological features of identity theft and to formulate prevention proposals in this regard.

2. The concept of identity theft

There is no uniformly accepted definition of identity theft in the literature. In the foreign literature, several names are used for the same phenomenon. On one hand, it is commonly referred to as identity theft (or in German: identitätsdiebstahl), which is more prevalent in the United States[2] and Germany.[3] On the other hand, in the United Kingdom[4] this form of crime is being apostrophized as identity fraud.

According to Charles M. Kahn and William Roberds, in the case of identity theft offender fraudulently uses another person's personal information.[5] Katie A. Farina's also emphasizes fraudulent element when she refers to the Identity Task Force definition: "the misuse of another individual's personal information to commit fraud"[6] According to Biegelman, who wrote a handbook on the subject, gives a simple definition: „identity theft is the stealing of your good name and reputation for financial gain."[7]

Several technical terms have appeared in the Hungarian legal literature as well. In a joint study by Dániel Eszteri and István Zsolt Máté, the term identity theft is used in connection with the conducts committed in software called *"Second Life",*

[2] Martin T. Biegelman, *Identity theft handbook: Detection, prevention, and security* (John Wiley & Sons, 2009), 2.

[3] Georg Borges, Jörg Schwenk, Carl-Friedrich Stuckenberg, Christoph Wegener, *Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte* (Springer-Verlag, 2011), 9.

[4] https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft (retrieved August 18, 2019).

[5] Kahn, C M. and W Roberds. "Credit and identity theft." Journal of Monetary Economics Vol. 55 (2008): 251-264.

[6]Katie A Farina, "Cyber Crime: Identity Theft," *International Encyclopedia of the Social & Behavioral Sciences.*, 2015, 633-637, 633.

[7] Biegelman, *Identity theft handbook: Detection, prevention, and security*, 2.

which simulates virtual reality.[8] Hámori also uses this term, and his definition focuses on the unlawful acquisition of personal data.[9]

In contrast to the above, Zsolt Haig uses the personality theft terminology. Referring to Scwhartau's book[10] , he classifies personality theft in the category of information warfare. If the crime is committed, their victim may suffer damage to their material and human dignity.[11]

Kinga Sorbán uses the term identity theft.[12] According to her, this form of crime has two moments. In the first phase, the offender steals the victim's personal information (e.g., the Social Security Number). The second phase is about the misuse of data. She points out that the Hungarian Criminal Code does not contain any special statutory provisions, and in her opinion this is not necessary, because the related behaviors establish existing crimes.[13]

In my view, all the technical terms are correct and cannot be ranked among them.

There is also an example of a legal definition in the United States. Section 1028 of Chapter 47 of the 18th title of the U.S. Code states that

"Whoever…

- *knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;*
- *knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;*

[8] See further in: Dániel Eszteri and Máté István Zsolt, "Identity Theft in the Virtual World," *Belügyi Szemle*, no. 3 (2017): . 79-107.

[9] Balázs Hámori, "Bizalom, Jóhírnév És Identitás Az Elektronikus Piacokon," *Közgazdasági Szemle*, no. 9 (2004): . 832-848, 840.

[10] Schwartau, W. Information warfare: Chaos on the electronic superhighway (New York: Thunder's Mouth Press, 1994.) 3-13

[11] Zsolt Haig, "Az Információs Hadviselés Kialakulása, Katonai Értelmezése.," *Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata.*, no. 1-2 (2011): pp. 12-28, 14.

[12] Kinga Sorbán, "Az Informatikai Bűncselekmények Elleni Fellépés Nemzetközi Dimenzió," *Themis*, no. 1 (2015): 343-375.

[13] Ibidem

- *knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;*
- *knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;*
- *knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;*
- *knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;*
- *knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or*
- *knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification… shall be punished...”*

If we analyze the definitions, all of them have common elements. All definitions include:

- the object of offense, which is information related to identity;
- a punishable act that can range from acquisition, to misuse;
- a subjective element that typically contains some form of intent (e.g., fraudulent intent),

- lastly, all authors agree that a crime occurs when the victim has not consented to their personal information being accessed and used.

The Hungarian Penal Code does not penalize identity theft as a separate crime, but the conducts related to it can lead to several criminal offenses (fraud, information system fraud, misuse of personal data, misuse of documents, forgery of public documents, misuse of a cash substitute payment instrument).

3. Manifestations of identity theft

There are several typologies of identity theft in the legal literature. The division of Hoffman and McGinley is based on what the crime is against. According to this, a distinction is made between personal and business identity theft.

In the case of personal identity theft, an individual's personal information is obtained with a fraudulent intent. This is usually done for illegal activities such as unauthorized use of services, purchase of goods, theft of money to support other criminal activities. The objects of the offense include the victim's name, address, telephone number, identity card number, bank card number and associated PIN code, biometric data, e-mail address, and mother's name.

Business identity theft is primarily directed against companies, financial institutions, and banks. The purpose of the perpetrator varies, but most often they commit to get financial gain or to cause financial damage. Business identity theft is typically aimed at obtaining the following data: company name, registered office, telephone number, e-mail address, logo, trademark, bank account number, tax identification number.[14]

According to a multi-authored study[15] we should differentiate between four types of identity theft:

- Identity takeover. In this case the offender takes over an existing identity of another individual without his consent.

[14] Hoffman – McGinley, Op. cit. pp. 3-5.

[15] Koops, B J., R Leenes, M Meints, N Meulen and D O. Jaquet-Chiffelle. "A typology of identity-related crime: conceptual, technical, and legal issues". n.p.: *Information, communication & society,* 12(1), (2009): 1-24,.

- Identity delegation. The difference here is that the actor uses an existing identity of another individual with their consent.
- Identity exchange. In this scenario two or more individuals, with mutual consent, use each other's identity. Here the study gives an example of customers swapping loyalty cards in a supermarket.
- Identity creation. As it names suggests this identity existed before and the actor creates a new one.

According to a more chiseled typology,[16] we can distinguish between financial, medical, criminal, synthetic, and child identity theft. As a special category we can also add the so-called identity cloning.

One of the most common forms is the financial identity theft where the perpetrator obtains another person's personal information for financial gain. This form of crime is primarily directed against bank account and credit card details.

A growing problem in the United States is the so-called medical identity theft. The perpetrators are attacking hospitals and health care provider servers to obtain the victims social security numbers. The stolen data can then be traded on the darknet as well. In some cases the perpetrator uses the medical services himself and in other cases he sells the social security number to others. In 2017, 300 health agencies in the United States filed a complaint that their data storage system had been hacked.[17]

In the case of criminal identity theft, the perpetrator identifies himself in the criminal proceedings with a stolen identity card (e.g. driving license). This phenomenon also arose in Hungarian legal practice. According to the No. 2/2004 Criminal law Unifying Decision from the Curia (formerly known as Supreme Court) if there is a criminal procedure against an offender, who presents himself as another existing person and this fact is recorded in public documents by the authorities than offender will commit the felony of false accusation.

And the so called intellectual administrative document forgery shall be applied.

[16] Manap, N A., A A. Rahim and H Taji. "Cyberspace identity theft: The conceptual framework." *Mediterranean Journal of Social Sciences* 6 (2015): 600-602.

[17] https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ (retrieved August 18, 2019).

If the offender even uses an administrative document issued under the name of another person in the criminal procedure against him, he shall be punishable for the felony of false accusation

and the so-called intellectual administrative document forgery alongside false accusation. There were relatively new similar cases before the Hungarian courts. The forgery of public documents also takes place in the case of the transfer of non-photographic documents if they are issued in the name of another person.[18] In another case the perpetrator was found guilty of the crime of forgery of public documents [Criminal Code. Section 342 (1) (b)], as well as the Criminal Offenses with Authentic Instruments [Criminal Code. Section 346 (1) (a)] because when he was illegally parking, he handed over his brother's passport to identify himself for the police officer.[19]

In the case of synthetic identity theft, the perpetrator uses one or more real identifying information another person (or a non-existent person), to create a new synthetic identity. This technique can be used, for example, to open bank account. It can be particularly damaging to someone whose social security number is being stolen.

Child identity theft can also be considered as a shoulder type of synthetic identity theft. In these offenses the perpetrators are trying to get the social security number for children and juveniles. The latency of the crime can last for years. It is possible that the victim only opens a bank account at the age of 18 and by then has already had a considerable amount of debt related to his or her social security number.

A specific case is identity cloning, when the perpetrator tries to obtain and then use not only one, but as much, preferably all, personally identifiable information as possible. The criminal de facto clones the victim, he becomes nothing more than the victim in another place, in another state. The main goal of criminals here is to hide their own identities and start a new life. Identity cloning can take place for purposes such as employment, marriage, and childbearing. The perpetrators are typically illegal immigrants or people with a criminal record.

[18] BH2014. 234. II.
[19] Kúria Bfv.1695 / 2017/6

4. Techniques of identity theft

Without being exhaustive, I will focus on the most common techniques committed for identity theft. According to Zeno Geradts, phishing is most often done by sending fake emails to different accounts. In these they ask to provide their personal information on behalf of the bank. These are usually easy to filter out because they are often sent from free email addresses (gmail, hotmail).[20]

Phishing emails can include a link that can take the user to a cloned page. They typically copy the pages of banks or online stores where the victim can type in their personal information. This phenomenon is called pharming in jargon.[21]

A similar technique to phishing is smishing.[22] In such attacks, the perpetrator sends a short text message (SMS) containing a link to a fake website where the victim can provide its personal information. Criminals usually send text messages asking for a credit card number, personal information, to solve problems that do not otherwise exist (e.g., avoiding to block a customer's bank account).

There have also been examples of criminals setting up a wireless network (Wi-Fi) to which, if unsuspecting users connect, they expose their personal information. This so-called Wi-phising.[23]

Vishing is also a similar phenomenon to phishing. In such cases, the perpetrators try to obtain data related to bank accounts through a telephone call with psychological manipulation (so-called social engineering). In this case, it is not the technology, but the credulity, naivety of the people that will be the main weapon of the attacker.[24]

---

[20] Zeno Geradts, "Identity Theft," in *Encyclopedia of Forensic Sciences*, ed. Jay Siegel (Amsterdam: Academic Press, 2013), 419-422., 419.

[21] Whitson, J R. and K D. Haggerty. "Identity theft and the care of the virtual self." *Economy and Society* 37 (2008): 572-594.

[22] Tajpour, A, S Ibrahim and M Zamani. "Identity theft methods and fraud types." IJIPM: *International Journal of Information Processing and Management* 4 (2013): 51-58.

[23] Ibidem

[24] Biegelman, *Identity theft handbook: Detection, prevention, and security*, 37.

Skimming is another common technique nowadays. The essence of this is that the perpetrators install miniature data recording devices in the opening of ATMs and thus obtain our credit card data.[25]

Lastly, a classic technique of identity theft is unauthorized intrusion (hacking). An example of this was the attack on the DSW shoe store network in 2005, which resulted in the theft of 1.4 million card traffic data from 108 stores.[26]

5. Damage to victims

In the United States, a 2019 report by a polling company called Javelin found that the number of victims in 2018 was 14.4 million.27 Empirical victimology research was conducted by Reyns and Henson on the harm done to victims by perpetrators. The authors conducted a survey of the Canadian population through the Canadian General Social Questionnaire. Their results suggest that routine online activities increase the occurrence of identity theft in a correlative manner.[28]

Damage to victims can be grouped as follows:

- property damage,
- damage to health,
- social and legal damage.

Above all, loss of property is the most common damage suffered widely by victims. According to a report issued by the Federal Trade Commission in 2018, in 2017, identity theft fraud caused a total of $ 905 million in damage to victims.[29]

---

[25] See further in: Dávid Tóth, "A Készpénz-Helyettesítő Fizetési Eszközökkel Kapcsolatos Bűncselekmények Büntetőjogi Szabályozása." in *Doktori Műhelytanulmányok*, ed. Gábor Kecskés (Győr: Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2015), 226-237., 252.

[26] Chawki, M and M Wahab. "Identity theft in cyberspace: Issues and solutions." *Lex Electronica* 11 (2006): 14.

[27] https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt (retrieved August 18, 2019).

[28] Bradford W.Reyns, Billy Henson, "The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory." *International journal of offender therapy and comparative criminology* 60 (2016): 1119-1139.

[29] https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers (retrieved August 18, 2019).

As for health damage, victims can go through emotional trauma, and fear of revictimization can further increase anxiety. Psychological problems can later cause other health problems such as sleep disturbances, headaches, fatigue. Medical identity theft further increases the risks, because after a registered false medical data, the "real" patient can be misdiagnosed and mistreated, which can result in death.

Social and legal damages include civil or criminal proceedings against victims due to the misuse of their names. Their reputation and social esteem may decline. If criminal proceedings are instituted against them, they will have to endure procedural acts, (e.g., wrongful detention, interrogations, and ultimately even a conviction for an act, Justizmord may occur). Not only members of society, but their immediate family environment and can stigmatize victims of identity theft.

A significant proportion of victims of identity theft do not report what happened to them. According to a Harell study,[30] 93% of victims did not report the crime to the police. Most people (68%) missed to file a complaint because their case was resolved differently.

6. Crime prevention suggestions and summary

In my opinion, three actors have a big role to play in crime prevention of identity theft: the state, financial organizations, and individuals.

It is the duty of the state to criminalize the related crimes (even considering a separate statutory provision facts). Law enforcement agencies, however, must enforce the state's criminal power in practice. Finally, there are models abroad for victim support services that deal specifically with victims of identity theft.[31]

Financial organizations have several responsibilities in the context of identity theft, I would highlight the following:

- confidential handling of personal data

[30] Erika Harell, "Victims of Identity Theft" *Bureau of Justice Statistics*, no. 1 (2019): , 1-28, 13.

[31] https://victimsupportservices.org/help-for-victims/crime-types/identity-theft/ (retrieved August 18, 2019).

- compliance with the law,
- setting up up-to-date security systems against potential attacks.

There are several helpful tips for individuals as well:

- share as little information as possible on social media, and only with friends,
- do not take photographs of personally identifiable documents,
- do not store credit card information online, etc.

If trouble has occurred, it is important for victims to be proactive:

- file a report to the police,
- if credit card details have been stolen, it is advisable to block the card and freeze the account,
- and contact financial institutions and victim support services.

Identity theft and related crimes has no borders, so a coordinated inter-state action against offenders is important. This can be particularly effective at the regional level. This requires harmonized legislation and coordinated cooperation between criminal authorities. In this respect, there are positive developments in the European Union. Previously, the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems dealt with this phenomenon only. Another development in this field is the Directive (eu) 2019/713 of 17 April 2019 of the European Parliament and of the Council. This regulation reforms the criminal law regulation of cash substitute payment instruments and deals with the misuse of virtual currencies.

László Kőhalmi* - Einige evidenz- und nicht evidenzbasierte Gedanken über die Sicherheit

1. Konzeptionelle Abenteuer

Eine ziemliche „wissenschaftliche Bürde" halst sich auf, wer versucht, den Begriff „Sicherheit" kurz, aber präzise zu definieren. Die Achillesferse des Problems wurzelt in der Tatsache, dass der Umfang der Subjekte, Objekte und Inhalte, die für die Definition relevant sind, praktisch unbegrenzt ist.

Als Ausgangspunkt kann der in der Rechtswissenschaft oft angewandte sogenannte Ansatz negativer Art einen ersten Ansatzpunkt liefern, da Sicherheit mit Mangel an Sicherheit korreliert. *Antal Ádám* versteht unter Unsicherheit eine Art Bedrohung, Gefahr, Schaden, Schädigung, Benachteiligung, Leiden mit Angst und/oder Qual. Sicherheit ist also ein Gegenpol zu dem, was gerade beschrieben wurde, d.h. sie stellt einen spezifischen Schutz- bzw. Erhaltungszustand dar[1]. Der Begriff von Sicherheit impliziert, dass er nicht bedeutet, dass ein Schaden für Rechtsgüter völlig ausgeschlossen werden kann.[2]

Aus alledem lässt sich auch schließen, dass das begriffliche Gegenteil von Sicherheit nicht Unsicherheit ist, da letztere nicht automatisch mit einem Nachteil verbunden ist[3]. Das Gegensatzpaar von Sicherheit ist der Mangel an Sicherheit. Laut *Ferenc Gazdag* und *Éva Remek* bedeutet dies – bezogen auf den Menschen –, dass die Person

*Professor, Head of Criminology and Penal Execution Law Department, University of Pécs, Faculty of Law

[1] Csaba Vida, „A biztonság és a biztonságpolitika katonai elemei." *Nemzetbiztonsági Szemle* I no. I (2013): 89.

[2] Hans-Jörg Albrecht, „Biztonság és bűnmegelőzés - Objektív biztonság szubjektív biztonság." in *Kriminológiai Tanulmányok* 47, ed. György Virág, (Budapest: OKRI, 2010.), 17.

[3] Antal Ádám, „A biztonság az értékek között." *JURA* 11, no. 1 (2005a): 33.

in Sicherheit ist, die sich nicht in Gefahr befindet. Ängste und Sorgen habe derjenige keine, der die Bedrohung nicht wahrnimmt, das heißt sie nicht „perzipiert“[4].

Die Erweiterung des Sicherheitsbegriffs hat eine substanzielle und eine formelle Dimension. „*Substanziell geht es um die Frage, was Sicherheit ist, durch was Sicherheit bedroht und durch wen Sicherheit hergestellt wird. Formell geht es um die Frage, auf welchem Wege Sicherheitspolitik entworfen und umgesetzt wird*“.[5]

Sicherheit und deren Mangel erschienen und erscheinen in den verschiedenen Zivilisationen in äußerst vielfältigen Interpretationen, und die Interpretation hängt vom Umfang, der räumlichen Ausdehnung, dem technischen Kapazitätsbestand usw. einer bestimmten Gefahr bzw. eines bestimmten Nachteils ab.

Bei der staatlichen Handhabung und Herangehensweise an Sicherheit stellt das Entstehen von Nationalstaaten und die in realen oder fiktiven „Gesellschaftsverträgen“ ausdrücklich oder impliziert enthaltene staatliche Sicherheitsgarantie eine wesentliche Zäsur dar. Staaten sind grundsätzlich damit beauftragt drei „Sicherheitsprodukte“ herzustellen: staatliche Sicherheit, nationale Sicherheit und öffentliche Sicherheit. Die „Ablieferung“ dieser Sicherheitstriade an die Kunden – die Staatsangehörigen – erfolgte und geschieht jedoch nicht durch nette Worte und freundliches Überreden, sondern auf mehr oder weniger grobe Weise, gegebenenfalls unter Einsatz gewaltsamer, militanter Mechanismen[6].

Während die Konfrontation des Kalten Krieges der Vergangenheit angehört, nimmt das Wettrüsten und die Zahl der blutigen Kriegskonflikte nicht ab und die Menschheit kommt der erstrebten friedlichen und sicheren Weltordnung nicht näher.

Nach der Auflösung des rigiden bipolaren Gegensatzes wurde sowohl von Vertretern der Rechtswissenschaft als auch der Politik das Bedürfnis formuliert, ein komplexes Sicherheitskonzept zu entwickeln und anzuwenden, das alle traditionellen und

---

[4] Ferenc Gazdag, and Éva Remek. *A biztonsági tanulmányok alapjai.* (Budapest: Studia Universitatis Communia, 2018), 17.

[5] Albrecht Hans-Jörg, „Der Wandel im Konzept der Sicherheit und seine Folgen für die europäische Innen- und Rechtspolitik.” *JURA* 11, no. 2 (2005): 9.

[6] Antal Ádám, „A biztonság mint jogi érték”. in *Tanulmánykötet Erdősy Emil professzor 80. születésnapja tiszteletére,* ed. Ágnes Balogh & Szabolcs Hornyák, (Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2005b), 13.

neuartigen Bedrohungen für den Menschen und die menschliche Gemeinschaft berücksichtigt[7] [8]. Die verschiedenen internationalen politischen, fachlichen und militärischen Kooperationsmechanismen (z. B. UNO, NATO, Europäische Union) hatten eine bedeutende Rolle und bedeutendes Verdienst bei der immer weiter verfeinerten Definition des Sicherheitskonzepts.

Unter den zahlreichen Ansätzen für den Sicherheitsbegriff verdient der UN-Bericht aus dem Jahr 1994 mit dem Titel „Redefining Security: The Human Dimension“[9] besondere Erwähnung. Laut *Enikő Száraz* ist dieses Dokument die Grundlage für die umfangreiche, jedoch bei weitem noch nicht abgeschlossene Forschung, für die Formulierung von Schlussfolgerungen und Änderungen und für die teilweise Anwendung der inhaltlichen Bestandteile der sog. humanen Sicherheit gewesen[10].

Der Begriff der humanen Sicherheit[11] muss mit holistischem Ansatz unter Berücksichtigung aller Bedrohungen und Schäden für Menschen und menschliche Gemeinschaften und auf interdependente Weise angegangen werden, und das alles schließt die Anforderung und den Schutz der nationalen Sicherheit, der internationalen Sicherheit oder der kollektiven Sicherheit nicht aus. *Antal Ádám* zufolge sind die für die humane Sicherheit unerlässlichen *differentia specifica* die Folgenden: (a.) vorrangige Orientierung an der Menschenwürde, (b.) bevorzugter Schutz für Ausgestoßene, Benachteiligte, für körperlich und geistig behinderte Menschen, (c.) Bekämpfung von Hunger, Armut, Arbeitslosigkeit und verbotener Diskriminierung, (d.) Maßnahmen gegen ansteckende und unheilbare Krankheiten menschlichen, tierischen und pflanzlichen Ursprungs und gegen zwanghafte Verhaltensweisen, (e.) Maßnahmen gegen Naturkatastrophen und technische Katastrophen, Umweltschäden und schockierende Verkehrsunfälle, (f.) Bekämpfung

[7] Ferenc Kondorosi, “A biztonság változásai és a Blackwater szindróma kérdése.” *Katonai Jogi és Hadijogi Szemle* 3 no. 2 (2015): 127.
[8] Antal Ádám, „A biztonság mint jogi érték” ed. Ágnes Balogh & Szabolcs Hornyák, (Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2005b), 15.
[9] Ian Holliday. & M. Brendan Howe, “Human Security: A Global Responsibility to Protect and Provide.” *The Korean Journal of Defense Analysis* 23 no. 1, (2011): 73-73.
[10] Enikő Száraz, „A biztonság új dimenziói.” *Külügyi Szemle 2 no. 2 (2003): 204.*
[11] Ivett Szászi, „A humánbiztonság koncepciója és mérésének lehetőségei.” *Nemzetbiztonsági Szemle* 7 no. 2, (2019): 112-113.

der organisierten und sonstigen Kriminalität und des Terrorismus, sowie (g.) lokale, regionale, staatliche, zwischenstaatliche und globale, aber in jedem Fall koordinierte Maßnahmen zur Bekämpfung von Zerstörungen durch Vandalismus[12].

Es muss erkannt werden, dass der wirksame Kampf gegen die schwerwiegenden Bedrohungen und Probleme heutiger und künftiger Generationen von Einzelpersonen, sozialen Gemeinschaften, dem Staat oder den Staaten allein und isoliert nicht geführt werden kann. Der koordinierte, gemeinsame Kampf gegen die oben genannten Bedrohungen ist das Gebot der Stunde. Die integralen Bestandteile dieses Kampfes reichen natürlich von der Prävention der die Gefahr auslösenden Umstände, über den Einsatz von kontinuierlichen Monitoring-Diensten bis hin zu Mechanismen zur Behebung eingetretener Kataklysmen und Katastrophen[13]. Humane Sicherheit (human security) bedeutet daher grundsätzlich, frei von allen Gefahren und Schäden unserer Zeit zu sein. Da eine Sicherheit solchen Inhalts leider unerreichbar ist, erfordert menschenzentrierte Sicherheit ein äußerst umfangreiches, komplexes Anforderungssystem und vielfältige Präventions-, Abwehr-, Schutz- und Rehabilitationsmaßnahmen.

Die humane Sicherheit ist untrennbar mit dem Schutz, der sog. human security defence, und der Erreichung, Vorbeugung, Abwehr und auch Wiederherstellung beinhaltenden Protektion, der safety, verbunden. All dies erfordert einen holistischen Ansatz, eine komplexe und koordinierte Prävention und die Anwendung sich ständig ändernder Prioritäten, die an die Art, Nähe und Schwere der Bedrohungen angepasst sind.

2. Sicherheit als Rechtsgut

Nach der pluralistischen Axiologie ist der Wert das, was das bewertende Subjekt als Wert ansieht. Der Wert ist somit das Produkt der menschlichen Bewertung, die

[12] Antal Ádám, „A jogi alapértékek harmóniája és versengése". *Polgári Szemle* 2, no. 7-8 (2006): 32-35.

[13] Antal Ádám, „Az alkotmányos jogállam újszerű feladata és működése." in *Ünnepi kötet Ivancsics Imre egyetemi docens, decan emeritus 70. születésnapjára,* ed. Ferenc Csefkó, (Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2008), 52.

Qualität des Objekts, die diesem vom Bewerter beigemessen wird[14]. Welche Werte, in welcher Zusammensetzung und in welcher Reihenfolge sie ein Wertesystem bilden, hängt in erster Linie auch von den bewertenden Subjekten ab. Werte, die weit verbreitet und langfristig verwirklicht/befolgt werden, führen zu Wertvorstellungen, z.B. religiösen Normen. Die menschlichen Bedürfnisse und Ansprüche bringen Werte hervor, und diese schaffen Wertehierarchien. Die sich gegenseitig voraussetzende Korrelation der sogenannten entgegengesetzten Qualitäten – z.B. Hell und Dunkel, Gesundheit und Krankheit, usw. – ist auch in der Dualität von Wertvollem und Wertlosem feststellbar. Es kann festgestellt werden, dass das Gewicht und die hierarchische Position eines jeden Wertes vom Grad der Schädlichkeit, des Nachteils, des Schadens usw. der als sein Gegenteil bestehenden Gefahr bestimmt oder zumindest stark beeinflusst wird[15]. Es gibt tagtäglich unzählige wirkungsreiche Orientierungseinflüsse auf Wertewahl und Wertorientierung, z.B. Religionen, Ethik, Schulbildung, Mode, Politik, Social Media-Portale, usw.

Bei den Werten kommt den rechtlichen Werten eine Schlüsselrolle zu, da sie auch durch Rechtsnormen geschützt sind. Im Bereich der rechtlichen Werte können je nach Art der betroffenen Rechtsnormen und dem Grad und Inhalt der Hierarchie Stufen und Gruppen unterschieden werden, z. B. völkerrechtlicher/supranationaler rechtlicher Wert[16]. Von den rechtlichen Werten sind die sogenannten rechtlichen Grundwerte von herausragender Bedeutung, die den Rahmen und die inhaltlichen Hauptbestandteile anderer rechtlicher Werte bestimmen und hierdurch auch nicht-rechtliche – z.B. wirtschaftliche, künstlerische, kulturelle, usw. – Werte beeinträchtigen. Rechtliche Grundwerte können auch aus bestimmten herausragenden internationalen Dokumenten, supranationalen Verträgen oder sogar aus nationalen Verfassungen abgeleitet werden[17].

Bei der Ausarbeitung und Bereicherung der rechtlichen Grundwerte haben die fortschrittlichen Kräfte und Organisationen der Menschheit – unter Berücksichtigung

[14] István Losonczy, „Jogfilozófiai előadások vázlata." In *Jogfilozófiák,* ed. Csaba Varga (Budapest: Szent István Társulat, 2002): 20.
[15] Antal Ádám, „Értékek és értékelméletek." *Társadalmi Szemle* LII, no. 5 (1997): 7.
[16] Antal Ádám, „Az alkotmányi értékek értelmezéséről." *JURA* 16, no. 2 (2010): 116.
[17] Antal Ádám, „Az alkotmányi értékek fejlődési irányairól." *JURA* 8, no. 1 (2002): 19.

auch der diktatorischen historischen Erfahrungen – nach dem Zweiten Weltkrieg hervorragende Ergebnisse erzielt. Diese Entwicklung ist jedoch kein abgeschlossener Prozess, da Veränderungen der Lebensbedingungen und der wissenschaftliche, technische und wirtschaftliche Fortschritt neue Bedürfnisse, unvorhergesehene Probleme und schwerwiegende Gefahren generieren. Denken wir nur an die Problemlösungspotentiale von Quantencomputern: Selbst die leistungsstärksten herkömmlichen Computer würden Zehntausende von Jahren benötigen – für sie ist es praktisch unlösbar –, um bestimmte Codes zu entschlüsseln. Bisher waren die im internationalen Bankensystem verwendeten kryptografischen Lösungen „sicher", denn selbst wenn ein Superbösewicht aus einem James Bond-Film eine Armee von Supercomputern zum Zweck einer Code-Entschlüsselung aufrüsten würde, würde sein Urenkel den entzifferten Klartext noch nicht erhalten.

Für die Entstehung von Sicherheit als rechtlicher Grundwert können eine Reihe von klassischen rechtsstaatlichen Grundchartas als regulatorischer Vorläufer angesehen werden, wie zum Beispiel:

- Die amerikanische Unabhängigkeitserklärung (1776), in der es heißt: *"Wir halten diese Wahrheiten für ausgemacht, daß alle Menschen gleich erschaffen worden, daß sie von ihrem Schöpfer mit gewissen unveräußerlichen Rechten begabt worden, worunter sind Leben, Freyheit und das Bestreben nach Glückseligkeit."*
- Die Erklärung der Menschen- und Bürgerrechte (1789) der französischen Revolution, die in Punkt II darauf hinweist, dass Freiheit, Eigentum, Sicherheit und Widerstand gegen Unterdrückung natürliche und unveräußerliche Menschenrechte sind. Nach Punkt XII setzt die Gewährung von Rechten die Aufrechterhaltung einer *force publicique* voraus, die dem Wohl des Ganzen und nicht dem der Personen, denen diese Befugnis übertragen wurde, zugutekommen soll.
- Die Verfassung von Massachusetts aus dem Jahr 1780, die besagt (Teil I Artikel X), dass ein jedes Mitglied der Gesellschaft das Recht

hat, dass es durch die bestehenden Gesetze beim Genuss seines Lebens, seines Eigentums und seiner Freiheit geschützt wird[18].

Die Beziehungen zwischen den rechtlichen Grundwerten sind konsistent – im Fall eines „Qualitätsgesetzgebers" –, d.h. sie sind widerspruchsfrei und kohärent, das wiederum heißt, sie bauen aufeinander auf und unterstützen sich gegenseitig in ihrer Durchsetzung. Erfahrungsgemäß funktioniert jedoch eine in der Theorie harmonisch scheinende Beziehung in der Praxis nicht unbedingt. Darüber hinaus besteht häufig eine Konkurrenz zwischen rechtlichen Grundwerten, und spektakuläre Konflikte und Kollisionen sind ebenfalls nicht selten.

Verschiedene Versionen der Sicherheit – nationale Sicherheit, staatliche Sicherheit, internationale Sicherheit, kollektive Sicherheit, öffentliche Sicherheit, Rechtssicherheit, soziale Sicherheit, Gesundheitssicherheit, persönliche Sicherheit, Sicherheit am Arbeitsplatz, Eigentumsschutz, usw. – werden aufgrund des Ergebnisses einer rechtlichen Regelung angemessenen Grades und Inhalts zu rechtlich geschützten Werten, vereinfacht gesagt, zu rechtlichen Werten[19].

Die verfassungsmäßige (grundgesetzliche) Definition der humanen Sicherheit bzw. ihrer bestimmten Bestandteile mit dem entsprechenden Inhalt impliziert, dass solche Sicherheit zu einem Verfassungswert wird und somit einen inhaltlichen Einfluss auf die Gesetze und Vorschriften hat, die die Aufrechterhaltung und den Schutz der Sicherheit regeln. Die direkte Folge dieses Prozesses ist, dass die humane Sicherheit als Verfassungswert einen anderen Schutz durch das Verfassungsgericht und die öffentliche Gewalt im Vergleich zu „niedrigeren" gesetzlichen Werten und dem Schutz vor nicht wertbezogenen Gefahren und Schäden genießt. Im Falle eines Konflikts im Bereich der Rechtsanwendung in Bezug auf die Rivalität oder Kollision zwischen Sicherheit als Verfassungswert und einem anderen Verfassungswert, kann das Verfassungsgericht als letztes Forum – nach Erschöpfung des ordentlichen

[18] István Szikinger, „Téveszmék a biztonságról." in *OKRI Szemle* ed. György Virág, (Budapest, 2012), 19.
[19] Antal Ádám, „A biztonság az értékek között." *JURA* 11, no. 1 (2005a): 36.

Rechtsweges – über Art, Inhalt und Verhältnis des Verfassungsschutzes für die Sicherheit in dieser Rivalität und Kollision entscheiden[20].

3. Kritik an Sicherheitstheorien

Einer der beliebtesten sicherheitspolitischen Ansätze unserer Zeit ist die sogenannte Balance Theory [21], die zu dem Schluss kommt, dass Sicherheit und Menschenrechte in umgekehrtem Verhältnis zueinander stehen[22]. Sicherheit kann nur durch die Einschränkung von Menschenrechten und Freiheiten gesteigert werden, und umgekehrt bedeutet die Erweiterung der Freiheiten eine Verringerung des Sicherheitsniveaus[23].

Die ideengeschichtlichen Keime dieser Konzeption finden sich, wie *István Szikinger* feststellte, bereits in *Thomas Hobbes*' Werk, nämlich dass Menschen in einem von der öffentlichen Hand nicht beschränkten Freiheitszustand nicht in der Lage sind, ihre individuellen Interessen und Bestrebungen den allgemeinen Erwartungen der Gesellschaft zu unterwerfen. Aufgrund der gegenseitigen Bedrohung kann nur eine in ihren Handlungsmöglichkeiten unbegrenzte Kraft bzw. Macht angemessenen Schutz bieten, und diese Macht wäre die Staatsmacht[24].

Nach Ansicht von *Josef Isensee* hat sich die Rolle des Staates in unserer Zeit verschoben, und um das erwartete Niveau der sozialen Sicherheit aufrechtzuerhalten, müsse das Konzept der rein liberalen Macht übertroffen werden[25]. Anstatt des auf das bloße Überwachen beschränkten Funktionierens brauche man immer mehr die Wahrnehmung organisatorischer und dienstleistender Aufgaben, die aktives Eingreifen erfordern. Es bestehe weiterhin die Verpflichtung seitens des Staates von

[20] Antal Ádám, „A biztonság az értékek között." *JURA* 11, no. 1 (2005a): 36.
[21] István Balogh, „Biztonságelméletek." *Nemzet és Biztonság* 6, no. 3-4 (2013): 41-45.
[22] László Korinek, "Merre tart a világ?" *Fundamentum* 10 no. 1 (2006): 83.
[23] Géza Finszter, "Közrend – közbiztonság – jogbiztonság (2000-2015)." ed. Géza Finszter & István Sabjanics, (Budapest: Dialóg Campus, 2017), 153.
[24] István Szikinger, „Téveszmék a biztonságról." in *OKRI Szemle* ed. György Virág (Budapest, 2012), 18.
[25] Josef Isensee, *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates.* (Berlin – New York: Walter de Gruyter, 1983): 17-18.

negativer Ausprägung, die Grundrechte zu achten, aber es sei auch notwendig, Schutz zu gewähren, der Aktivität voraussetzt. Letzterem entspreche das Grundrecht auf Sicherheit[26]. *Uwe Volkmann* weist dagegen neben der eigentlichen Fürsorge- und Gefahrenabwehrpflicht des Staates auch auf die Gefahren staatlicher Exzesse hin. Staatliche Aktivitäten können nämlich so weit gehen, dass sie die Täter von noch nicht begangenen Straftaten negligieren oder liquidieren (*Volkmann* 2004, 700-703)[27]. Dies wiederum fällt bereits in die Kategorie „Gedankenverbrechen" sozialistischer Diktaturen. In diesem Fall kann das Schild „Rechtsstaat" in Bezug auf einen solchen Staat entfernt und muss stattdessen das Aushängeschild „Polizeistaat" aufgehängt werden. Die Schwäche der von *Isensee* vertretenen Auffassung über das Grundrecht auf Sicherheit besteht darin, dass die öffentliche Gewalt in der Praxis, im tatsächlichen, alltäglichen Leben die größte Bedrohung für die menschliche Freiheit darstellt bzw. darstellen kann.

Der Ordnungsfanatismus, die Neugierde, die Machtlust und der Unterwerfungseifer erfordern nach Ansicht von Winfried *Hassemer* den Schutz der klassischen Grundrechte – die Unverletzlichkeit der Wohnung, die Meinungsfreiheit usw. – durch verfassungsmäßige Mittel. Man muss erkennen, dass das Recht auf Sicherheit nur durch Beschränkungen anderer Grundrechte verwirklicht wird. Wenn wir das akzeptieren, unterschreiben wir einen Blankoscheck, der unsere Freiheit einschränkt. Freiheit kann nicht dem Wert nach der Auffassung der öffentlichen Macht ausgeliefert werden[28]. Staatliche Macht, die die Garantie der Sicherheit verspricht, entwertet nämlich die Freiheit[29] und sendet eine Botschaft an die Staatsangehörigen, dass Sicherheit ein „primus inter pares" der Grundrechte sei.

[26] István Szikinger, „Téveszmék a biztonságról." in *OKRI Szemle* ed. György Virág (Budapest, 2012), 23.
[27] Uwe Volkmann, „Sicherheit und Risiko als Probleme des Rechtstaats." *JuristenZeitung* 59 no. 14 (2004): 700-703.
[28] Winfried Hassemer, „Staat, Sicherheit und Information." in *Umbruch von Regelungssystemen in der Informationsgesellschaft – Freundesgabe für Alfred Büllesbach,* ed. Johann Bizer & Bernd Lutterbeck & Joachim Rieß (Stuttgart: 2002), 232-233.
[29] István Szikinger, „Téveszmék a biztonságról." ed. György Virág, 17-36. (Budapest, 2012), 25.

Die obigen Ansätze sehen die Verwirklichung von Sicherheit noch im Rahmen der Rechtsstaatlichkeit[30], aber es gibt Konzepte, die bereits den Rubikon der Rechtsstaatlichkeit („rule of law“) überschritten haben[31]. Im Falle von Ausnahmezuständen, Ausnahmesituationen – z.B. Großkatastrophen, Aufstände, Kampfeinsätze gegen Terroristen und organisierte Kriminelle, usw. – wird das Aufhängen eines Schildes mit der Aufschrift „wegen Funktionsstörung vorübergehend geschlossen“ als zulässig angesehen. Es ist kein Zufall, dass sich das Konzept der „Sekurisation” in Literatur und Politik etabliert hat. Sekurisation bedeutet eigentlich das Scheitern normaler politischer Prozesse, nämlich dass der demokratische Rechtsstaat eine Funktionsstörung hat[32] . All dies ist gefährlich, da Diktator-Kandidaten**,** die Sicherheit versprechen**,** leicht zu entscheidenden politischen Akteuren werden und die Garantieeinrichtungen des demokratischen institutionellen Systems (z.B. Gerichte, Verfassungsgerichtsbarkeit) in Bereitschaftszustand („stand-by-Modus“) versetzen können, wie es auch die aktuellen politischen Schwankungen zeigen.

Einige politische Akteure generieren praktisch eine kontinuierliche virtuelle Kriegssituation**,** um ihre eigenen politischen und rechtlichen Untaten zu legitimieren. Die rechtliche Projektion dieser politischen Stimmungsmache ist das Anti-Terror-Recht, da der rechtliche Grundwert der Sicherheit die legitimierende Basis für die Annahme und Anwendung von Sonderrechten bedeutet, z.B. Standgericht, Ausschluss der Berufung.

Die Anti-Terror-Rechtsnormen ermöglichen eine stärkere und radikalere Einschränkung des Rechts als je zuvor unter Berufung auf das Versprechen einer „schönen neuen Welt“. In diesem politischen Klima ist natürlich das Konzept der rechtmäßigen Folter oder des Auslöschens des Lebens eines mutmaßlichen Terroristen, das im Kern bereits bei Jeremy Bentham zu finden ist, aber welches in

[30] Hans-Jörg Albrecht, „A büntetőjog európaizálódása és a belső biztonság Európában.” *Belügyi Szemle* 48, no. 3 (2000): 36-37.
[31] István Szikinger, „Terrorizmus és jogkorlátozás.” *Fundamentum* 9 no. 3 (2005): 73.
[32] István Szikinger, „Téveszmék a biztonságról.” in *OKRI Szemle* ed. György Virág, (Budapest, 2012), 28

seiner postmodernen Fassung *Alan Dershowitz* zugeschrieben wird, sympatisch[33]. Der brasilianische Elektriker *Jean Charles de Menezes,* der irrtümlicherweise in London aufgrund einer Verwechslung aus nächster Nähe mit sieben Schüssen praktisch hingerichtet wurde, stellt den Preis dieser sicheren Weltordnung dar. Er war zu falschen Zeit am falschen Ort.

Die Sicherheit, die durch die Einschränkung der Garantienormen des Strafverfahrens[34] und durch die Missachtung der Menschenrechte erreicht werden kann, ist wertlos, da ein solcher Zustand die schöpferische Kraft der Gesellschaft zerstört[35].

4. Sicherheit und Migration

Migration als soziales Phänomen ist ein wertneutraler Ausdruck, der eindeutig positive (z.B. Bevölkerungszuwachs und nachteilige (z.B. Menschenhandel) Auswirkungen haben kann[36].

Bereits seit den 1980er Jahren ist ein sicherheitspolitisches Narrativ wahrzunehmen, das die Migration als Gefahrenquelle darstellt[37]. Dieser Ansatz wurde insbesondere nach den Terroranschlägen vom 11. September verstärkt[38]. Heutzutage sind viele wirtschaftlich fortschrittliche Länder der Welt unbemerkt zu multinationalen Gesellschaften geworden, doch die theoretischen Grundlagen für das Verständnis der Kräfte, die die Migration antreiben, fehlen oder sind jedenfalls lückenhaft. Da wir

[33] Alan M. Dershowitz, "The torture warrant: a response to Professor Strauss." *New York Law School Review* 48, no. 2 (2003): 275-278.

[34] Géza Finszter, & László Korinek, "Maradhat-e alkotmányos jogállam Magyarországon? *Jogtudományi Közlöny* LXX no. 12 (2015): 575.

[35] Géza Finszter, "Közbiztonság és jogállam." *Jog-Állam-Politika* I no. 3 (2009): 168.

[36] Margit Rácz, *Uniós kihívások és válaszutak a 2000-es években.* (Budapest: Akadémiai Kiadó, 2007), 71.

[37]László István Gál, "Korrelációs kapcsolat az illegális migráció és a terrorizmus finanszírozásának volumene között." in *A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői*, ed. Gyula Gaál & Zoltán Hautzinger, (Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 2019), 217-224.

[38] Laura Gyeney, "Legális bevándorlás az Európai Unióba, különös tekintettel a családi élet tiszteletben tartásának jogára." in *A Pázmány Péter Katolikus Egyetem Jog-és Államtudományi Karának Könyvei – Doktori Értekezések 6.* (Budapest: Pázmány Press, 2014.) 32-33.

keine evidenzbasierte Antwort auf die Frage „qui prodest?“ geben können, dient Migration Pro und Contra als Feld für verschiedene politische Spiele[39]. Einige zivilgesellschaftliche Theorien, die den Marxismus leugnen oder zumindest kritisieren und die Migration als potenzielle Quelle des Arbeitskräfteangebots betrachten, stützen sich grundsätzlich auf die marxistische ideologische Basis. Die Bewegung von Menschen lässt sich durch die die Migration strukturell bestimmende Dynamik der sich immer weiter internationalisierenden kapitalistischen Wirtschaft, das Interesse des Kapitals, erklären. Alle anderen Argumente sind lediglich – euphemistisch ausgedrückt – ideologisches Gewäsch.

Die Erstellung einer einwanderungsbezogenen Bilanz ist eine scheinbar einfache Aufgabe[40], da durch eine SWOT-Analyse die potenziellen Vorteile (z.B. Bevölkerungswachstum, Arbeitskräfteangebot, Bevölkerung in bestimmten Ländern, Dienstleistungsvielfalt) und Nachteile (z.B. Inzidenz tropischer Krankheiten, Anstieg der Kriminalität, vermindertes Sicherheitsgefühl, Schwarzarbeit, Wettbewerb auf dem Arbeitsmarkt für die Ärmeren) modelliert werden können[41]. Diese Kosten-Nutzen-Analysen sind jedoch aus historischer Sicht eher kurzfristig und sie können nicht zeigen, welche günstigen oder ungünstigen Entwicklungen die innerhalb einiger Jahre potenziell auftretenden Vor- oder Nachteile nach zwei, drei Jahrzehnten in sich bergen. Soziale Wahrnehmungsprozesse sind schwer vorhersehbar und sind mit der Gefahr einer Janusköpfigkeit behaftet[42].

Die Nähe oder die Distanz zwischen sozialen, kulturellen, religiösen, rechtlichen Unterschieden und solchen in der Lebensführung zwischen verschiedenen Völkern stellt inhärent einen Problemfaktor dar. Die die Wahrheit verdrehende Wirkung von auf im Grundsatz richtigen Zielsetzungen basierender Ersatzreligion und politischer

---

[39] László Kőhalmi, “A migráció néhány biztonságpolitikai összefüggése.” *Szakmai Szemle* 12 no. 4 (2016): 83.

[40] Csaba Vida, „A biztonságpolitikai leírómátrix (Elméletek, alapok és alkalmazás).” *Hadtudomány* 21 no. (2011): 36.

[41] Ferenc A. Szabó, *A nemzetközi migráció és korunk biztonságpolitikai kihívásai*. (Budapest: Zrínyi Kiadó, 2006), 11.

[42] Szilveszter Póczik, „Nemzetközi migráció – biztonságpolitikai, rendészeti aspektusok.”in *Új népvándorlás – Migráció a 21. században Afrika és Európa között,* ed. István Tarrósy & Viktor Glied & Dávid Keserű, 35-51.(Pécs: IDResearch Kft./Publikon Kiadó, 2011), 49-50.

Korrektheit – z.B. liefern die Behörden keine oder nur verzerrte Informationen über die Täter von schwerer Kriminalität – macht es schwierig, eine klare Sicht auf der Grundlage von wissenschaftlicher Evidenz zu haben.

Einige Migranten sind nicht bereit, sich zu assimilieren, sie wollen nach ihren eigenen „Regeln" leben. Dies kann sogar zu einer Entstehung paralleler Rechtssysteme in dem betreffenden Land führen. In der No-Go-Zone, die es nicht gibt und die es doch gibt, ist die Polizei nicht mehr Herr der Lage. Als Jo-Jo-Effekt ist jedoch auch vor den Gefahren einer Verschärfung der politischen Extreme (z. B. Fremdenfeindlichkeit) zu warnen[43]. Migranten können von bestimmten politischen Kräften leicht mit kriminellen Risikoprofilen in Verbindung gebracht werden, was rassistische Tendenzen verstärken kann[44] bzw. als Bezugsgrundlage für die Verbreitung stigmatisierender Kriminalpolitik dienen kann[45].

Einflussnahme auf Migrantengruppen bietet günstige Gelegenheiten für verschiedene Geheimdienste[46]. Der Flüchtlingszustrom, mit dem Europa heute konfrontiert ist, würde eindeutig erfordern, dass die politischen Entscheidungsträger die finanziellen und personellen Ressourcen erhöhen, die für nationale Sicherheitszwecke eingesetzt werden sollen[47]. Die neue Migration, die derzeit stattfindet, bedeutet einen massiven Zustrom von Menschen, der keinen gründlichen „Sicherheitsfilter" auf der Ebene der nationalen Sicherheit ermöglicht; das Feedback auf diesem Gebiet ist nur minimal[48]. Man kann nur hoffen, dass verschiedene Terroristengruppen ihre Zellen nicht eingeschleust haben bzw. einschleusen[49].

---

[43] Szilveszter Póczik, „Nemzetközi migráció, kisebbségek, társadalmi kockázatok és megoldások*." Polgári Szemle* 2 no. 12, (2006): 32-33.

[44] Hans-Jörg Albrecht, „A biztonságkoncepció átalakulása és ennek következményei az európai bel-és jogpolitikára." *Belügyi Szemle* 54, no. 2 (2006): 23.

[45] Hans-Jörg Albrecht, „A bűnözésben mutatkozó változások, ezek okai és a kriminálpolitika szerepe." *Belügyi Szemle – Külföldi Figyelő* (2002): 31.

[46] Balázs Laufer, *"A migráció rendvédelmi és nemzetbiztonsági kihívásai."* (PhD diss., Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, 2013), 69-70.

[47] István Resperger, A világ kockázatai. in Nemzetbiztonsági alapismeretek ed. István Resperger (Budapest: Ludovika Egyetemi Kiadó, 2018), 57-61.

[48] Fruzsina Csatlós, „A menekültkérdés kezelésének nemzetbiztonsági aspektusai válságövezetekben és itthon." *Szakmai Szemle* 10, no. 2 (2014): 165.

[49] László Kőhalmi, "Some security aspects of migration." *National Security Review* 3 no. 1 (2017): 80.

Eine beträchtliche Anzahl von Migranten kommt aus Gebieten, in denen die Gesundheitsbedingungen leider eher unterentwickelt sind, was die Gesundheitssicherheit gefährden kann (z.B. Ausbreitung invasiver Arten)[50].

5. Schlussbemerkungen

Sicherheit ist ein bestimmender politischer Mainstream unserer Zeit[51], der Jolly Joker der Politiker, die eine Null-Toleranz-Politik empfehlen[52]. Durch die Propagierung des Schlagworts Sicherheit kann jede gemeine Idee oder jedes gemeine Ziel an die Öffentlichkeit verkauft werden.

Es gibt jedoch ein Sicherheitsproblem, das heutzutage noch relativ oberflächlich behandelt wird, nämlich das Problem des Klimawandels und der damit einhergehenden Folge des Wassermangels, der an die Tür Europas klopft. Einige multinationale Unternehmen privatisieren bereits das Trinkwasser und die apokalyptisch-futuristischen Bilder von Mad Max-Filmen könnten sogar Realität werden. Wer die Kontrolle über das Wasser hat, wird der Herr sein. Trinkwasser wird in absehbarer Zeit von Polizei, Sicherheitskräften und Freiwilligen bewacht werden. Dies ist die größte Sicherheitsherausforderung der Menschheit. Aber auch wenn diese nicht ganz so schmeichelhafte Vision Wirklichkeit werden sollte, sollte man die richtige Einstellung nicht aufgeben: in dubio pro libertate.

---

[50] István Szilárd & Árpád Baráth, „Migráció és egészségügyi biztonság: új foglalkozás-egészségügyi kihívások." in *Pécsi Határőr Tudományos Közlemények XII – Tanulmányok a „Rendészeti kutatások – a rendvédelem fejlesztése című konferenciáról* ed. Gyula Gaál & Zoltán Hautzinger (Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 2011) 269-278.

[51] Hans-Jörg Albrecht, „A biztonságkoncepció átalakulása és ennek következményei az európai bel-és jogpolitikára." *Belügyi Szemle* 54, no. 2 (2006): 3.

[52] Hans-Jörg Albrecht, „Sicherheit, Sicherheitserwartungen und Sicherheitsgefühle. " in *Egy jobb világot hátrahagyni... Tanulmányok Korinek László professzor tiszteletére*, ed. László Kecskés, Géza Finszter, László Kőhalmi, & Zsuzsanna Végh (Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2016,) 131.

Matko Guštin* & Veronika Sudar* - Contemporary Challenges of National Security – the Case of Croatia

1. Introduction

Since their existence, countries have always been exposed to threats, primarily to military threats with a goal on conquering territory. The gradual development of countries as a community also changed security challenges. Thus, the States had to change their security interests. By the mid-20th century, states have concentrated their security resources in territory protection (which they undoubtedly still do today), which is also one of the three constitutive elements of the state. However, today's information age, accompanied by a strong development of computer networks and information systems will impose an obligation on countries to protect their virtual territory which is accessible to broad social groups. While this availability has several advantages, this poses security risks for states, starting from the level of financial investment needed for protection, through education and to concrete implementation. Cybernetics, represented by a unique definition of systems management science, is becoming a new governmental branch which operates effectively according to predefined principles for these cyber threats. In addition to cyber threats, it is important to prevent hybrid wars which directly cause damage to state in the long run, mainly by presenting certain actions of state leaders in a negative context. The aim of this paper is to point out that cyber threats and hybrid wars are indeed threats to national security, and the way normative regulation of these issues as a preventive response of the states themselves to this issue. Specifically, the activities of the Republic of Croatia and the European Union shall be analyzed.

* 5th year student of the Integrated Undergraduate and Graduate Study of Law, Faculty of Law Osijek
* 5th year student of the Integrated Undergraduate and Graduate Study of Law, Faculty of Law Osijek

2. The information age society and the concept of cybernetic action

Modern society exists in information age where the main task is to deliver information on time. The so-called information age society consists of digital literate citizens who are focused on moving away from the classic state-bureaucratic apparatus. They use information (and other technologies) as the most important resource of today characterized by distance from traditional social values. Information as a resource should focus enhanced creativity, primarily on moving away from strict hierarchies and rules.[1] Older authors viewed this society exclusively in an economic-social sense.[2] Modern components of society are: *i)* digital databases (transparency and better accessibility), *ii*) computer and program resources (storage, processing, and data transfer), *iii*) communication channels and systems (enabling communication in general), and *iv*) users.[3] These components are interconnected and cannot function without each other. Their meaningful order is also visible. It starts from the data, as a basic concept, and ends with user. The user must know how to use data as a resource in the best possible way, which is directly reflected in the creation of information capitalism where it is important to have the right information. Consequently, if the information is misused and (or) by the wrong person, it results in a security threat. Therefore, it is necessary to establish quality information systems, specifically regarding the protection of state data. The globalization of social processes also has its impact in the development of the information society, and in particular the concept of information infrastructure also occurs in the European Union. Today, during the information revolution which has been extremely powerful in the last 20 years, more revolutionary changes have occurred than through the long period of industrial revolution. Information is the most valuable resource of a society and requires a high

[1] Dražen Dragičević, *Pravna informatika i pravo informacijskih tehnologija* (Zagreb: Narodne novine, 2015), . 50-51.
[2] Zoran Žugić, „Information and „Information society" as (meta)social concepts," *Politička misao* 24, no. 1 (1987): 64.
[3] Jacinta Grbavac, Goran Popović, and Vitomir Grbavac, „The importance of communication system sin the process of Croatian information society," *Media, culture and public relations* 3, no. 1 (2012): 45.

degree of protection. That is precisely why the information should be seen through the media that directly create society's image.

2.1. The concept of cybernetics

Norbert Wiener named the concept of cybernetics in 1948. He studied this scientific discipline as the legality of managing systems with control of the operation and information exchange as its basic determinants.[4] It follows that cybernetics acts as a protective factor for information and today plays a key role in shaping societies and policies. On the other hand, its opposite concept is cyber threat, which focuses on addressing adequate protection and misuse of information. In addition to acting as a protective factor of information, cybernetics is a much broader area that operates analytically through several developed methods. There is also a theoretical definition of law in terms of the right to information as a form of ethical control over communications, which government conducts when it adopts sufficiently strong legal norms by which it sets effective sanctions.[5] With the development of cybernetics, legal cybernetics developed in parallel, which does not differ significantly from the general definition of cybernetics. Only difference is that legal cybernetics emphasizes the effectiveness of legal norms in the regulation of cyberspace.

2.2. Cyberspace and cyberthreats

Cybernetics mostly works virtually, but its effects are also visible in physical form. The totality of virtual action is called cyberspace. Such virtual action has no set limits and gives a wide possibility of action in it, which is why on the one hand it represents the Internet as a general social network, while on the other hand it represents all those places where some form of communication takes place.[6] Unlimited communication

[4] Željko Panian, *Poslovna informatika: koncepti, metode i tehnologija* (Zagreb: Potecon, 2001), 7.
[5] Norbert Wiener, *Kibernetika i društvo: ljudska upotreba ljudskih bića* (Beograd: Nolit, 1973): 138.
[6] Dragičević, *Pravna informatika i pravo informacijskih tehnologija,* 165.

also leads to an unwanted occurrence in cyberspace - cyber threats. Today, it justifiably represents national security challenges and represents any executed or potential attack on data (as the smallest unit) within an information system. The concept of a cyber threat is of general meaning and consists of: *i*) cybercrime, which is the most regulated area of cyber threats, *ii*) cyber warfare, which are generally used by countries to endanger national security by attacking national information systems, *iii*) cyberterrorism, which has given legitimate fears to states after terrorist attacks occurred in the United States, and *iv*) cyber espionage that can lead to one of the cyber threats mentioned above.[7] A particularly prominent cyber threat is the cyber warfare that "destroys" information systems. This form of warfare is still rare because many countries have managed to eliminate the previous stages of cyber threats in a timely manner and thus prevent unwanted consequences. The basic feature of cyber warfare is that it is not limited in any way - neither geographically, nor temporally, nor in any other way, and the goals are achieved extremely quickly.[8] Also, the key means of this form of warfare are information systems, computers (as physical components) and networks (as virtual components).[9]

3. Croatian legislation

The Republic of Croatia is exposed to numerous global threats which can significantly harm national security. That is why it acts against cyber threats through numerous regulations and the establishment of institutions. The key provision to be linked to cyber security is found in the Constitution of the Republic of Croatia, in Article 37, according to which everyone is guaranteed the security and confidentiality of personal data, and their use is prohibited for a purpose contrary to their collection.[10] The law,

[7] Hrvoje Vuković, „Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj," *National security and the future* 13, no. 3 (2012): 17.
[8] Davor Božinović, *Globalna sigurnost: sigurnosni izazovi u 21. stoljeću* (Zagreb, Narodne novine, 2016): 125.
[9] „Cybernetics," Britannica, accessed January 17, 2021, https://www.britannica.com/science/cybernetics.
[10] Constitution of the Republic of Croatia, Official Gazette No. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.

on the other hand, regulates data protection and supervision over the operation of information systems in the country.[11] This constitutional formulation is the basis for further normative action on the protection of cyberspace and finally national security.

3.1. Criminal law

The Criminal Law of the Republic of Croatia from 2011 regulates criminal offenses against computer systems, programs, and data, leading by the example of the Convention on Cybercrime.[12] The only significant difference from the Convention is the prescribing of specific penalties, while the classification of criminal offenses remains the same as in the Convention itself (more details in Chapter 4. European legislation). According to the Criminal Code of the Republic of Croatia, the criminal offenses in this chapter are unauthorized access, interference with the computer system, damage to computer data, unauthorized interception of computer data, computer forgery, computer fraud and misuse of devices.[13] Regarding the previous Croatian criminal legislation, the Criminal Code from 2011 regulates the criminal offense of unauthorized access, which refers to the computer system, its part or computer data, and for which the legislator imposes imprisonment for up to two years. In the case of committing this criminal offense, according to the computer system of a state authority, the sentence of imprisonment is up to three years.[14] It is not surprising that penalties are imposed for unauthorized access to data and computer systems of public authorities, as this is justified by the fact that most bodies use their data in electronic databases, and the data themselves are extremely valuable, so their destruction or any other form of damage caused, in addition to damage, social danger.[15] This criminal offense was introduced because the old regulations did not provide adequate protection for this increasingly significant problem. The ultimate

[11] Article 37 of the Constitution of the Republic of Croatia.
[12] Criminal Law, *Official Gazzete*, No. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18.
[13] Articles 266 – 272 of the Criminal Law.
[14] Article 266 of the Criminal Law.
[15] Slavko Šimundić, Siniša Franjić, and Krešimir Vdovjak, „HOAX," *Zbornik radova Pravnog fakulteta u Splitu* 49, no. 3 (2012): 478.

purpose of this offense is to protect the computer system and enable data management. Compared to the previous criminal code, this is a new criminal offense.[16] For criminal offenses of interfering with the operation of a computer system, damage to computer data, unauthorized interception of computer data and computer forgery (the specificity of the criminal offense of computer forgery is that the data caused by its commission), imprisonment of up to three years is envisaged for attempting to commit the said offenses.[17] The criminal offense of computer fraud was also regulated by the previous criminal law. It unlawfully obtains unlawful material gain, enters, alters, deletes, damages, or renders unusable computer data, for which a prison sentence of six months to five years is envisaged.[18] Therefore, this criminal offense means, for example, a change in the balance on bank accounts by breaking into computer systems, payment with fake card numbers and other.[19] Compared to the previous criminal law, the criminal offense of computer forgery has been revised by reducing the part relating to state authorities to the criminal offense of unauthorized access. A criminal offense is, also, the misuse of devices which includes the manufacture, purchase, import, sale, distribution, or possession of a device that commits cybercrime offenses, which is punishable by imprisonment for up to three years, and confiscation of devices and destruction of such data.[20]

Cybercrime is also taken seriously as a threat to national security through the Criminal Code. Serious criminal offense can be made against computer systems, programs and data against the computer system or data of state authorities, the Constitutional Court of the Republic of Croatia, local and regional self-government units, public institutions, public companies or international organizations of which the Republic of Croatia is a member (regulated by Article 273 of the Criminal Law, and includes criminal offenses of interfering with the operation of a computer system, damage to computer data, unauthorized interception of computer dana and computer forgery) is

[16] Dragičević, *Pravna informatika i pravo informacijskih tehnologija,* 201.
[17] Article 271 of the Criminal Law.
[18] Article 271 of the Criminal Law.
[19] Goran Vojković and Marija Štambuk-Sunjić, „Convention on cybernetic criminal and penal Code in Croatia," *Zbornik radova Pravnog fakulteta u Splitu* 43, no. 1 (2006): 133.
[20] Article 272 of the Criminal Law.

punishable by imprisonment of up to five years. By defining such a crime, the Criminal Code goes beyond the established framework of the Convention on Cybercrime, which does not provide for special mechanisms for the protection of state computer systems. It is not surprising given the period of its adoption and the numerous changes that subsequently occurred, so in its context, the crimes of this group are characterized as qualified.[21]

3.2. Preventive normative-institutional system

3.2.1. Preventive legislation

Criminal legislation and courts play main role in defending cyberspace. But there are several national authorities acting preventively. First, the "preventive" legislation of the Republic of Croatia dealing with this issue is:

- Homeland Security System Act,[22] which establishes the overall institutional framework for security risk management and crisis management, and cyber security is undoubtedly part of our national security,
- Cyber Security Act of Key Service Operators and Digital Service Providers,[23] which regulates procedures and measures for achieving a common level of cyber security by digital service providers, and generally with the aim of functioning of the digital market,
- National Security Strategy of the Republic of Croatia,[24] which sets a clear vision for the protection of its population, sovereignty, national identity and human rights and freedoms,

[21] Ivica Kokot, „Criminal-law Protection of Computer Systems, Programs and Data," *Zagrebačka pravna revija* 3, no. 3 (2014): 325-326.
[22] Homeland Security System Act, *Official Gazette*, No. 108/17.
[23] Cyber Security Act of Key Service Operators and Digital Service Providers, *Official Gazette,* No. 64/18.
[24] National Security Strategy of the Republic of Croatia, *Official Gazet*te, No. 73/17.

- Information Security Act,[25] Article 2, where information security is defined as a state of confidentiality, integrity and availability of data that is achieved through the application of prescribed measures and standards, and it is the most important document,
- National Cyber Security Strategy,[26] which establishes the principles of inclusiveness, integration, proactive approach and strengthening resilience as key in combating cyber threats.

Sectors in which cybersecurity needs to operate are the public, academic, and economic sectors. All the regulations listed so far indicate seriousness of cyber threats. That is why the National Cyber Security Strategy lists data protection, technical coordination of computer security incident handling, international cooperation, and education, research, and awareness-raising on cyber security as key links to cyber security.

In addition to the National Cyber Security Strategy, the National Security Strategy of the Republic of Croatia also has significant importance. Strategy pays particular attention to the global level of protection, more precisely to the problems arising from the development of information and communication technologies. Attacks in cyberspace threaten individuals, organizations, and states, and these attacks in cyberspace cause casualties and damage to the material world.

The way to combat attacks in cyberspace is envisaged by using new knowledge and technologies, but also by better knowledge of the human rights and freedoms protection system. The Armed Forces of the Republic of Croatia also play an important role in the fight against cyber-attacks.[27]

The Information Security Act aims to achieve a high level of information security through: *i)* security checks, *ii)* physical security, *iii)* data security, *iv)* information system security, and *v)* business cooperation security. This regulation is significant since it presented the beginning of the harmonization of Croatian information

[25] Information Security Act, *Official Gazette*, No. 79/07.
[26] National Cyber Security Strategy, *Official Gazette*, No. 108/15.
[27] „Exercise Cybernetic Shield 2019 hel at the Ministry of Defense.“ Office of the National Security Council, accessed January 18, 2021, https://www.uvns.hr/hr/aktualnosti-i-obavijesti/u-ministarstvu-obrane-odrzana-vjezba-kiberneticki-stit-2019.

legislation with European one. Thus, CERT was established as a national body for the prevention and protection against computer threats to the security of public information systems.[28]

3.2.2. Institutional organization

Institutional organization is also needed for cybersecurity regulations security and implementation. Key institutional organizations are:

- National Security Council, which represents the central coordinating body of the security system of the Republic of Croatia with the task of considering and assessing security threats and risks, adopting guidelines and conclusions on ways of protection and realization of national security interests,[29]
- Institute for Information Systems Security, a technical body that performs more specific tasks, such as standard security of information systems and their security accreditation, management of cryptocurrencies and general tasks of computer threat prevention,[30]
- Security Intelligence Agency perform the detection and control of cyber-attacks against state systems and cooperate with national authorities and other international partners for this purpose,[31]

It is important to note that the organizational sector of the Ministry of the Interior, and the Cyber Security Service, which participates in the implementation and development of the national legislative framework, participates in numerous activities aimed at preventing these threats, analyzes crimes related to cyber-attacks and performs several other tasks.[32] The Armed Forces of the Republic of Croatia also find

[28] Articles 8 and 20 of Information Security Act.
[29] „About us," Office of the National Security Council, accessed January 18, 2021, https://www.uvns.hr/hr/o-nama/vijece-za-nacionalnu-sigurnost.
[30] „About us," Institute for Information Systems Security, accessed January 18, 2021, https://www.zsis.hr/default.aspx?id=13
[31] „Cyber Security," Security Intelligence Agency, accessed January 18, 2021, https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/.
[32] Article 96 of the Regulation on the Internal Organization of the Ministry of the Interior, *Official Gazette*, No. 97/20.

their role in the defense of cyberspace, so the cyber exercise Cybernetically Protects is held within the Ministry of Defense. This exercise is a simulation exercise in which important actors of the Coordination for the Homeland Security System can monitor the functioning of the entire system in crisis situations.[33]

3.3. Actual security level

The analysis of the normative and institutional structure, as well as strategic interests, undoubtedly shows that countries today clearly experience cybersecurity as a real threat to national security. Although states create mostly a high-quality institutional framework in the fight against cyber threats, security intelligence agencies play a key role. According to the National Security Agency of the Republic of Croatia, even seven attempts of cyber-attacks against state information systems have been detected in 2016.[34] On the other hand, the intentions of cyber-attacks include the collection of data on Croatian security, political, economic, and other processes, as well as data on Euro-Atlantic associations of which the Republic of Croatia is a member.[35] The 2017 report provides concrete examples of cyber-attacks through the Internet forms. It is crucial to note that the cyber-attacker does not have to directly obtain the data of the computer owner, because databases located on that computer are the real target.[36] Speaking on concrete cybercrime indicators in the Republic of Croatia (2018), 33% of frauds are related to cybercrime, every third organization has faced cybercrime, and 47% of business respondents said that cybercrime interrupted or disrupted their

[33] Office of the National Security Council, „About us."
[34] „Public Report of the Security and Intelligence Agency of the Repubilc of Croatia for 2017," Security Intelligence Agency, accessed January 17, 2021, https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/.
[35] Security Intelligence Agency, „Public Report of the Security and Intelligence Agency of the Republic of Croatia for 2017."
[36] „Public Report of the Security and Intelligence Agency of the Republic of Croatia for 2018," Security Intelligence Agency, accessed January 17, 2021, https://www.soa.hr/hr/dokumenti/javni-dokumenti-soa-e/.

business processes.[37] However, the awareness of citizens about the dangers of cybercrime are visible and developing, so 53% of respondents would share information about this type of attack.[38]

When it comes to cybercrime, it is necessary to consider the statistical indicators of the Ministry of the Interior of the Republic of Croatia. According to the Statistical Survey of the Ministry of the Interior of the Republic of Croatia for the year 2019, total of 2 930 cybercrime offences were reported, 2 768 were successfully resolved while 1 844 cybercrime offences were subsequently detected. Of the total number of cybercrime offenses, the most - 1,785 of them were computer fraud offenses, followed by computer forgery and exploitation of children for pornography. Compared to the year before, in 2018, the number of criminal offenses of computer fraud increased by 36.3%, computer forgery by 2,865.3% and the exploitation of children for pornography by 78.2%. Generally speaking, in 2018, a total of 1,564 criminal offenses of cybercrime were recorded, so in 2019 there was an increase in these criminal offenses by as much as 87.3%. Geographically, the largest number of cybercrime offenses in the Republic of Croatia was recorded in the wider area of the city of Zagreb, mountain areas and the central part of the Adriatic. The lowest number of cybercrime crimes in the Republic of Croatia was recorded in the mountainous area of Lika and central Croatia.[39]

4. European legislation

At the beginning of the 21st century, which can justifiably be considered the information age, the Council of Europe, as a separate European organization dealing with the protection of human rights and freedoms, adopted the Convention on

[37] „Research on economic crime and fraud in Croatia – Report for Croatia for 2018.“ PricewaterhouseCoopers, accessed January 17, 2021, https://www.pwc.hr/hr/usluge/forenzicke-usluge/globalno-istrazivanje.html.

[38] PricewaterhouseCoopers, „Research on economic crime and fraud in Croatia – Report for Croatia for 2018.“

[39] „MIA Statistics and Road Safety Bulletins,“ Ministry of the Interior, accessed January 17, 2021, https://mup.gov.hr/pristup-informacijama-16/statistika-228/statistika-mup-a-i-bilteni-o-sigurnosti-cestovnog-prometa/283233.

Cybercrime.[40] This Convention classifies cybercrime offenses into several groups: *i)* criminal offenses against the secrecy, integrity and availability of computer data and systems, *ii)* computer criminal offenses, *iii)* criminal offences relating to the content of offences related to child pornography, and *iv)* criminal offenses against copyright and related rights.[41]

In the European Union, the Directive of the European Parliament and Council on measures for a high common level of security of network and information systems throughout the Union is significant.[42] The key purpose of this Directive is to harmonize cybersecurity legislation throughout the European Union. This Directive sets as basic objectives the obligation of Member States to adopt national strategies for the security of network and information systems, the creation of groups for cooperation between states, creation of the "CSIRT network" which would allow Member States to respond effectively to cyber-attacks.[43] The European Union bases its concrete actions on the work of numerous agencies, so in the field of cyber security there is the European Union Agency for Network and Information Security, which performs all tasks related to the protection of information security in the EU.[44] The role of this Agency was reflected in the adoption of the Cybersecurity Act (in legal force, this Act is a regulation that is directly applicable in the Member States).[45]

5. Disinformation warfare

Although they are part of our reality, hybrid wars still do not have a uniform definition. But the concept of a hybrid war, however, indicates that it is a new,

[40] „Details of Treaty No. 185," Council of Europe Portal, accessed January 18, 2021, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[41] Article 10 of the Convention on Cybercrime.
[42] Directive of the European Parliament and the Council on measures for a high common level of security of network and information systems throughout the Union, Official Journal of the European Union, L 194/1 from July 19, 2016.
[43] Article 1 of the Directive on measures for a high common level of security of network and information systems throughout the Union.
[44] „About ENISA," European Union Agency for Cybersecurity, accessed January 18, 2021, https://www.enisa.europa.eu/about-enisa.
[45] Cybersecurity Act, *Official Journal of the European Union*, L 151/15.

advanced, and sophisticated method of warfare, as well as the fact that information is the most important resources of today. Hybrid wars are the use of propaganda, disinformation, hacker attacks and information warfare for the purpose of political, economic or any other purpose, or hybrid action that includes the use of media and fake news.[46] The concept of information war fully corresponds to today' s information society in which it is important to have the right information, so it is not surprising to use misinformation in order to achieve various, primarily market goals. The question of endangering national security by hybrid warfare, hybrid action, or special warfare, is more than obvious. This security is threatened in the first place by showing weakness of security intelligence agencies in combating this form of attack (this does not mean that security intelligence agencies or national news agencies should censor or carry out any other actions against the media, but such delicate media appearances should be well checked and analyzed). On the other hand, the position of the state in international relations is endangered. An even more dangerous effect of hybrid action exists when it turns into daily political squabbles that divert attention from more important topics and again present the state in a frivolous outward light. That is why such threats affect national security and are proof that states have had to develop their security strategy in a multidimensional way.[47]

6. Conclusion

After everything mentioned above, the thesis that cyber threats and hybrid, special wars are threats to national security is clearly confirmed. When it comes to cyber threats, the danger lies precisely in the fact that they are virtual and that they can meet the opponent completely unprepared and thus lead to extremely severe consequences.

[46] „What is a hybrid war and is it being fought in Croatia?" Večernji list, accessed January 18, 2021, https://www.vecernji.hr/vijesti/sto-je-to-hibridni-rat-i-vodi-li-se-on-u-hrvatskoj-1210522.

[47] Davor Solomun, Critical infrastructure security in an expanded national security concept, in *Proceedings of III. International scientific-professional conferences "New security threats and critical national infrastructure,"* ed. Krunoslav Antoliš (Zagreb: Police Academy – Service for the Development of Police Education and Publishing and Book Activity, 2013): 346.

On the other hand, hybrid wars are somewhat less intense on national security, which are generally perceived as a distortion of information by media activities aimed at undermining state credibility in international circles.

Although a small country, the Republic of Croatia has taken seriously the challenges of a globalized world and regulated the issue of cyberspace protection according to the highest world standards. Especially significant is the parallel action of the so-called preventive and criminal legislation, which penalizes existing threats and prevents potential ones. Cybernetic action as a modern form of attack on national security shows the practical implementation of numerous theoretical postulates on national security, but also the idea of human rights. In addition to classical human rights, some other things are important to the population of a country today, such as data protection and freedom in virtual (cyber) space.

Mészáros Pál Emil* - Jóhiszemű pervitel és annak problematikája a Polgári perrendtartásban

1. Bevezetés

A jóhiszemű eljárás, mint alapelv a felek illetve a bíróság jogait és kötelezettségeit általánosságban meghatározó, korlátozó jogintézmény. Az eljárási alapelvekkel összefüggésben legszorosabb kapcsolata az igazmondási kötelezettséggel van, azonban annál tágabb körű és túlmutatóbb alapelv. Az igazmondási kötelezettség alapján a felek nem állíthatnak olyan tényeket, amelynek valótlanságáról tudnak, továbbá nem vitathatnak olyan tényeket, amelyek valóságtartalmában biztosak.[1] A jóhiszemű joggyakorlás elve tárgyát tekintve nem kizárólagosan a nyilatkozatokra, hanem a felek valamennyi perbeli cselekményére kiterjed. Az igazmondási kötelezettség, valamint a jóhiszemű joggyakorlás követelményének megsértése hasonló következményekkel jár, hiszen pénzbírság vagy egyes perbeli cselekmények figyelmen kívül hagyása, mint szankció alkalmazására kerül sor.

2. A jóhiszeműség elvének alapjai

A liberális polgári per során a jóhiszemű pervitel, mint követelmény nem jelent meg. Ezen felfogás alapján a jogvitát a felek magánügyének tekintették, ahol a „jogért folytatott küzdelem" zajlott[2], így ezen alapelvek alkalmazhatóságára nem volt lehetőség. Ugyanakkor a liberális polgári per elvei alapján készült 1877. évi német polgári perrendtartás is épített be biztosítékokat a felek magatartásával szemben.[3] Ilyen biztosíték volt például, hogy a bíróság az alperes védekezését figyelmen kívül

---

* Tanársegéd, Büntető és Polgári Eljárásjogi Tanszék

[1] Varga István, Éless Tamás, *Szakértői Javaslat az új polgári perrendtartás kodifikációjára (Budapest*, HVG-Orac Kft., 2016.) 41.

[2] Jhering, Rudolf, *Das Kampf ums recht*, (Wien, 1873.) 34.

[3] Habscheid, Walther, *Richtermacht oder Parteifreiheit? Über Entwicklungstendenzen des modernen Zivilprozessrech*ts (Zeitschrift für Zivilprozess, 1968.) 179.

hagyhatta, ha azt nagyfokú gondatlanság miatt nem időben tette meg az alperes.[4] A szociális per eszmélye alapján készült 1895. évi osztrák polgári perrendtartás már tartalmazta az igazmondási kötelezettséget, mint alapelvet. Az alapelv bevezetése szorosan kapcsolódott azon tényhez, miszerint a bíróságnak a jogvédelmet nemcsak az ítélet révén, hanem az egész eljárásban kell biztosítania.[5] Ez alapján a felek nem valós tényállításai során közre kellett hatnia és a pert megfelelő mederben kellett tartani a bíróságnak. Az igazmondási kötelezettség a „Plósz Sándor féle" 1911. évi Polgári Perrendtartásunkban is megjelent, hiszen a törvény a német és az osztrák polgári perjogot tekintette alapjának. A törvény alapján pénzbírsággal lehetett marasztani azt a felet, aki nyilvánvalóan valótlan tényt állított vagy tagadott legjobb tudomása ellenére.[6]

A szocialista polgári per alapján megalkotott 1952. évi polgári perrendtartás az igazmondási kötelezettségen túlmutatva és azt magába olvasztva, már tartalmazta a jóhiszemű eljárás alapelvét.[7]

A jóhiszemű eljárás elvének tartalmi köre szélesebb, hiszen minden olyan cselekményt vagy magatartást magában foglal, amely alkalmas a per elhúzására[8] vagy a tisztességes eljárás lefolytatását meghiúsítja. A jóhiszemű eljárás elve egyfajta biztosíték, mivel az egyes más eljárási alapelvek által biztosított jogok visszaélésszerű használat megakadályozásának eszköze.[9] Ezen alapelv megsértésének következménye közvetlen illetve közvetett jellegűek lehetnek.[10] Közvetlen jellegű következmény a rosszhiszemű magatartás miatt kiszabott pénzbírság vagy egyes nyilatkozatok megtételének kizártsága. Közvetett következmény a rosszhiszeműen okozott felesleges perköltség viselésének kötelezettsége pernyertesség esetére is, amelyre példa lehet a bírósági meghagyással szembeni ellentmondás illetékének

[4] Kengyel Miklós, *A bíróság és a felek közötti felelősségi viszony a polgári per*ben (Budapest, ELTE-ÁJK, 1989.) 15.
[5] Klein, Franz, *Zeit- und Geistesströmungen in Pro*zesse (Dresden, 1901., Frankfurt, 1943.) 28.
[6] Kengyel Miklós, i.m. 54.
[7] 1952. évi III. törvény 5. §
[8] Bacsó Ferenc, (Szerk) Beck Salamon, Móra Mihály, (Szerk) Névai László, Magyar Polgári Eljárásjog (Budapest, Tankönyvkiadó, 1962.) 83.
[9] Szerk.: Beck Salamon, Névai László, i.m., 84.
[10] Névai László, Szilbereky Jenő, *Polgári Eljárásjog* (Budapest, Tankönyvkiadó, 1977.) 80.

viselése. A hatályos 2016. évi CXXX. Törvény (Továbbiakban: Pp.) a korábbi szabályozáshoz képest absztrahál, továbbá példálózó jelleggel sem határoz meg magatartásokat, amelyek a jóhiszemű pervitel szabályaival ellentétesek. Ezen jogalkotói döntéstől függetlenül a kialakult bírói gyakorlat a továbbiakban is követendő.

3. A jóhiszemű pervitelről általánosságban

A bíróság köteles biztosítani, hogy a felek és a per többi résztvevője jogaikat rendeltetésszerűen gyakorolják és perbeli kötelességeiknek eleget tegyenek. Ez egyben megalapozhatja a tisztességes eljárás követelményének teljesülését is.[11] A bíróság köteles megakadályozni minden olyan eljárást, cselekményt, vagy egyéb magatartást, amely a jóhiszemű joggyakorlás követelményeivel ellentétes, így azt, amely a per elhúzására irányul, vagy erre vezethet. Ki kell emelnünk azt a tényt, miszerint a jóhiszeműség - principle of good faith - a magánjogban olyan objektív követelmény, mely az eljárási jogok gyakorlása és a perbeli kötelezettségek teljesítése tekintetében is objektív zsinórmértéket jelent. Az objektivitás alatt azt értjük, hogy a jóhiszemű eljárással ellentétes magatartások, cselekmények megállapíthatósága független a jogalany szubjektív tudatától, annak megítélése körében a magatartás szubjektív oldalának nincs relevanciája.[12]

A bíróság a feleket a perbeli jogok jóhiszemű gyakorlására figyelmeztetni köteles. A figyelmeztetésnek ki kell terjednie a rosszhiszemű pervitel következményeire is. A bíróság pénzbírsággal sújtja azt a felet vagy képviselőt, aki akár a tárgyaláson, akár valamely periratban jobb tudomása ellenére vagy nagyfokú gondatlanságból:

- az ügyre vonatkozó olyan tényt állított, amelyről bebizonyult, hogy valótlan, vagy az ügyre tartozó olyan tényt tagadott, amelyről bebizonyult, hogy igaz,

[11] Kiss Daisy: „A fair eljárás“. In: Papp Zsuzsanna (szerk): *A magyar polgári eljárásjog és az EU jogharmonizáció a kilencvenes években.* Dr. Németh János egyetemi tanár tiszteletére (Budapest, ELTE, Eötvös Kiadó, 2003.) 117-140.

[12] Gáspárdy László, *Alapvető elvek, in: Polgári eljárásjog - Kommentár a gyakorlat számára* (szerk: Petrik Ferenc) (Budapest, HVG-ORAC Kiadó, 1994.) 21.

- olyan tényt elhallgatott, amelyről tudnia kellett, hogy a per eldöntése szempontjából jelentős, vagy
- nyilvánvalóan alaptalanul hivatkozott valamely bizonyítékra.

A bíróság pénzbírsággal sújtja azt a felet, aki valamely nyilatkozatot indokolatlanul késedelmesen tesz meg, vagy azt felhívás ellenére sem teszi meg és ezáltal a per befejezését késlelteti. A bíróság azt a felet, aki egyes perbeli cselekményekkel indokolatlanul késedelmeskedik, valamely határidőt, vagy határnapot mulaszt, vagy más módon felesleges költségeket okoz, a törvény értelmében a költségek megtérítésére való kötelezésen felül - pernyertességre, pervesztességre való tekintet nélkül - pénzbírság megfizetésére kötelezi, továbbá a feleket a törvényben meghatározott más jogkövetkezményekkel sújtja. A Pp. az eljárásbeli jogok rendeltetésellenes gyakorlásának valamennyi lehetséges esetén átfogja és megszabja a visszaélésszerű joggyakorlás következményeit is, amelyet az adott ügyben eljáró bíróságnak kell alkalmazni. Ezeknek az eljárási jogi jogkövetkezményeknek alkalmazására külön perben nincs lehetőség, a Ptk. 5. §-a pedig nem a rosszhiszemű pervitel jogkövetkezményeinek megalapozására szolgál.[13]

4. A kereset benyújtása és kiterjesztése

A jóhiszemű pervitel kérdése a perindításkor is felmerül. Elképzelhető véleményem szerint az, hogy egy „notórius" perlővel szemben, akár pénzbírságot is kiszabjon a bíróság, amennyiben a perindítás egyértelműen megalapozatlan és csak az ellenérdekű fél zavarására használják. Általánosságban azonban a magánjogi jogviszonyokban kialakult érdemi vita, konfliktus kezelésének jogállami eszköze a perindítás. A perindítás önmagában nem alapoz meg személyiségvédelmet az ellenérdekű fél javára akkor sem, ha a jogosnak vélt igény alaptalannak bizonyul.[14] Amennyiben a jogkereső állampolgár peres eljárást indít jogosnak vélt érdekeinek védelme érdekében, majd később pervesztes lesz, úgy ez nem alapozhatja meg a jóhiszemű pervitel megsértését, illetve ezen okból kifolyólag vele szemben nem lehet

[13] Kúria Pfv. 20.367/2015/6.
[14] BDT2017. 3691.

peres eljárást indítani. Nem érhet senkit hátrány amiatt, ha az általa jogosnak vélt, szerződésszegés miatt fennálló követelését peres eljárásban, rendeltetésszerű joggyakorlás mellett érvényesíti, még ha az alaptalannak is bizonyul.[15]

A fent tett megállapításomat a kialakult bírói gyakorlat is megerősíti, miszerint a rosszhiszemű perlekedést az állam nem támogatja. A bírói úthoz való alapvető jogból – amely a felek nyilvánvaló joga[16] - nem következik, hogy az államnak a rosszhiszemű perlekedést és ennek kibontakozását is támogatnia kell.[17] A költségmentességgel kapcsolatos rendelkezések célja az, hogy a rosszhiszemű követelések érvényesítéséhez a fél ne kapjon külön segítséget azáltal, hogy a bíróság a költségeknek az állam által való viselését megkönnyíti. A rosszhiszemű, visszaélésszerű pereskedés esetén a felet költségmentességben részesíteni nem lehet akkor sem, ha egyébként annak feltételei fennállnának, illetve a már engedélyezett személyes költségmentességet meg kell vonni.[18]

Nem az elsőfokú eljáráshoz kapcsolódik szervesen, azonban itt kell megemlíteni a jogorvoslathoz való jogot, ami azonban véleményem szerint kapcsolódik a bírói úthoz való alapvető joghoz. A jogorvoslathoz való jog az Alaptörvény XXVIII. cikk (7) bekezdésén alapuló alapvető jog. A jogorvoslat joga mindenkit megillet, az Alaptörvény szerinti alapvető jog gyakorlása kártérítési igényt nem alapozhat meg, így a fél nem alapozhat kárigényt arra a tényre, hogy más a jogorvoslati jogával élt.[19]

A bíróság köteles megakadályozni minden olyan eljárási cselekményt, vagy egyéb magatartást, amely a jóhiszemű joggyakorlás követelményével ellentétes. Amennyiben az adott ügyben rendelkezésre álló adatok alapján megállapítható, hogy a notórius pereskedő felperes rendszeresen visszaél a számára jövedelmi és vagyoni viszonyai alapján engedélyezett személyes költségmentesség kedvezményével, és az

---

[15] EBD2014. P.12. elvi határozat

[16] Andrews, Neil, *Principles of Covil Procedure* (London, Sweet&Maxwell, 1994.) 37.

[17] Alkotmánybíróság 539/AB/1997. számú ügyben hozott határozata

[18] BDT2009. 2014.: A fentiekből következően a felperes által a keresetben érvényesített kár nem az I. rendű alperes mulasztásával vagy magatartásával áll okozati összefüggésben, hanem annak következménye, hogy a bíróság jogerősen elrendelte a felperes felszámolását. A fizetésképtelenség megállapítására, a felszámolás elrendelésére pedig a felperes magatartása adott okot, mivel a jogerős határozat meghozataláig a fizetésképtelenség megállapítása alapjául szolgáló nem vitatott tartozását nem egyenlítette ki.

[19] Pécsi Ítélőtábla Gf. 40.027/2017/5.

ennek keretében részére biztosított pártfogó ügyvéd kirendelésének lehetőségével.[20] A felperes effajta magatartása az eljárás indokolatlan elhúzódásához és fölösleges költségek okozásához vezet. A személyes költségmentesség jogintézményét a jogalkotó az arra rászorulók számára történő jogi segítségnyújtás keretében kívánta megteremteni, nem pedig azért, hogy a peres eljárások számát indokolatlanul megnövelje. A törvényalkotó szabályozta azokat az eseteket, amikor a felet nem lehet költségmentességben részesíteni, noha egyébként annak feltételei fennállnának. Ezzel a rendelkezéssel a rosszhiszemű, vagy teljesen eredménytelen pereskedést kívánja megakadályozni a jogalkotó.[21]

A keresetkiterjesztéssel kapcsolatban a Pp. kötelezően előírja a pénzbírság kiszabását, ha a fél a par befejezését késlelteti.[22] Amennyiben a fél eljárási jogait nem jóhiszeműen gyakorolva azért terjeszt elő keresetkiterjesztést, hogy ezáltal a hatáskörrel és illetékességgel rendelkező, illetve a kijelölt bíróság eljárását ellehetetlenítse, a kizárás tárgyában határozó bíróságnak minden eszközt igénybe kell venni ahhoz, hogy - az eljárás ésszerű határidőn belül történő befejezéséhez való alapjog biztosítása érdekében - a feleket eljárási jogaik jóhiszemű gyakorlására szorítsa.[23]

Az Emberi Jogok Európai Bíróságának ítéletei szerint a bíróságoknak szükséges az eljárásjog adta lehetőségekkel élni és azt a felet, aki maga is nagymértékben

---

[20] Megjegyzés: A felperes a bíróságokkal rendszeres levelezésben áll, egy eljárás tartama alatt többször is előterjeszt alaptalan elfogultsági kifogást, ugyanakkor hangsúlyozva azt, hogy számára szükséges a pártfogó ügyvéd jogi segítsége, a bíróságok által kirendelt pártfogó ügyvédekkel rendre nem veszi fel a kapcsolatot.

[21] BH 1986. 422.: Az ítélőtábla álláspontja szerint a felperes magatartása egyértelműen rosszhiszeműnek, a személyes költségmentesség és annak egyik részjogosítványa - a pártfogó ügyvéd kirendelése iránti igény - visszaélésszerű gyakorlásának minősíthető. Az Alkotmánybíróság 539/AB/1997. számú ügyben hozott határozata is kimondta, hogy a bírói úthoz való alapvető jogból az nem következik, hogy az államnak támogatnia kell még a rosszhiszeműnek látszó pereskedést és ennek kibontakozását is. Az Alkotmány 57. § (1) bekezdése szempontjából elégséges, ha az ilyen perlekedést az általános szabályok szerint, de külön gazdasági-pénzügyi támogatás nélkül engedik kibontakozni. A költségmentességgel kapcsolatos rendelkezések célja az, hogy a rosszhiszemű követelések érvényesítéséhez a fél ne kapjon a bíróságtól külön segítséget azáltal, hogy azzal a bíróság a költségeknek az állam által való viselését megkönnyíti.

[22] Nagy Adrienn - Wopera Zsuzsa, Polgári eljárásjog I. (Szerk) (Budapest, Wolters Kluwer Kft., 2017.) 109.

[23] BDT2007. 1677.

hozzájárul az eljárások elhúzódásához pénzbírsággal sújtani vagy egyéb eljárásjogi következményeket vele szemben alkalmazni. A felperes azon magatartása, hogy a kereset kiterjesztésével elérje, hogy a jogvitát ne a hatáskörrel és illetékességgel rendelkező bíróság, illetve ne a kijelölt bíróság, hanem másik bíróság bírálja el, kimeríti a visszaélésszerű joggyakorlás kritériumait.[24]

A Pp. által előírt tájékoztatási kötelezettség célja annak biztosítása, hogy a fél a bizonyítási indítványait a jóhiszemű és célszerű pervitel követelményeinek megfelelően előterjeszthesse. A tájékoztatásnak az adott tényállításokra vonatkozóan egyediesítettnek és teljes körűnek, valamennyi elbírálásra kerülő kérelemre kiterjedőnek kell lennie. A tájékoztatási kötelezettség nem teljesíthető csupán általános tájékoztatással.[25] A tájékoztatási kötelezettség a bíróság oldalán felmerülő olyan kötelezettség, amely feltétele annak, hogy a későbbiekben rosszhiszeműen eljáró féllel szemben a bíróság meghatározott jogkövetkezményeket tudjon alkalmazni. Ez a fajta tájékoztatási, kitanítási kötelezettség nem korlátlan, hiszen a bíróság nem válhat az egyik fél „tanácsadójává".[26]

5. Perbeli nyilatkozatok relevanciája

A jóhiszemű pervitellel kapcsolatos egyik részterület a felek nyilatkozata, az azokban közölt tények valóságtartalma. Amennyiben a fél valótlan tényt közöl vagy valós általa ismert tényt tagad, akkor ezen esetekben helye lehet vele szemben pénzbírság kiszabásának. Kérdésként merül fel azonban, hogy mely nyilatkozatok minősülnek az üggyel összefüggő nyilatkozatoknak, amelyek valójában a per kimenetelét illetve annak idejét befolyásolják.

A Pp. a per elhúzására irányuló, feleslegesen többletköltségeket okozó magatartások mellett az igazmondási kötelezettség megsértését tekinti a pénzbírság kiszabását megalapozó, rosszhiszemű magatartásnak. A Pp. azonban nem általában a valótlan tényállítások megtételét, vagy valós tények tagadását kívánja pénzbírsággal

[24] BDT2007. 1677.
[25] 1/2009. (VI. 24.) PK vélemény
[26] Rechberger, Walter, *Kommentar zur ZPO. 2. A*ufl. (Wien, 2000.) 1161-1162.

szankcionálni, hanem csak az ügyre vonatkozó valótlan tényállításokat és csak az ügyre tartozó való tények tagadását. A Pp. nem bármilyen, hanem csak a per eldöntése szempontjából jelentőséggel bíró tény elhallgatásának tulajdonít a pénzbírság kiszabása szempontjából jelentőséget.

A félnek a költségmentesség engedélyezése iránti kérelmében a vagyoni, jövedelmi viszonyaira vonatkozó valótlan nyilatkozata nem minősül „az ügyre vonatkozó valótlan tényállításnak", ezért emiatt vele szemben pénzbírság kiszabása nem alkalmazható. A valótlan adatok közlésének büntetőjogi következményei lehetnek. Az egyes peres eljárásokban az a körülmény, hogy a felperes a költségmentesség engedélyezése iránti kérelmében jövedelmi viszonyaira vonatkozóan esetleg valótlan tényállítást tett, nem érintette, nem érinthette az ügy érdemi elbírálását, annak az adott ügyben a költségmentesség megvonása szempontjából van jelentősége.[27]

A Pp. által meghatározott nyolc-, illetőleg háromnapos tárgyalási időköz hiánya esetén a tárgyalás megtartásának nincs akadálya, ha az alperes megjelent, és a tárgyalás elhalasztását nem kéri. Ha azonban az alperes a tárgyalás elhalasztását kéri, a tárgyalási időköz hiánya alap lehet a halasztásra, de ebben a vonatkozásban is irányadó, hogy a felek perbeli jogaikat jóhiszeműen kötelesek gyakorolni. Ha a halasztást kérő fél nem jelent meg, a tárgyalási időköz hiánya esetén a tárgyalást megtartani nem lehet.[28]

6. Bíróság tájékoztatása és az általa meghatározott kötelezettség teljesítése

A Pp. jóhiszemű joggyakorlás követelményét fogalmazza meg és az ezzel ellentétes perbeli magatartásokat szankcionálja. A Pp. szerint az a fél vagy képviselő, valamint más perbeli személy sújtható pénzbírsággal, aki valamely nyilatkozatot indokolatlanul késedelmesen tesz meg, vagy azt felhívás ellenére sem teszi meg, és ezáltal a per befejezését késlelteti. A pénzbírság alkalmazásának tehát két együttes feltétele van, a szankciót csak mindkét feltétel megléte esetén lehet alkalmazni.[29]

[27] BH2011. 46.
[28] PK 169. szám
[29] Pécsi Ítélőtábla Cgf. V. 30.086/2006/2.

Ha a bíróság a felet határidő tűzésével okirat becsatolására hívja fel, a felhívást csak akkor lehet teljesítettnek tekinteni, ha a fél azokat a mellékleteket is becsatolja, amelyekre magában az okiratban utalás történt és amelyek nélkül az okirat tartalmát nem lehet értelmezni. A bíróság köteles biztosítani, hogy a felek és a per többi résztvevője jogaikat rendeltetésszerűen gyakorolják, és perbeli kötelezettségeiknek eleget tegyenek. A bíróság köteles megakadályozni minden olyan eljárási cselekményt, vagy egyéb magatartást, amely a jóhiszemű joggyakorlás követelményével ellentétes, így azt, amely a per elhúzására irányul, vagy arra vezethet. A bíróság pénzbírsággal sújtja azt a felet, valamint más perbeli személyt, aki valamely nyilatkozatot indokolatlanul késedelmesen tesz meg, vagy azt felhívás ellenére sem teszi meg, és ezáltal a per befejezését késlelteti.[30]

Az eljárási törvény az indokolatlan késedelmet rendeli szankcionálni. A késedelem akkor indokolatlan, ha a fél előzetesen nem jelzi a bíróság felé a határidő betartását akadályozó körülményeket. Ha az indokolatlan késedelem miatt a tárgyalási határnapot el kell halasztani, megvalósul a szankció kiszabásának másik feltétele, a per befejezésének késedelme. A szankció alkalmazásának ezen feltételek megléte esetén is csak akkor van helye, ha a bíróság előzetesen figyelmeztette a felet a rosszhiszemű pervitel következményeire. A per befejezésének késleltetése megvalósul ha a tárgyalási határnapot a bíróságnak hivatalból el kell halasztania.[31]

A bíróság tájékoztatási kötelezettsége a Pp. alapján a pártfogó ügyvédi képviselet lehetőségére is kiterjed. A tájékoztatást az adott eset és a peres fél konkrét körülményeihez képest, részletesen és teljes körűen, a peres eljárásban akár többször is meg kell adni. Súlyos eljárási szabálysértés, ha a tájékoztatás, és ennek következtében a jogi képviselet mellőzése miatt a peres fél igényérvényesítése csorbát szenved[32]

A fél tájékoztatásával kapcsolatos fontos követelmény, hogy annak egyediesítettnek kell lenni, az adott helyzethez kell igazodnia. Amennyiben a tájékoztatásokat a fél „láthatólag” nem értette meg, úgy a bíróságnak közre kell hatnia és a tájékoztatást

[30] BDT2005. 1252.
[31] BDT2006. 1392.
[32] BH2014. 184.

olyan formában kell megtenni, amelyet a fél megért. A bíróság tájékoztatási kötelezettsége az adott helyzethez képest szükséges tájékoztatásra vonatkozik. Ez a fajta tájékoztatás lehet akár szóbeli, akár írásbeli tájékoztatás.[33]

A bíróság a Pp. által előírt tájékoztatási kötelezettséget az igény felmerülésekor - az eljárás folyamán akár több alkalommal is - teljesíteni köteles. Az első tárgyalásra szóló idézés toldatában, általánosságban megfogalmazott tájékoztatás az adott esetben, amikor több alkalommal is felvetődik, hogy a fél nincsen tisztában az őt illető jogokkal és érvényesítésük módjával, nem elegendő. Így a perben eljáró bíróság nem tesz eleget a Pp.-ben megfogalmazott tájékoztatási kötelezettségének, ha a fél számára általánosságban ad tájékoztatást.[34]

A bíróság által meghatározott kötelezettségekkel kapcsolatosan érdekes kérdés az, ha a bíróság fejt ki olyan tevékenységet, amely miatt az eljárás elhúzódik. ebben az esetben függetlenül a bíróság által meghatározott kötelezettségtől lehet-e a felet „büntetni" a perköltség viselésével avagy sem. Véleményem szerint erre nincs lehetőség, hiszen a perköltség leszállítását nem alapozza meg az, hogy az elsőfokú bíróság a részítéletet elhúzódó meghozatalával indokolatlan többletköltséget okozott. Ezt a fél hátrányára nem lehet figyelembe venni. A perköltség a Pp. szerint a felek célszerű és jóhiszemű pervitelével kapcsolatban felmerült költség. Amennyiben a fél a bíróság felhívásainak eleget tett, a tárgyalásokon idézés alapján részt vett, percselekményei elősegítik a per céljának megvalósítását, felmerült költségeinek megtérítésére - pernyertessége esetén - igényt tarthat, függetlenül attól, hogy a bíróság részéről a felhívás, idézés, egyéb eljárási cselekmény szükséges és indokolt volt-e. Ha a bíróság feleknek a jogviták elbírálásához, a perek tisztességes lefolytatásához és ésszerű időn belül történő befejezéshez való jogát megsérti, ennek jogkövetkezménye a Pp. szerinti külön perben érvényesíthető, mivel az ebből eredő költségek nem tartoznak a Pp. szerinti költségek körébe.[35]

[33] BH2014. 184.
[34] BH2014. 184.
[35] Pécsi Ítélőtábla Gf. 40.015/2014/5.

7. A jóhiszemű pervitel alapelvének érvényesülése nemperes eljárásokban

A jóhiszemű pervitel vagy jóhiszemű joggyakorlás követelménye nem kizárólagosan a polgári perekben érvényesülő alapelv, hanem minden egyes nemperes eljárásban[36] is figyelemmel kell rá lenni, amelynek háttérjogszabálya a Pp. A jóhiszemű pervitel követelményével kapcsolatban azonban nem kizárólag a Pp. szabályaira kell figyelemmel lenni, hanem az adott eljárás szabályaiból eredő eltérésekre is és így ezeknek megfelelően, méltányosan kell alkalmaznia az eljáró bíróságoknak az egyes rendelkezésükre álló jogkövetkezményeket.

A cégeljárásban benyújtott változásbejegyzési eljárásban a Pp. alapján nem lehet pénzbírságot kiszabni, mert annak egyik feltétele - az eljárás befejezésének késleltetése - a szigorú törvényi határidőkre tekintettel nem következhet be.[37] A cégeljárások során a törvény által meghatározott határidő be nem tartása a kérelem elutasítását vonja maga után, az eljárásban érdekelt félnek nincsenek olyan lehetőségei, mint egy peres eljárásban, így nincs meg az a lehetősége sem, hogy az eljárást elhúzza.

A cég képviselőjét terheli felelősség a cégbejegyzési kérelem határidőben történő benyújtásáért. Ezért a késedelmes benyújtás miatt nem a jogi képviselővel, hanem a cég képviselőjével szemben van helye pénzbírság kiszabásának. A jogi képviselővel szemben a cégbejegyzési eljárásban általában csak a Pp. szabályainak alkalmazásával van helye pénzbírság kiszabásának, és csak a cégbejegyzési eljárás folyamatban léte alatt elkövetett mulasztásai, késedelmei miatt.[38]A változásbejegyzési kérelem késedelmes benyújtása miatt tehát csak a cégvezető tisztségviselőjével szemben, a cégbejegyzési eljárásra vonatkozó jogszabály alapján van helye pénzbírság kiszabásának.

Ugyanúgy, mint a cégeljárások során a végelszámolási eljárásban is felmerül a vezető tisztségviselő felelőssége. A végelszámolási eljárásban a végelszámolót a mulasztása

[36] Például: Fizetési meghagyásos eljárás, hagyatéki eljárás, felszámolási eljárás, csődeljárás, cégeljárás
[37] BDT2006. 1405.
[38] Legfelsőbb Bíróság Cgf. II. 31.002/1998/2. számú határozata

miatt - a törvény különös rendelkezése hiányában - a Pp. szerint lehet bírsággal sújtani, ám csak a mulasztás jogkövetkezményeire történt előzetes figyelmeztetés eredménytelensége esetén. Fontos azt megjegyezni, hogy a bírság a végelszámoló szervezettel, és nem a nevében eljáró természetes személlyel szemben szabható ki.[39] Amennyiben a bíróság nem figyelmezteti a végelszámolót a jóhiszemű joggyakorlás követelményére, valamint annak megszegésének következményeire, úgy vele szemben pénzbírság kiszabásának nincsen helye.

Ahogy a fentebb már megfogalmaztam a szankcionálás akkor lehetséges, ha a fél magatartása az eljárás elhúzódásához vezet és az indokolatlan volt. Amennyiben a hitelezői igények teljesebb körű kielégítésére lehetőség látszik, a felszámolási eljárás befejezésére előírt kétéves határidő meghosszabbodhat. A felszámolónak azonban ilyen esetben is kötelessége, hogy felhívásra közölje a bírósággal, ha a végzésben előírtak teljesítésének bármilyen akadálya van. Ennek elmulasztása esetén helye van pénzbírság kiszabásának.[40] A Csődtv. szerint a felszámolási eljárás befejezésére meghatározott kétéves időtartam betartatása is a bíróság feladata, bár a kialakult bírósági gyakorlat nem követeli meg ennek a törvényi előírásnak a merev kikényszerítését.[41]

A Csődtv. utaló szabálya szerint a felek jóhiszeműen kötelesek gyakorolni eljárási jogaikat, elősegítve azt, hogy az eljárás ésszerű időn belül befejeződjön. A hitelezők méltányolható érdekei indokolttá tehetik azt, hogy a Csődtv.-ben meghatározott határidő leteltét követően mégse nyújtson be záróanyagot a felszámoló az elsőfokú bírósághoz. Ebben az esetben azonban a Csődtv. szerint újabb közbenső mérleget kell a felszámolónak előterjesztenie. Ha a felszámoló ezen bejelentési kötelezettségének nem tesz eleget és késlekedésének indokait a pénzbírság kiszabását megelőzően nem közli az elsőfokú bírósággal, akkor a bíróság jogszerűen sújthatja a felszámolót pénzbírsággal.[42]

[39] BDT2013. 3018.
[40] BDT2015. 3259.
[41] Szegedi Ítélőtáblának a Gf. I. 30 012/2011/3. határozata
[42] BDT2015. 3259.

A Ptk. 1:3-5. §-ainak megsértése - a jóhiszeműség és tisztesség követelményének, az elvárható magatartásnak, a joggal való visszaélés tilalmának a sérelme - nem állapítható meg, amennyiben a fél polgári igényt kíván érvényesíteni egy másik féllel szemben. „Helyesen fejtették ki az eljárt bíróságok, hogy sem a felszámolás iránti kérelem előterjesztése, sem a kérelemtől elálló nyilatkozat megtételének elmaradása, sem pedig az egyezség elleni fellebbezés nem ad alapot erre. A másodfokú bíróság helyes indokolása szerint a Cstv. 26. § (3a) bekezdése a felszámolási kérelemtől való elállással kapcsolatban csak azt fogalmazza meg, hogy a felszámolás kezdő időpontjáig nem szükséges hozzá az ellenérdekű fél hozzájárulása, de nem tartalmaz kötelezettséget az elállásra vonatkozóan. Amint a másodfokú bíróság ugyancsak helyesen rámutatott, ez azért sem volt elvárható az I. rendű alperestől, mert a felperessel szemben nem csak nem vitatott, hanem vitatott követelése is volt, a felperes pedig csak a nem vitatott követelésnek megfelelő összeget utalta át a fizetésképtelenség megállapítását követően, a vitatott követelésrészt nem, és a vitatott követelés tekintetében a felszámolási ügyben eljárt bíróság a hitelezői igényt a Cstv. 57. § megfelelő pontjainak megfelelő hitelezői csoportba besorolta a felszámolás elrendelésekor. Semmilyen jogszabályból - ideértve a Ptk. 6:519. §-át is - nem vonható le olyan következtetés, hogy a hitelező a nem teljesített követelése által megalapozott igényét ne érvényesíthetné megfelelő jogi eljárás keretében és az ezzel ellentétes magatartása felróható lenne. Az I. rendű alperes igényérvényesítésre irányuló, felperes által sérelmezett valamennyi jogcselekménye megfelel az elvárható magatartásnak, nem sérti sem a jóhiszeműséget, sem a tisztességet és nem minősül joggal való visszaélésnek. Az I. rendű alperes jogszerű magatartást tanúsított, az nem róható fel, ezért a Ptk. 6:519. §-ában foglalt törvényi feltételek együttes fennállásának hiányában a felperes kártérítési követelése alaptalan.”[43]

[43] Kúria Pfv. 20.634/2018/10.

8. A jóhiszemű pervitel követelménye a bizonyítással kapcsolatban

A Pp. által az I. Fejezetben szabályozott alapelvek a polgári peres eljárások valamennyi szakára illetve valamennyi különleges pertípusra irányadóak. Ez alapján a bizonyítási eljárással kapcsolatban is fontos szerephez jut a jóhiszemű pervitel, hiszen az új szabályozás által a jogi képviselők számára a pertaktikai megoldások száma csökken. A régi Pp. sem támogatta az indokolatlan késlekedést a bizonyítási eljárásokkal kapcsolatban, azonban véleményem szerint a Pp. alapján még szigorúbban kell a felek bizonyítási indítványaikat és cselekményeiket felügyelni.

A másodfokú eljárás során felmerülhet a kérdés, hogy a bíróság a tárgyalás megtartásával összefüggésben megsértheti-e a fél tisztességes eljárás lefolytatásához való jogát illetőleg arra, azzal hogy a személyes nyilatkozat megtételének lehetetlenné teszi. A Pp. értelmében ugyanis a fellebbezési tárgyalásra szabályszerűen megidézettnek, vagy valamelyiküknek az elmaradása a tárgyalás megtartását és a fellebbezés elintézését nem gátolja. A Pp. szerint a fellebbezésben szükséges teljes körűen megjelölni, hogy a fél a határozat megváltoztatását mennyiben és milyen okból kívánja, továbbá a fellebbezésben új tény állítására, illetve új bizonyíték előadására főszabály szerint nem kerülhet sor. Ezen szabályok együttes értelmezéséből következik, hogy a fél tárgyalásról való távolmaradása melletti ítélethozatal a fél perbeli jogait és a tárgyalás tisztességes lefolytatásához fűződő jogát nem sérti.[44]

Abban az esetben, ha a fél a jóhiszemű pervitellel össze nem egyeztethető módon terjesztette elő bizonyítási indítványát, akkor-e tekintetében egyértelmű eljárásjogi parancsként írja elő a Pp. a bizonyíték illetve bizonyítási indítvány mellőzését. Erre figyelemmel a rosszhiszemű pervitel, mint feltétel bekövetkezése után a bíróságnak nincs mérlegelési joga a felajánlott bizonyítást illetően, azt mellőznie kell. Ezért nincs ilyen esetekben jelentősége annak sem, hogy ezt követően a per tárgyalása folytatódott-e.

[44] Kúria Pfv. 21.008/2015/6.

A másodfokú eljárásban alkalmazott szabályokkal együtt alkalmazandó jóhiszemű pervitel elve, amely a bíróság és rajta keresztül nevesítetten „a felek és a per többi résztvevője" - ezáltal a fél jogi képviselője - számára is egyértelmű eljárásjogi kötelezettségként írja elő a rendeltetésszerű joggyakorlást és a perbeli kötelezettségek teljesítését. Ehhez kapcsolódó preklúziót tartalmaz a Pp., amely szerint a fél köteles a tényállításait, nyilatkozatait, bizonyítékait - a per állása szerint - a gondos és az eljárást elősegítő pervitelnek megfelelő időben előadni és előterjeszteni.

Abban az esetben, ha a fél rendelkezésére álló magánszakértői véleményt nem csatolja hosszú időn keresztül, holott erre lehetősége lenne és erre nem is hivatkozott már a jóhiszemű pervitel elvének határát igencsak súroló magatartás. Amennyiben a magánszakértői véleményt csupán a kirendelt szakértőnek a tárgyalásról történt távozását követően terjeszti elő, semmiképpen nem egyeztethető össze a „per állása szerint", és a „megfelelő időben" történő előterjesztés kötelezettségével. A fél által hivatkozott „pertaktikai ok" mint indok nem fogadható el egy ilyen perelhúzást célzó cselekménysorozat esetében. Következetes a bírói gyakorlat[45] abban, hogy jogszabálysértés nélkül mellőzi a bíróság a bizonyítási indítvány folytán a további bizonyítás elrendelését, ha a fél azt a jóhiszemű pervitellel össze nem egyeztethető módon terjesztette elő.[46]

A régi Pp. alapelve az, hogy a bíróságnak egyértelműen, világosan - félreérthetőséget elkerülve - kell megfogalmaznia a határozatait. Ez az alapelv véleményem szerint jelenleg is irányadó. A bíróság eljárása nem jogszabálysértő, hiszen az anyagi jogi jogosultság hiánya nem érinti az eljárási jogok gyakorlását. Amennyiben a fél nyilatkozatot tesz a bíróság felhívására és azzal szemben nyilatkozata megtétele előtt pontosítást nem kér, úgy véleményem szerint az eljáró bíróság tájékoztatási kötelezettségének maradéktalanul eleget.[47]

---

[45] Kúria Pfv. 21.982/2016/5.

[46] BH2013.18.

[47] Kúria Pfv. 22.407/2017/9.: „Alperes álláspontja szerint az elsőfokú bíróság végzései nem voltak világosak, mivel az 52. sorszámú végzés a következő felhívást tartalmazta: „... a 2016. december 13. napján kézbesített alperesi előkészítő iratra és annak mellékleteire 5 napon belül nyilatkozzon...". A bíróság 2016. december 13-án az alperes szakértői véleménnyel kapcsolatos észrevételeit kézbesítette, így a beadványában erre reagált. A jogutódlással kapcsolatos konkrét nyilatkozattételre felhívást nem kapott. A mellékletekkel kapcsolatos

Abban az esetben, ha a fél a bíróság tájékoztatása ellenére bizonyítási indítványt nem terjeszt elő és kizárólag a korábban csatoltcsatolt iratok tartalmával kívánja igazolni keresete jogalapját, összegszerűségét, akkor utóbb nem hivatkozhat arra, hogy bizonyítási indítványainak megtételére nem volt lehetősége, hiszen a bíróság korábban erre felhívta, azonban saját döntése által nem élt azzal a lehetőséggel, hogy bizonyítási indítványt tegyen.[48]

A fél rosszhiszemű pervitelének, a való tényekkel ellentétes előadásának a nem vagyoni kártérítés összegére nincsen kihatása, annak szankcionálására a Pp. 8. §-ában meghatározott módon van lehetőség, amennyiben a jóhiszemű pervitel követelményére és a rosszhiszemű pervitel következményeire a bíróság a felet előzetesen tájékoztatta.[49] Ez alapján megállapítható, hogy a rosszhiszemű bizonyítási cselekmény nem hat ki a per egészére úgy, hogy az alapján a kár vagy annak nagysága megállapítható vagy módosítható lenne. Ezen magatartásnak kizárólag eljárásjogi következményei lehetnek.

észrevételezésre felhívás félreérthető volt. Válasziratában az alperes szakértői véleményre tett észrevételeire adott korábbi nyilatkozatait tartotta fenn, tehát láthatóan nem akként értelmezte a mellékleteket, ahogyan az elsőfokú bíróság szerette volna értelmezni. Félrevezető volt a bíróság azon eljárása, hogy jóllehet 2016. október 19-e óta rendelkezésére állt a per iratai között az engedményezési szerződés, mégis nyilatkozatra hívta fel a szakértőt és a feleket. Annak ellenére, hogy az engedményezési szerződés ismeretében kérdéses volt a személye, illetve eljárási jogosultsága, őt is megidézte a tárgyalásra."

[48] Pécsi Ítélőtábla Gf. 40.027/2017/5.

[49] Pécsi Ítélőtábla Pf. 20.043/2015/4.: „Téves az alperesnek az a fellebbezési hivatkozása, hogy a felperest ért hátrányok jellegének, mértékének megítélésénél az elsőfokú bíróság figyelmen kívül hagyta a tanúvallomásokat. A felperes nem vitásan azt állította, hogy a káresemény hatásai, elsősorban az önértékelési és párkapcsolati problémák a peres eljárás időszakában is fennálltak. A perben kihallgatott tanúvallomások alapján azonban az elsőfokú bíróság a felperes előadásával szemben tényként fogadta el, hogy a felperes párkapcsolati problémái rendeződtek, átmeneti megszakadást követően barátnőjével a kapcsolat helyreállt, pszichés problémái és önértékelési panaszai pedig ugyan átmenetiek voltak, a határozat meghozatalának időpontjában azok már nem álltak fenn. A sérülések és hátrányok tartóssága (évekig, esetlegesen évtizedekig való fennállása) pedig az elsőfokú döntésben is kifejezésre jutó bírói gyakorlat szerint a nem vagyoni kártérítésnek nem feltétele."

Melania Nagy* - Weapons instead of balls - Children in uniform

1. Salma and Zahra Halane: The Twins of Terror, (Case Study)

Salma and Zahra from Chorlton, Greater Manchester, entered Syria on 16 July 2014 at the age of 16. On June 26, 2014, they reported their disappearance from their family home. Like many other women migrating to ISIS, the twins were introduced to the ISIS ideology "offline" in advance. Ahmed Ibrahim Mohammed Halane, the brother of the two twin 21-year-old boys, left the UK in 2013 to join ISIS. Ahmed may have been the primary influencing factor for the twins in learning about ISIS's violent extremist ideology, and his departure and joining may have been exemplary for the twins. The family was called "very religious" by close acquaintances. Zahra and Salma's friends report the twins as being easily integrated into the school community, having many friends and being extremely intelligent. The girls were preparing for a medical career.

The girls had very active Twitter and Instagram users. Several posts have been posted, including, "Happy 9/11. The happiest day of my life, we hope there will be many more. "

The girls often referred to "Ummah" i.e. belonging to the global Muslim community as a pull factor. Within a few weeks of their arrival, the girls were married to a jihadist, and thus began to proclaim the story of their love during the recruitment process.

Zahra hinted that she was happy to be the wife of a "green bird". This is a general aspiration that Western women seek to achieve. This is expressed in "paradise" by

* Nagy Melánia, PTE-ÁJK, Büntetőjogi Tanszék, egyetemi tanársegéd,
A tanulmány „Az Innovációs és Technológiai Minisztérium ÚNKP-20-4-I-PTE-580 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült."

their firm belief in the possibility of reunification. This is reinforced by the twins by publicly praising the stories of their husbands 'deaths.

It is reasonable to assume that the twins underwent a fairly similar process of radicalization during their last months in the UK. However, differences can be discovered through their online activities. Zahra's online identity shows a higher level of political commitment in recruitment strategy, while Salma is much more introspective. Salma answers questions from anonymous senders, including how a widow lives in the territory of the Islamic State. Their entries have undergone significant transformation since 2015, much more extreme than at the start of accession. It can be shown that their activities had an influential effect on women joining the territory of Great Britain.

The motivations that lead women to ISIS are portrayed in another dimension by Katharina Kneip. It is hypothesized that the emancipation of Western women can be interpreted as freeing them from self-restraint or control. In her research, she focused on online activities and set up a motivational network based on blogs. The reason for the Internet approach was to gain insight into the ideas of individual women and to learn about ISIS's propaganda activities.

His findings are as follows:

a) Lifting from parental restraints, In research on identity, community and sense of belonging, where fraternities play an important role

b) Tradition of being deprived of choice, Making independent decisions about their lives and future

c) They are seen as victims of Islam in Western countries from Western restrictions

Gain power and control over their husbands / families

There is a need to increase respect for the community as a female jihadist[1]

Participants included 15- and 16-year-old girls, respectively. Online magazines produced by the Islamic State, including Dabiq and Rumiyah, may respond to the

[1] Kneip, Katharina, *Female Jihad - Women in the ISIS*. https://www.researchgate.net/publication/306296253 (date of download 23.02.2021.)

increase in numbers. [2]In these magazines, PR strategies recognized by ISIS have appeared about women joining. A separate propaganda network was set up, which focused only on recruiting and encouraging women. One such example is the tactically important message for women when ISIS announced in 2015 its willingness to release a captured Japanese journalist if a female terrorist imprisoned in Jordan is released. Also one kind of motivational, recruiting magazine is "Samikha," which is nothing more than "an Islamic jihadist magazine written for women".[3] We distinguish two groups among emigrants. One group includes those who start with their husbands and families, while the other group consists of single women. Of the individuals traveling alone, three primary causes were identified: grievances, fulfillment of desire for solutions, and personal motivations. There have been a number of cases of Western fighters bringing entire families into the ISIS-controlled area, including young children and wives. Some governments, such as the Finnish government, have publicly stated that they are aware of a number of children and women who have escorted male fighters to ISIS-dominated territory. However, the number of these cases is less than that of single women. The first phase of the journey for Western women is the processing of separation from the family. However, it can be shown that families, if they are aware of migration, can have a very large deterrent. Lack of family is difficult for them to deal with, so it can help change your mind.[4]

2. Children as a suicide bombers, the process of bombing

Training is a very complex process for suicide bombers. Training camps are usually set up in abandoned schools or houses offered by locals. In some camps, such as the Nawazkot facility, paintings depicting Paradise adorn the walls, such as images of

[2] Ingram, Kiriloi, *IS's appeal to Western Women: Policy Implications*. (ICCT Policy Brief, 2017) 3.
[3]https://www.migraciokutato.hu/hu/2015/12/07/szuletett-dzsihadista-felesegek-nok-a-dzsihadista mozgalmakban/ (date of download 25.02.2021.)
[4] Hoyle, Carolyn - Bradford, Alexandra - Grenett, Ross, *Becoming Mulan? Female Western Migrants to ISIS Institute for Strategic Dialogue.* 10. https://www.isdglobal.org/wpcontent/uploads/2016/02/ISDJ2969_Becoming_Mulan_01.15_WEB.pdf (date of download 25.02.2021.)

river milk rivers with fairies walking in lush green valleys. Training camps are usually located in areas where the government has little oversight or control, which reduces the need for camp safety. At night, however, an older trainee guards the camp. There is no way out of the camp for participants and no one can leave the training, even after the night prayers. The sites themselves are changed from time to time for security reasons. In the camp, adults and minors are usually separated from each other and receive special training. Suicide bombers range in age from seven to forty. Suicide training camps are divided into two categories: there is a junior camp and a senior camp for the older age group. In terms of age distribution, 16 is the dividing line. Trainees aged 16 or over already belong to the senior camp, while youth camps have trainees from the age of seven to the age of 15 and a half. Usually, family members do not approve of their relatives 'participation in the preparation and in such cases travel to the camp to retrieve them. Such efforts are not hampered by camp operators if children want to leave of their own free will. The experience, however, is that trainees who are pulled out of the camp by their families often leave their homes to return to camp. One prospective suicide bomber admitted, "Yes, I had a great time in camp life, I felt happy with my peers there. We had good food, pocket money, good friends and even our cars. " In the winter months, it becomes difficult to carry out the training due to the harsh weather, at which point the members melt into the general civilian population. The average number of trainees in the camp ranges from 30 to 35, but this can vary.

Camp members wake up before sunrise to take part in special night vigils, followed by morning prayer. After breakfast, most students receive driver education and practice vehicle maneuvers. Experienced driving instructors will teach them how to handle motorcycles and cars in preparation for suicide attacks carried out with or carried by vehicles (VBIED).[5]

During the morning session, some trainees will be at the camp, where they will be involved in cleaning the camp or just preparing lunch. Lunch is usually served around noon, followed by lunch prayers. The trainees are then divided into two groups and

[5] Tajik, S., *Insight into a Suicide Bomber Training Camp in Waziristan*. (CTC Sentinel, 2010/3.) 10.

study the Qur'an. A new recruiter is usually paired with an older member to help him teach prayers. The trainees then start again for outdoor driving lessons after drinking tea with cookies. In the summer months, they usually take a few hours of quiet rest after lunch before gathering for afternoon prayers. They attend the evening prayers together. This is followed by dinner where trainees have informal conversations with each other or show each other jihadist videos on a DVD player. Afterwards, after the night prayers are over, they go to sleep immediately and no activity is allowed after the last prayers. Instructors give emotional speeches throughout the training period aimed at influencing the trainees. Both local and guest speakers give lectures at religious education. Before the attack is carried out, only the top leaders know the target. The other members of the training camp will not be informed about the assassination in advance. Some record "video wills" before they leave, which are issued to families after the mission is completed. Usually, suicide bombers visit their relatives for a final meeting before embarking on their mission. When a suicide bomber begins his mission, his camp mates say goodbye to him and then ask him to recommend them to paradise. The bomber is instructed to take a bath, put on clean new clothes, and shave his pubic hair. The bomber recites verses from the Qur'an and continues reciting until the actual explosion. The rahbar (commander of the assassin) instructs the bomber in advance to schedule the explosion properly, and the bomber begins preparations ahead of time. The rahbar's duty is, among other things, to take the bomber to a predetermined target either a few days before the attack or on the actual day. It also helps the assassin get to know the environment where he will carry out the plot. Rahbar also plays a mediating role by liaising directly with headquarters to inform them of the success or failure of the attack. On the day of the attack, the rahbar decides the most appropriate time for action. The rahbar has a crucial role to play in the operation, which is why it is very important for the candidate to stand in the direction of the rahbar with obedience and loyalty already in the camp. A suicide bomber has the option to change his leader, but there must be a compelling reason for it. This includes, but is not limited to, a case where the rahbar asks the bailiff to attack an impossible target or one that results in too few casualties. A normal target must result in the death of at least 10 people, except for VIP targets where the number of

deaths is negligible. Rahbar does not strictly follow the suicide bomber in the days before the attack. The bomber is free to spend his time in the target city until he starts the attack. The bomber is coded for the time of the final attack. The code word may vary, but typically the word “marriage” was used to indicate that the attacker could blow himself up. When Benazir Bhutto was assassinated, the code word was “ready food”. In the attack, the perpetrators wear the explosive vest under casual clothing so it is properly hidden. Typically, an orange cord connects the explosives to the explosive vest or jacket, and the detonator device at the cord outlet is secured to the left wrist of the bomber with adhesive tape. When the target is reached, the structure is activated with the right hand and an explosion occurs. [6]

3. Summary

The case study and the implementation of the suicide bombings highlighted how easily children are influenced by the extremist ideologies in their environment and by the internet. The biggest problem with the phenomenon of child soldiers is that in societies where a large number of minors go to war, there is a strong fear that in the future, based on patterns learned in childhood, it will necessarily reproduce the factors that it has the victim. Put simply, "where the little ones are harassed, exploited and killed, the children will do nothing but harass, exploit, kill others."

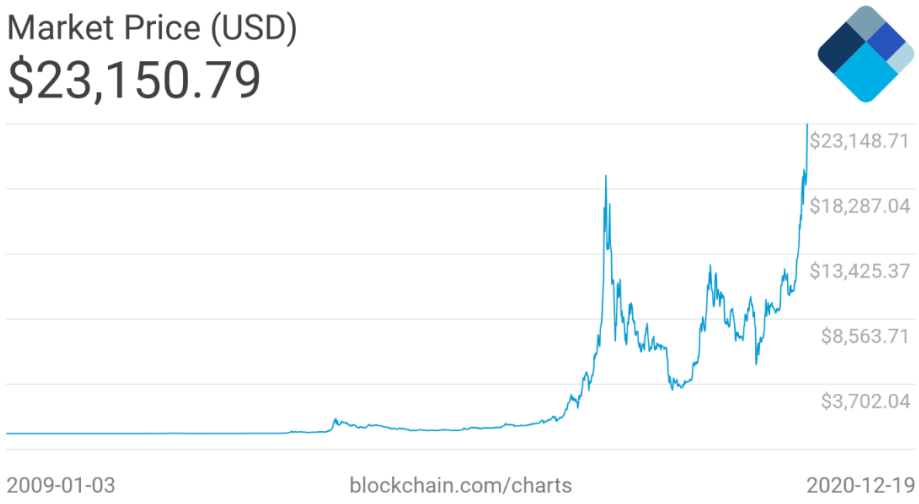
[6] Tajik, S., *Insight into a Suicide Bomber Training Camp in Waziristan*. (CTC Sentinel, 2010/3.)10.

Zsolt Gáspár* - La utilización de las criptomonedas en los cibercrímenes

1. Introducción

En los últimos 40 años el mundo esta enteramente cambiado. Con la evolución extremamente rápida de la tecnología, se han aparecido nuevos tipos de crímenes y los que ya existieron, han sido cambiados, alcanzando hasta la dirección de la red mundial y hasta las computadoras. La aparición de las criptomonedas y la red oscura fueron catalizadores para este fenómeno. Las criptomonedas (especialmente la Bitcoin) tuvieron un crecimiento enorme entre 2009 y 2020 (1. tabla), que resulto en la aparición de nuevas monedas y tokens, y, por supuesto, la popularidad de estos sistemas. Los delincuentes también detectaron las características beneficiarias de las criptomonedas y las utilizan frecuentemente para facilitar sus actividades. Según la evaluación de 2020 de los riesgos del crimen organizado en la Internet de Europol (Internet Organized Crime Threat Assessment o en corto IOCTA) en 2019 han sido 10 casos confirmados en que transacciones de criptomonedas fueron hackeadas, causando un daño de 240 millones de euro.[1]

* Estudiante de PhD, Facultad de Derecho de la Universidad de Pécs
[1] Europol Internet Organized Crime Threat Assessment (IOCTA) 2020, p. 17.



1. tabla: El crecimiento de Bitcoin en USD. Recurso: www.blockchain.com/charts, acceso: 20.12.2020.

La pandemia COVID-19 también ha influido en la situación de los ciberdelitos, porque ha forzado millones personas a sus casas, que resultó en aún más frecuente utilización de la Internet.[2] La mayoría de estas personas hoy en día tienen que trabajar en el modo "home-office", las empresas, las escuelas y las instituciones se expanden sus infraestructuras en la red y cambian a trabajar online, tanto como sea posible. El cambio fue extremadamente rápido con la aparición de la pandemia, por eso muchas empresas no tuvieron bastante tiempo para desarrollar su sistema electrónico, que resulto en graves vulnerabilidades. En estos tiempos, los perpetuadores también están en casa todo el día, teniendo más tiempo para cometer crímenes y lanzar ataques.

[2] Los que todavía pueden trabajar desde sus casas están en mejor situación, pero miles de personas han perdido sus trabajos debido a la pandemia. Según István László Gál, esta situación tiene un efecto criminógeno y, probablemente un gran crecimiento de crímenes es esperado durante y después de la pandemia COVID-19. Para más información sobre el tema véase: István László Gál, "Egy elfeledett bűncselekmény társadalomra veszélyességének feléledése 2020-ban." in *Sic itur ad astra: Ünnepi kötet a 70 éves Blaskó Béla tiszteletére.* eds. Sándor Madai; Anikó Pallagi y Péter Polt (Budapest: Ludovika Egyetemi Kiadó, 2020), 191-199.

Entre junio de 2019 y junio de 2020 un crecimiento de 108% para ataques de ransomware y un 833% para ataques a redes de IoT fueron mensurables.[3]
Nosotros tenemos que acostumbrarnos con la situación actual y desarrollar nuestros conocimientos informáticos sobre los ciberdelitos. En la primera parte del estudio demuestro las características de las criptomonedas. En la segunda parte del estudio presento la conexión entre las criptomonedas y los diferentes ciberdelitos. La última parte del presente estudio será una suma de conclusiones sobre los anteriores.

2. Las criptomonedas

2.1. Sobre las criptomonedas en general

La realización de las criptomonedas empezó con un estudio publicado en la lista de e-mail sobre criptografía, por "Satoshi Nakamoto" en 2008. Su estudio fue sobre un nuevo sistema de financiación "peer-to-peer", llamado Bitcoin. En el próximo año, la primera versión del programa cliente del Bitcoin fue emitido[4] y la primera criptomoneda fue creada. Pero ¿qué son las criptomonedas? Las criptomonedas son valores digitales descentralizados que no son monedas de curso legal, pero son herramientas de intercambio generalmente aceptadas y utilizadas, emitidas por un desarrollador o un grupo de desarrolladores (en lugar de un banco central) y que utilizan la criptografía[5] para emitir y mantener nuevas unidades y para registrar las transacciones.[6] Las criptomonedas utilizan una tecnología bastantemente complicada: la cadena de bloques. La "blockchain" (la cadena de bloques) es un distribuido libro

[3] Rodrigo Mariano Díaz, "La ciberseguridad en tiempo del COVID-19 y el tránsito hacia una ciberinmunidad." *Boletín FAL* 382. no. 6 (2020): 11.
[4] "Satoshi Nakamoto" acceso: 23.11.2020., https://www.bitcoinbazis.hu/utmutato/kicsoda-satoshi-nakamoto/
[5] En el mismo año de la creación de Bitcoin, ya fueron investigadores quienes consideraban la criptografía como una amenaza peligrosa en los manos de los criminales. Véase: Flórián Tremmel; Csaba Fenyvesi y Csongor Herke, *Kriminalisztika* (Budapest – Pécs, Dialóg Campus Kiadó, 2009): 278.
[6] Judit Glavanits y Péter Bálint Király, "A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége." *Jog Állam Politika: Jog- és Politikatudományi Folyóirat* no. 3. (2018): 179.

de registro, esencialmente una base de datos descentralizada, que incluye todas las transacciones y es registrado en miles de ordenadores. Los datos son compartidos en bloques, que tienen una identificación única.[7] Los bloques incluirán sumas de comprobaciones (hashes) que muestran las modificaciones en el bloque. Así se puede verificar cualquier bloque en la cadena navegando hasta el bloque inicial.[8] Simplificando, todas las transacciones en el sistema son colectadas en bloques, los cuales aparecen en el software de todos los usuarios.[9]

Las criptomonedas pueden tener varias formas, pero la clasificación más común se las divide en dos grupos: las monedas virtuales que tienen su propria cadena de bloques, y los "tokens", que utilizan la "blockchain" de otras monedas. Se puede agrupar las monedas también como el Bitcoin o las criptomonedas alternativas, llamado "altcoins". Como el Bitcoin es de código abierto, los usuarios tienen la posibilidad de altear el código del software. El motivo de cambiar el código es dar nuevas características al software y, así crear una moneda nueva. Por supuesto, se puede crear nuevas monedas también, si se crea una cadena de bloques enteramente nueva.[10]

Las características más importantes de las criptomonedas pueden ser resumidos en los siguientes puntos:

- la tecnología "blockchain" garantiza para sus usuarios ser anónimos,
- no son dependientes de ningún gobierno, agencia o autoridad,
- se las puede convertir fácilmente a diferentes monedas (como por ejemplo dólar estadounidense o euro), así tiene una liquidez bastante grande,
- es difícil falsificar[11] (más o menos imposible).

---

[7] Tamás, Gábor y Gábor Dávid, Kiss, "Bevezetés a kriptovaluták világába." *Gazdaság és Pénzügy*, no. 1. (2018): 38.

[8] José Miguel Domínguez Jurado; Ricardo García Ruiz, "Blockchain y las criptomonedas: el caso bitcoin." *Oikonomics* 10 (2018): 60-61.

[9] Cath Senker, *Cybercrime and the darknet. Revealing the hidden underworld of the internet* (London, Arcturus Holdings Limited, 2017), 127.

[10] Gyöngyi Bugár y Márta Somogyvári, "Bitcoin: digitális szemfényvesztés, vagy a jövő valutája?" *Hitelintézeti Szemle* no. 1. (2020): 137-138.

[11] Michelle Vásquez Leiva, "Bitcoin: ¿Moneda o burbuja?" *Revista Chilena de Economía y Sociedad* no. 1-2. (2014): 54.

Es importante notar que una transacción se puede realizar con criptomonedas, pero como las naciones no las aceptan como monedas de curso legal, si "compramos" algo con criptomonedas, legalmente no es compra sino un intercambio de bienes o mercancías.[12] A pesar de este hecho, tenemos que resumir que el desarrollo de las criptomonedas es un proceso beneficioso, porque la propagación de las innovaciones digitales puede mejorar la competitividad del sistema financiero[13], también la tecnología de libros descentralizados puede ser utilizada para el desarrollo de los contratos o registros electrónicos.[14]

3. La relación entre las criptomonedas y los ciberdelitos

3.1. El ciberterrorismo y la financiación del terrorismo con el uso de las criptomonedas

Como el fenómeno de ciberterrorismo todavía no tiene una definición internacionalmente aceptada, solamente podemos entender a través de las diferencias que tiene comparado al terrorismo "tradicional" y otros cibercrímenes.
La regulación húngara sobre el terrorismo se puede encontrar en la Ley C de 2012 sobre el Código Penal, bajo el parágrafo 314, titulado "Acto de Terrorismo":
"Una persona que, con el propósito de
a) coaccionar a un órgano estatal u otro estado u organización internacional para hacer, no hacer o tolerar algo,
b) intimidar a una población,
c) cambiar o interferir con el orden constitucional, social o económico de otro estado, o interferir con el funcionamiento de una organización internacional comete un delito violento contra una persona, un delito que cause peligro público o un delito

[12] András Kecskés y Zsolt Bujtár, "A kriptovaluta ökoszisztéma európai uniós és a svájci szabályozásának összehasonlítása." *JURA* no. 2. (2018): 427.
[13] Alexander Szívós, "A pénzügyi kultúra." acceso: 28.12.2020., https://arsboni.hu/a-penzugyi-kultura/
[14] Zsolt Bujtár, „A kriptovaluták európai és máltai szabályozásának összehasonlítása. A máltai sólyom szárnyalása." *Európai Jog* no. 5. (2018): 14.

relacionado con un arma, según se especifica en el párrafo (4), es culpable de un delito grave y será castigado con prisión de diez a veinte años o cadena perpetua."[15]

Si hablamos sobre los actos del terrorismo, podemos decir que su perpetración generalmente necesita presencia personal, a veces sospechosos actos de preparación (como la compra de armas o explosivos), y recursos financieros, también. En contraste, el ciberterrorismo no requiere la presencia personal, debido al hecho que la mayoría de sus actividades sucede en el ciberespacio, que también proporciona anonimato a los ciber-terroristas. Además, la única cosa que tienen que comprar es un ordenador.

Como fue anteriormente mencionado, el ciberterrorismo no tiene una definición uniformemente aceptada, pero varios investigadores intentaron crearla.[16] Hay autores quienes piensan que actualmente no existe el fenómeno de ciberterrorismo[17], pero todos los investigadores del tópico están de acuerdo en la amenaza que el ciberterrorismo significa (sea ahora o en el futuro). Sobre la definición hay dos puntos de vista: unos autores dicen que el ciberterrorismo incluye todos los actos que los grupos terroristas conducen en la red, y otros piensan que el ciberterrorismo es un fenómeno más estrecho, como por ejemplo ciberataques en contra de instituciones o gobiernos.[18] Los autores que piensan que el ciberterrorismo todavía no existe, en general creen en la definición estrecha. Hoy en día, la definición más amplia tiene más sentido, porque ya podemos encontrar ejemplos concretos para el uso terrorista de la red, pero normalmente el fenómeno se agota en la difusión de las ideas en sitios web como Twitter, Facebook u otras páginas web o el reclutamiento de miembros en la media social.

La red oferta nuevas oportunidades para la financiación de los grupos terroristas también, y entre estas nuevas maneras las criptomonedas también pueden entrar en

---

[15] Ley C de 2012 sobre el Código Penal, 314. § (1)

[16] En un estudio de 2004, Mohammad Iqbal recogió una serie de definiciones de varios autores. Para más información Véase.: Mohammad Iqbal, "Defining Cyberterrorism." *John Marshall Journal of Computer and Information Law* 22, no. 2. (2004): 397-408.

[17] Eddy Willems, *Cyberdanger. Understanding and Guarding Against Cybercrime* (Cham, Springer International Publishing, 2019), 51.

[18] "Ciberterrorismo" acceso: 31.12.2020., http://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

juego. Sin embargo, todavía hay sólo un corto número de casos confirmados y públicamente documentados de la financiación del terrorismo con la utilización de criptomonedas.[19] Esto lo que puede significar con dos posibilidades. La primera sea la alta latencia[20] de estas formas del crimen, que es una característica determinada de los delitos cometidos con la tecnología "blockchain". La segunda posibilidad proviene de la desconfianza de terroristas en el sistema de monedas virtuales.[21] Como es una tecnología bastante nueva, todavía tiene varias vulnerabilidades. Los ataques cometidos contra un sistema de criptomonedas pueden tener diversas formas: el robo de la clave privada del usuario ("theft"), la prevención del proceso de las transacciones ("spending denial"), la revelación de la identidad del usuario ("deanonymization") o los ataques sistemáticos que apagan el sistema para todos los usuarios ("systemic attacks"). Es claro, que los ataques mencionados pueden ser cometidos contra el monedero de los grupos terroristas también. Esta inseguridad puede ser el motivo de que la forma de financiación del terrorismo todavía no se cambió totalmente.[22]

3.2. El blanqueo de dinero y las monedas virtuales

Un buen ejemplo puede ser al blanqueo de dinero, el caso de Liberty Reserve, que posiblemente fue el más grande blanqueo de dinero en la red tratado en los Estados Unidos. Con origen costarricense, esta moneda era utilizada para blanquear miles de millones de dólares. El sistema era demasiado fácil de utilizar: para abrir una cuenta Liberty Reserve, solamente tenían que dar un nombre, una fecha de nacimiento y una dirección, pero no requería que los usuarios registraran para validar su identidad con

[19] Cynthia Dion-Schwarz; David Manheim y Patrick B. Johnston, *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats* (Santa Monica, RAND Corporation, 2019), 22.
[20] Para información sobre la latencia véase: László Korinek, *Rejtett bűnözés* (Közgazdasági és Jogi Könyvkiadó, Budapest, 1988)
[21] Es evidente, que con la evolución de las criptomonedas esta causa no se quedará general. Por supuesto, ya existen excepciones, pero el uso terrorista de este sistema todavía no es enteramente seguro. Por ejemplo, véase el caso siguiente: https://www.nytimes.com/2020/08/13/us/politics/bitcoin-terrorism.html, acceso: 14.12.2020.
[22] Dion-Schwarz, Manheim y Johnston, *Terrorist Use of Cryptocurrencies*, 38.

copias de identificaciones oficiales (por ejemplo, tarjetas o licencias). Por lo tanto, los delincuentes fácilmente fueron capaces de utilizar identidades ficticias o anónimas para conducir sus transacciones[23], que favoreció para el crimen organizado[24].

3.3. Los esquemas de pirámide y el ciberespacio: el rol de las monedas virtuales

Con la popularización de esas monedas virtuales, para los inversores también han empezado a ser interesantes, lo que se ha convertido en el crecimiento de los esquemas de pirámide en conexión con las criptomonedas. Algunos investigadores dicen que el Bitcoin y esas monedas son esquemas de pirámide también, pero en el caso del Bitcoin los inversores han recibido una moneda que tiene valor real, y que se puede gastar en lo que quieran, además se puede cambiarlas fácilmente en cualquier moneda. Por eso, el Bitcoin no representa un riesgo directo para los inversores, ni ofrece una rentabilidad increíblemente alta[25] (que son las características más importantes de esos esquemas). Basado en estos hechos, el Bitcoin puede considerarse una forma de inversión relativamente segura, pero hay que señalar que cada criptomoneda es de un origen diferente, por lo que los inversores todavía tienen que tener cuidado con las nuevas monedas virtuales. Un ejemplo relevante puede ser el caso OneCoin, que prometió a sus inversores una rentabilidad de 5% por mes o 1% por semana que es libre de riesgos, pero al final resultó en ser parte de un esquema piramidal internacional.[26] El caso de BitConnect también puede servir como un buen ejemplo. La esencia del caso fue que una empresa ofrecía más de 1000% de ganancias

[23] Alan Brill; Lonnie Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?" *Defence Against Terrorism Review* no. 1. (2014): 18-20.
[24] Para ver más información sobre el crimen organizado véase: László Kőhalmi, "Szervezett bűnözés" in *Alkalmazott kriminológia,* ed. Tünde A. Barabás (Budapest, Ludovika Egyetemi Kiadó, 2020), 461-474.
[25] Eszteri Dániel, , *A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben.* (Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2015), 159-161.
[26] Tóth Dávid, "A virtuális pénzekkel kapcsolatos visszaélések." in *Rendészet-Tudomány-Aktualitások. A rendészettudomány a fiatal kutatók szemével*, eds. Noémi Emőke, Baráth y József, Mezei (Budapest. Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, 2019), 244.

utilizando un algoritmo matemático. Este grupo del crimen organizado[27] ofreció una comisión a sus inversores para recaudar más personas a depositar su dinero en el esquema y mantener sus depósitos en la empresa durante un período determinado de tiempo.[28] Según la investigación de T. Moore, J. Han y R. Clayton, los inversores con conocimientos cibernéticos probablemente saben sobre las actividades ilegales detrás de estos sitios web, pero su objetivo es ocupar una posición alta en la pirámide con sus inversiones tempranas. Los investigadores argumentan que las criptomonedas como Liberty Reserve o Perfect Money son elementos esenciales de tales juegos, ya que brindan anonimato a los perpetradores. La mayoría de estas monedas se encuentran en países latinoamericanos como Costa Rica o Panamá, y la mayoría de sus ganancias provienen de los HYIP[29] (High Yield Investment Program).[30] De lo anterior, podemos ver que las criptomonedas se pueden relacionar con esquemas piramidales de dos formas: si la moneda se crea con la intención de ser un esquema piramidal en sí mismo, o si la moneda virtual no es originalmente un esquema de pirámide, sino que se usa para ello.

3.4. La "Cryptojacking"

Para entender el fenómeno de "cryptojacking", primero tenemos que saber cómo funciona la minería de las criptomonedas. La minería es un proceso en que ordenadores de alta potencia resuelven problemas matemáticos computacionales en el sistema de bitcoin u otras monedas virtuales. Cada vez un problema está resuelto,

---

[27] Se puede leer más sobre el crimen organizado en: Dávid, Tóth; István László, Gál y László, Kőhalmi, "Organized Crime in Hungary." *Journal of Eastern-European Criminal Law* no. 1. (2015): 22-27.

[28] Simon Béla, "Kriptovaluták – rendészeti válaszok" *Belügyi Szemle* no. 10. (2018): 82.

[29] Los programas de inversión de alto rendimiento (o HYIP para abreviar) son formas típicas de esquemas piramidales en la red mundial. Son sitios web que ofrecen constantes beneficios y enormes rendimientos sin riesgo, pero en realidad son inversiones fraudulentas. Véase para más información: https://www.investor.gov/protect-your-investments/fraud/types-fraud/high-yield-investment-programs, acceso: 07.10.2020.

[30] Tyler Moore; Jie Han y Richard Clayton, "The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs" in *Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 7397,* ed. A.D., Keromytis (Berlin, Heidelberg, Springer, 2012), 41-56.

el sistema genera nuevos bitcoins para estos usuarios que ayudan al sistema. El proceso también sirve para verificar las informaciones de transacciones en los bloques.[31] Hoy en día, la minería es el recurso más importante de bitcoin, pero los problemas matemáticos cada vez son más difíciles, y por eso, rápidamente este método va a ser inalcanzable para la mayoría de los ordenadores.[32] Cualquier persona que tiene un ordenador bastantemente fuerte puede empezar a minear. Pero el problema con el proceso es que los ordenadores consuman mucha energía mientras trabajan, además los procesos matemáticos son complejos y con tiempo, pueden causar daños en los componentes de ordenadores.
La "cryptojacking" es un proceso en que un programa maligno está instalado al ordenador de la víctima que permite al perpetuador tomar el control sobre el ordenador, que se va a utilizar para minear criptomonedas a su proprio monedero sin el permiso de la víctima.[33] Como ya ha sido mencionado, minear puede causar daños en el ordenador, además el proceso gasta mucha energía, que puede costar un montón de dinero al usuario. Por eso, la cryptojacking también es un crimen peligroso, una forma de enriquecimiento injusto que se incluye en el acceso no autorizado de un sistema de tecnología computacional.

4. A modo de conclusión

La aparición de las nuevas tecnologías siempre resultan en un "vacuum iuris", y plantean la pregunta de la regulación, causando problemas para los legisladores. La situación es la misma con las criptomonedas. Es evidente que alguna forma de regulación es necesario, porque el sistema mantiene un montón de posibilidades para los perpetuadores de delitos trasladados a la red como los fraudes, los esquemas de pirámide, o para los hackers cometiendo nuevos crímenes como la cryptojacking. Además, tenemos que contar con la amenaza de que la evolución de estas monedas

[31] "Minería de Bitcoin" acceso: 20.12.2020, https://www.investopedia.com/terms/b/bitcoin-mining.asp
[32] Tibor Gazdag y Zoltán Kovács, "Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei" *Nemzetbiztonsági Szemle* no. 2. (2014): 42.
[33] Willems, *Cyberdanger*, 108-109.

va a ser más favorable para los criminales quienes todavía no utilizan la tecnología, debido a las deficiencias del sistema (por ejemplo, la financiación del terrorismo o el ciberterrorismo). En mi opinión, la identificación y el reconocimiento de los desarrolladores de criptomonedas sea la clave para empezar una negociación con ellos sobre la regulación. Por otro lado, estas monedas fueron creadas con la intención de que no sean controladas y reguladas por ningún estado, gobierno, banco o agencia. La razón más grande de su utilización es el anonimato. Esto significa, que con la regulación de las criptomonedas sus sentidos elementales serán destruidos y la mayoría de los usuarios dejen de utilizarlas con el comienzo de la regulación, y como siempre, los criminales empiecen a buscar nuevos métodos.

El otro problema urgente que tenemos que resolver es la creación de las definiciones adecuadas. El primer escalón de la escalera hacia la regulación de los nuevos cibercrímenes y las criptomonedas será la elaboración de las definiciones en que todavía no estamos de acuerdo. Para esta fase, la cooperación de los juristas y los profesionales de T.I. es fundamental, porque una legislación adecuada asume altos conocimientos informáticos.