

Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

**Jelen tudományos munka az értekezés nem végleges, műhelyvitára szánt
változata**

Gáti Balázs

**A személyes adatok védelme a bűnügyi tudományokban az irányelvi
szabályozás tükrében**

Doktori értekezés



Témavezetők:

Prof. habil. Dr. Kőhalmi László tanszékvezető, egyetemi tanár

Dr. Tóth Dávid egyetemi adjunktus

Pécs, 2024

„Az okok és okozatok hatalmas láncolatában egyetlen adat sem vizsgálható elszigetelten”

Alexander von Humboldt

Köszönetnyilvánítás

Hálával és tisztelettel tartozom témavezetőmnek, Kőhalmi László professzor úrnak, aki nem csak szakterületének kiváló ismerője, hanem olyan átfogó szemlélettel rendelkező tudós, aki már évekkel korábban megjelent tudományos munkáiban is olyan kérdéseket vetett fel – akár a technikai fejlődés és a jog, akár az emberi jogok vagy az adatvédelem területén –, amelyek ma az uniós jogalkotás aktuális kérdései. Példamutatása, segítőkészsége és iránymutatásai rendkívül hasznosak voltak számomra. Társ-témavezetőm Tóth Dávid adjunktus, precizitásával, saját kutatási módszertanának megismertetésével, közvetlen tanácsaival és közös publikációinkkal segítette előmeneteletem.

Szeretném köszönetemet kifejezni egykori tanáromnak, Szőke Gergely László adjunktusnak, aki mellett eltöltött demonstrátori éveim meghatározóak voltak számomra. Az adatvédelmi reform iránti lelkesedése és kutatásai a jelen kutatómunkához vezető út kiindulópontját jelentették számomra.

Megtiszteltetés volt számomra velük és minden kedves kollegámmal együtt dolgozni.

Tartalomjegyzék

I. Bevezetés	7
1. A témaválasztás indoklása, aktualitása	9
2. A kutatás célja, hipotézisek	12
3. A kutatás módszerei.....	13
4. Az értekezés tárgya és felépítése	14
II. Előzmények	15
1. Az adatvédelem fogalmával kapcsolatos megfontolások	16
2. Az adatvédelmi jog fejlődésének főbb állomásai	19
3. Az Európai Unió jelenlegi szabályozása – A személyes adatok védelmének általános jogszabályi háttere és intézményei	22
3.1. Az adatvédelmi reform	22
3.2. Az Európai Adatvédelmi Biztos és az Európai Adatvédelmi Testület és az Európai Bíróság szerepe	25
3.2.1. Az Európai Adatvédelmi Testület (EDPB)	25
3.2.2. Európai Adatvédelmi Biztos (EDPS).....	28
3.2.3 Bűnüldözésű célú releváns irányelvek az EDPB és EDPS gyakorlatában.....	29
3.2.4. Az Európai Unió Bírósága (EUB).....	35
III. A Bűnügyi Adatvédelmi Irányelv (LED) - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv és jogharmonizációja	36
1. A bűnügyi adatvédelmi irányelv bemutatása.....	36
2. A bűnügyi irányelv jogharmonizációja	52
2.1. A bűnügyi irányelv átültetése a magyar nemzeti jogba	54
2.1.1. Előzmények	54
2.1.2. Implementálás a 2011. évi CXII. törvénybe	55
2.2. A bűnügyi irányelv átültetése a német nemzeti jogba	62
2.2.1. Előzmények.....	63
2.2.2. A német szövetségi adatvédelmi törvény az adatvédelmi reform után	65
2.3 A bűnügyi irányelv átültetése a francia nemzeti jogba.....	75
2.3.1 Előzmények.....	75
2.3.2. A francia adatvédelmi törvény első módosítása, az 1978. január 6-i 78-17. számú törvényhez	77
2.3.3. A francia adatvédelmi törvény második módosítása, az 1978. január 6-i 78-17. számú törvényhez.....	78

2.4 A bűnügyi irányelv átültetése a svéd nemzeti jogba.....	84
2.4.1. Előzmények.....	84
2.4.2. Az SFS 2018:218 számú törvény, az EU adatvédelmi rendelete szerinti kiegészítő rendelkezésekkel	85
2.4.3. A svéd bűnügyi adatokról szóló törvény SFS 2018:1177	89
3. Az egyes nemzeti szabályozások összehasonlító vizsgálata	92
3.1. Jogharmonizáció a nemzeti jogrendszer sajátosságai alapján	93
3.2. Az egyes nemzeti szabályozások összehasonlítása az Irányelv egyes szempontjai szerint.....	95
IV. A bűncselekményekhez kapcsolódó személyes adatok védelme.....	105
1. Elméleti megfontolások a bűnügyi célú adatkezelések kapcsán	105
2. A büntetőeljárás adatvédelmi vonatkozásai	107
2.1. A gyanúsított személyes adatainak kezelése.....	111
2.2. A tanú személyes adatainak kezelése	114
2.3. A vádlott személyes adatainak kezelése	115
2.4. A sértett személyes adatainak védelme.....	118
3. A szakértő a büntetőeljárásban és a személyes adatok védelme	119
4. Az adatkezelés jogalapja és az adatvédelem a büntetőeljárás törvényben	121
5. A személyes adatok zártan történő kezelése.....	123
6. A tárgyalás nyilvánosságának elve és a természetes személyek adatainak védelme	127
7. A bírósági adatkezelési műveletek ellenőrzése	139
8. A büntetésvégrehajtás adatvédelmi vonatkozásai	141
8.1 Általános megfontolások	141
8.2. Jogszabályi háttér.....	144
8.3. Adatkezelési elvek a büntetésvégrehajtás során	146
8.3.1.A Bv.tv. alapvető rendelkezései.....	146
8.3.2. Bv.tv. - Az adatkezelésre vonatkozó rendelkezések	149
8.4. A fogvatartott nyilvántartása.....	154
8.5. Mesterséges intelligencia rendszerek és a büntetésvégrehajtás kapcsolata és annak hatása a személyes adatok védelmére	158
V. Az adatvédelem és a kiberbűnözés kapcsolata.....	161
1. A kiberbűnözés fogalma.....	162
2. A kiberbűncselekmények jellegzetességei	165
2.1 Hacking és adathalász jellegű bűncselekmények	165
2.2. Online térben elkövetett zsarolás jellegű bűncselekmények	166
2.3 Jogszabályi háttér	167

3. Személyes adatok - mint a kiberbűncselekmények elkövetési tárgyai.....	170
3.1. A Bűnügyi Adatvédelmi Irányelv és a GDPR lehetséges hatásai a személyes adatok védelmére a kiberbűnözés vonatkozásában	171
3.2. Az (EU) 2022/2555 Irányelve (NIS 2) és az adatvédelem kapcsolódási pontjai.....	175
3.3. A személyiséglopás jelensége.....	179
VI. A személyes adatokkal kapcsolatos bűncselekmények de lege lata	182
1. Személyes adattal visszaélés	183
1.1. Jogi tárgy.....	184
1.2. Tényállási elemek és stádiumok	184
1.3. Minősített esetek	188
1.4. Rendbeliség.....	189
2. Magántitok megsértése	192
2.1. Jogi tárgy.....	192
2.2. Tényállási elemek	192
2.3. Stádiumok és tettesség	194
2.4. Bűncselekményi egység és a bűncselekmények találkozása	194
3. Levéltitok megsértése	195
3.1. Jogi tárgy.....	196
3.2. Tényállási elemek	196
3.3. Stádiumok és tettesség	197
3.4. Minősített esetek	197
3.5. Jogellenesség hiánya.....	198
3.6. Bűncselekményi egység és a bűncselekmények találkozása	198
4. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények	198
4.1. Tiltott adatszerzés	199
4.1.1. A bűncselekmény jogi tárgya: a személyes adat, magántitok, gazdasági titok, üzleti titok védelme.	200
4.1.2. Elkövetési tárgy és magatartás	200
4.1.3. Tettesség.....	201
4.1.4. Minősített esetek	201
4.2. Információs rendszer vagy adat megsértése	202
4.2.1. A bűncselekmény jogi és elkövetési tárgya	202
4.2.2. Elkövetési magatartások.....	203
4.2.4. Rendbeliség	206
4.3. Információs rendszer védelmét biztosító technikai intézkedés kijátszása	207
4.3.1. A bűncselekmény tárgya	207

4.3.2 Elkövetési magatartás.....	207
4.4. Az információs rendszer felhasználásával elkövetett csalás.....	209
4.4.1. Jogi tárgy és a tényállás szerkezete	210
4.4.2 Elkövetési tárgy.....	210
4.4.3 A bűncselekményi alakzat elkövetési magatartásai	210
4.4.4. Stádiumok.....	211
4.4.5 Tettesség.....	211
4.4.6 Minősített esetek	212
4.4.7. Bűncselekményi egység és a bűncselekmények találkozása.....	212
4.4.8. Elektronikus készpénz-helyettesítő fizetőeszközzel való visszaéléssel megvalósuló alakzat	212
VII. Összefoglalás - Az eredmények bemutatása.....	215
1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése	215
2. Első hipotézissel kapcsolatos eredmények áttekintése - A Bűnügyi Adatvédelmi Irányelv (LED) és jogharmonizációja	216
3. Második hipotézissel kapcsolatos eredmények áttekintése - Bűncselekményekhez kapcsolódó személyes adatok védelme a büntetőeljárás és a büntetésvégrehajtás során...	222
4. Harmadik hipotézissel kapcsolatos eredmények áttekintése - Az adatvédelem és a kiberbűnözés kapcsolata	228
5. Negyedik hipotézissel kapcsolatos eredmények áttekintése - A személyes adatokkal kapcsolatos és az információs rendszerrel kapcsolatos bűncselekmények	230
VIII. Summary	237
IX. Irodalomjegyzék.....	238

I. Bevezetés

A globalizáció térnyerése és az információs technológia fejlődése jelentősen átalakította az adatkezelés és adatvédelem területét, új kihívások elé állítva az Európai Uniót. Az Európai Bizottság 2012-ben kezdeményezett egy adatvédelmi reformot célzó javaslat csomagot, melynek célja az adatvédelem modernizálása volt a digitális kor igényeihez igazodva. Ennek eredményeképpen az Európai Parlament és a Tanács 2016 áprilisában elfogadta az új uniós adatvédelmi csomagot, amely két fő jogforrást tartalmaz: az általános adatvédelmi rendelet¹ és a bűnüldözési célú adatkezelésre vonatkozó irányelvet.²

Az EU 2016/680 irányelve az adatvédelmi jogok biztosítására irányul a bűnüldözési céllal kezelt személyes adatok esetében, elősegítve ezzel az áldozatok, tanúk és gyanúsítottak jogainak védelmét.³ Az uniós és schengeni országok illetékes hatóságai által kezelt személyes adatok védelmére vonatkozó szabályok harmonizálásával hozzájárul a hatóságok közötti bűnüldözési célú adatcsere bizalmának és biztonságának növeléséhez, és ezáltal a bűnözés és a terrorizmus elleni küzdelemben a határokon átnyúló együttműködés megkönnyítéséhez^{4,5}.

¹Európai Parlament és Tanács. 2016. "(EU) 2016/679 Rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)." *Hivatalos Lap L 119* (2016. május 4.): 1–88.

²Európai Parlament és Tanács. 2016. "(EU) 2016/680 Irányelv a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről." *Hivatalos Lap L 119* 89–131.

³Eszteri, Dániel. "A bűnügyi adatvédelmi irányelv." In: Buzás, Péter; Péterfalvi, Attila; Révész, Balázs (eds.) *Magyarázat a GDPR-ról*. Budapest, Hungary: Wolters Kluwer, 2018, pp. 385-401.

⁴European Commission. "A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – Első jelentés az EU biztonsági unió-stratégiájáról," COM (2020) 797 final,

⁵Nagy Zoltán András, Mezei Kitti. „Az Európai Unió Bűnügyi Adatvédelmi Irányelvről” In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) *A XXI. század biztonsági kihívásai Pécs, Magyarország* : Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport (2018) 378 p. pp. 229-234.

Ennek érdekében az irányelv specifikus, differenciált szabályokat állít fel, amelyek meghatározzák a rendőrségi és igazságügyi adatkezeléseket, biztosítva az adatok szabad áramlását.⁶

Ahogy a rendeletet, úgy az irányelvet is megelőzték a technikai-ipari forradalom jelentős változásai.⁷ Az Unió Biztonsági stratégiája⁸ hangsúlyozza, hogy az olyan új technológiák, mint a mesterséges intelligencia, hatékony eszközként használhatók a bűnözés elleni küzdelemben.^{9,10} E lehetőségek kiaknázása azt is jelenti, hogy biztosítani kell az alapvető jogoknak való megfelelés legmagasabb szintű normáit. A személyes adatok védelmét szabályozó jogszabályok képezik ezen normák alapját, amelyre további ágazati szabályozások épülhetnek.

A negyedik ipari forradalom korában élünk, amely nem csak a gazdasági és technológiai területeken hozott forradalmi változásokat, hanem a bűnözési módszerekben is új dimenziókat nyitott meg.^{11,12} Ez a helyzet újabb és egyre összetettebb kihívások elé állítja a jogalkotókat, akiknek folyamatosan alkalmazkodniuk kell az új bűnelkövetési formákhoz, miközben a jogi keretrendszert is naprakészen kell tartaniuk.^{13,14,15} Ebben a kölcsönhatásban értelmezhető az adatvédelem is. Szükségessé válhat a jelenlegi szabályozási gyakorlat felülvizsgálata, további

⁶(EU) 2016/680 Preambulum (10) A Lisszaboni Szerződést elfogadó kormányközi konferencia zárónyilatkozatához csatolt, a büntetőügyekben folytatott igazságügyi, valamint a rendőrségi együttműködés területén a személyes adatok védelméről szóló 21. sz. nyilatkozat.

⁷Szöke Gergely László. *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén.* Budapest: HVG–ORAC Lap- és Könyvkiadó Kft., 2014,

⁸ European Commission. "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy," COM (2020) 605 final,.

⁹ Fantoly, Zsanett; Herke, Csongor. "A mesterséges intelligencia a hatékonyabb büntetőeljárás szolgálatában." *Magyar Jog*, 48:4, 223-228, 2023.

¹⁰ Eszteri, Dániel; Péterfalvi, Attila. "Amikor a gépeink tanulnak minket, avagy a mesterséges intelligencia alapú döntéshozatal és profilozás szabályozásának európai uniós törekvéseiről." *Századvég*, 2022:1, 95-119, 2022.

¹¹ Schwab, Klaus. *The Fourth Industrial Revolution.* World Economic Forum, 2016.

¹² Ambrus, István. *Digitalizáció és büntetőjog.* Budapest: Wolters Kluwer, 2021, p.290.

¹³ Brynjolfsson, Erik, and McAfee, Andrew. "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies." W.W. Norton & Company, 2014.

¹⁴ Hannes Westermann, Michael Joyce, and Benoit Dupont: *Artificial Intelligence in the Context of Crime and Criminal Justice.* 2019. Korean Institute of Criminology.

¹⁵ Nagy Zoltán András. "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor, 49. Budapest: Dialóg Campus, 2020, p.50

pontosítása a büntetőjogi szankciókat, a nyomozást, vádeljárást, a büntetésvégrehajtást és az adattovábbításokat érintő területeken is.

1. A témaválasztás indoklása, aktualitása

Témaválasztásom indoka, hogy a bűnügyi személyes adatok védelmének szabályozása, jogharmonizációja és gyakorlata az Európai Unió tagállamaiban eltérő lehet, ami kihívásokat és komplex jogi kérdéseket vet fel az adatvédelmi normák egységes értelmezése, ennek következtében az adattovábbítás, a határokon átnyúló bűnügyi együttműködés^{16,17} szempontjából. Az európai adatvédelmi jogharmonizáció és az egyes tagállamok gyakorlatának összevetése rávilágíthat arra, hogy mely területeken szükséges további összehangolás vagy jogalkotási intézkedés, hogy a bűnüldözés és az adatvédelem közötti egység biztosított legyen az Unió területén.^{18,19}

Alapvető fontosságú, hogy hogyan járul hozzá az adatvédelmi reform a nemzetközi bűnüldözés elleni küzdelemhez a hazai és az egyes tagállami jogi szabályozás gyakorlata révén.^{20,21}

¹⁶ Köhalmi, László. "A nemzetközi bűnügyi együttműködés." In *Magyar büntetőjog: Általános rész*, szerkesztette Balogh Ágnes és Tóth Mihály, 375-386. Budapest: Osiris Kiadó, 2010.

¹⁷ Eszteri, Dániel. (2021) "A bűnügyi adatvédelmi irányelv az Infotv. kontextusában." In *Magyarázat a GDPR-ról: második, bővített kiadás*, szerkesztette Bendik, Tamás; Árvay, Viktor; Bojnár, Katinka; Eszteri, Dániel; Majsa, Ágnes; Osztopáni, Krisztián; Sziklay, Júlia - Péterfalvi, Attila; Buzás, Péter; Révész, Balázs, 489-506. Budapest, Magyarország: Wolters Kluwer Hungary

¹⁸ Gál, István László, és Tóth, Mihály.(2016) "Az uniós jog és a magyar jogrendszer viszonya - büntető anyagi jogi jogharmonizáció." In *Az uniós jog és a magyar jogrendszer viszonya*, szerkesztette Tilk Péter, 463-494. Pécs: PTE Állam- és Jogtudományi Kar

¹⁹ Jánosi, Andrea.(2022) "Bűnüldözési célú adatkezelés – releváns EU jogforrások, az EU rendszereinek interoperabilitása." *Miskolci Jogi Szemle: A Miskolci Egyetem Állam- és Jogtudományi Karának Folyóirata*, 17:5, 151-161

²⁰ Köhalmi, László.(2012) "Európai biztonság avagy az egységes európai büntetőjog víziója." In *A rendészettudomány határkövei: Tanulmányok a Pécsi Határőr Tudományos Közlemények első évtizedéből*, szerkesztette Gaál Gyula és Hautzinger Zoltán, 257-276. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport

²¹ Bendik Tamás (2021) "A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása." In *Magyarázat a GDPR-ról: második, bővített kiadás*, szerkesztette Bendik, Tamás; Árvay, Viktor; Bojnár, Katinka; Eszteri, Dániel; Majsa, Ágnes; Osztopáni, Krisztián; Sziklay, Júlia - Péterfalvi, Attila; Buzás, Péter; Révész, Balázs, 489-506. Budapest, Magyarország: Wolters Kluwer Hungary

Ezen belül fontosnak tartom az Európai Bizottság (továbbiakban Bizottság) által véleményezett és vizsgált gyakorlatot, és annak nemzeti jogba történő átültetését, amely irányadó a büntetőjogi szabályozás területén is.²²

Globalizált világunkban a bűnözés, különösen a számítógépes bűnözés és más, a kibertérrel összefüggő bűncselekmények egyre inkább határokon átnyúló jellegűek.^{23,24} Az illetékes hatóságok még a belföldi ügyek kivizsgálása során is egyre gyakrabban találkoznak határokon átnyúló helyzetekkel, mivel az információkat elektronikusan gyakran egy harmadik országban tárolják.²⁵ Ez fokozza a nemzetközi együttműködés szükségességét a bűnügyi nyomozásokban, mind a tagállami hatóságok, mind az olyan uniós szervek, mint az Europol és az Eurojust részéről.²⁶ Ez az együttműködés, és különösen az elektronikus bizonyítékok gyűjtése és cseréje gyakran személyes adatok átadásával járnak, ezért alapvető fontosságúak a megfelelő adatvédelmi biztosítékok.²⁷ Erre jó példa a Budapesti Egyezmény 2. Kiegészítő jegyzőkönyve, mely az elektronikus bizonyítékok határon túli továbbításának szabályozása mellett külön fejezetet szentel az adatvédelmi biztosítékoknak.^{28,29}

Az ilyen biztosítékok hozzájárulnak a bűnüldöző hatóságok közötti bizalomépítéshez is, gyorsabb és hatékonyabb információcserét biztosítanak, és erősítik a jogbiztonságot a büntetőeljárásokban.³⁰ Ebben a tekintetben az irányelv fontos eszközkészletet biztosít a

²² Gombos, Katalin. *Az Európai Unió Joga*. Budapest: Patrocinium Kiadó, 2017.p.128

²³ Mezei Kitti. (2020.) "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre." *Állam- és Jogtudomány* 61, (4) ,p.66

²⁴ Ambrus, István. *Digitalizáció és büntetőjog*. Budapest, Magyarország: Wolters Kluwer Hungary, 2021.

²⁵ Simon, Béla, Gyarak, Réka.(2020) "Kiberbűncselekmények felderítése és nyomozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss, Tibor, 121-150. Budapest, Magyarország: Dialóg Campus Kiadó,

²⁶ Szijjártó, István (2019). "Az Europol és az Eurojust szerepe a közös nyomozócsoportokban." *Ügyészek Lapja*, 26 (6), 59-73

²⁷01/2021.számú ajánlás a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti megfeleléségi referenciáról https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_hu.

²⁸ Gáti, Balázs.(2021) "Az adatvédelem számítástechnikai bűnözéssel összefüggő aktuális kérdései - Adatvédelmi kérdések a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv Tervezetével kapcsolatban." In *PhD Tanulmányok 15*, szerk. Kőhalmi, László, 23-58. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola

²⁹ Sorbán, Kinga.(2019) "Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában: Felelősség és kötelezettségek." In *Medias Res*, VIII, 1, 84-101

³⁰ Szendrei, Ferenc. (2019.) "Bűnügyi Együttműködés." In *A Bűnügyi Hírszerzés Kézikönyve*, szerkesztette: Szendrei Ferenc , Dialóg Campus Kiadó, 221–242.

személyes adatoknak az EU-ból harmadik országba vagy nemzetközi szervezethez - például az Interpolhoz - történő személyes adatok továbbításának megkönnyítésére, miközben biztosítja, hogy a személyes adatok továbbra is megfelelő szintű védelemben részesüljenek.^{31,32,33}

A téma aktualitását egyrészt a GDPR és a bűnügyi irányelv bevezetésével egyidejűleg az adatkezelőkre rótt kötelezettségek, valamint az azóta eltelt időszak tapasztalatai indokolják, ideértve a tagállami átültetés szerepét is.^{34,35}

Másrészt az informatika rohamos fejlődésének köszönhetően az egyes deliktumok elkövetése a kibertéren keresztül - az esetek túlnyomó többségében a személyes adatok sérelmével egyidejűleg - valósul meg. A digitális technológiák fejlődése és az online térben történő adatgyűjtés exponenciális növekedése új kihívásokat jelentenek a személyes adatok védelme területén.³⁶

A személyes adatok védelme nem csak az egyének jogainak garantálását szolgálja, hanem fontos eszköz a számítógépes bűncselekmények elleni küzdelemben is. A Fehér Könyv³⁷, és a Mesterséges Intelligencia törvénytervezet³⁸ példái annak, hogy az adatvédelmi kérdések egyre inkább integrálódnak a jogi szabályozásba a technológia fejlődésével párhuzamosan. Az adatvédelmi intézkedések közvetetten segíthetnek megakadályozni a kibertámadásokat.³⁹ Az

³¹(EU) 2016/680, Preambulum 25

³² Sorbán, Kinga. (2016) "A digitális bizonyíték a büntetőeljárásban." *Belügyi Szemle*, 64 (11), 81-96.

³³ Krasznay, Csaba. (2021) "Húsz év a globális kiberbűnözés elleni küzdelemben - A Budapesti Egyezmény értékelése." *Külügyi Szemle*, 20: Különszám, 191-214,

³⁴ Péterfalvi, Attila; Bendik, Tamás; Tóásó, Bálint. "A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai." Konferencia előadás, 1-12. 42. Jogász Vándorgyűlés, Miskolc-Lillafüred, Magyarország, 2019.

³⁵ Somssich, Réka. 2020. "A jogharmonizációs kötelezettségek teljesítésének módszertana és eszközrendszere 15 évvel a csatlakozás után." *Állam- és Jogtudomány LXI*, no. 2: 44-50.

³⁶ Eszteri, Dániel. "Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás." In *Szemelvények az információs jogokról - a rendszerváltástól napjainkig*, 164-193. Budapest: Patrocinium Kiadó, 2021.

³⁷ Fehér könyv a mesterséges intelligenciáról - A kiválóság és a bizalom európai megközelítése, COM(2020)65 final, 2020/C 364/12., https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf. (hozzáférés: 2021. február 2.)

³⁸ Európai Parlament és a Tanács. "Javaslat a Mesterséges Intelligenciára Vonatkozó Harmonizált Szabályok Megállapításáról és Egyes Uniós Jogalkotási Aktusok Módosításáról," COM(2021) 206 final

³⁹ Brown, A. (2020). "Enhancing Cybersecurity Through Data Protection Measures." *International Journal of Cybersecurity*, 12(4), 321-335.

adatvédelmi szabályok lehetővé teszik a hatóságok számára, hogy hatékonyabban és gyorsabban nyomozzanak az online bűncselekmények ügyében⁴⁰.

A megfelelő adatvédelmi intézkedések nem csak az egyének személyes adatainak védelmét szolgálják hagyományos környezetben, hanem hozzájárulnak a digitális környezetben való biztonság és stabilitás biztosításában.^{41,42,43}

2. A kutatás célja, hipotézisek

A kutatás célja, hogy a bűnügyi adatvédelmi irányelvi szabályozása alapján a bűnügyi tudományok területén megvizsgálja a természetes személyek adatainak védelmét a tagállami szintű szabályozás és a magyar büntetőeljárás, büntetésvégrehajtás és büntetőjogi szabályozás területén. Ennek érdekében célja,

- az EU bűnügyi adatvédelmi szabályozásának és jogértelmezésének elemzése: A jogharmonizáció vizsgálata a Bizottság és az Európai Adatvédelmi Testület felméréseinek fényében, valamint az irányelv gyakorlati megvalósulásának elemzése a tagállami jogba való átültetés során. Az elemzés célja további szabályozás és/vagy pontosítás szükségességének felmérése.
- a bűnügyi irányelv tagállami jogba történő átültetésének vizsgálata : A magyar jogi keretrendszer és intézményrendszer bemutatása, összehasonlítva a német, francia és svéd joggyakorlatokkal.
- a személyes adatok védelmének vizsgálata a büntetőeljárás- és végrehajtás kontextusában: A magyar joggyakorlat elemzése a gyanúsítottak, áldozatok és tanúk személyes adatainak védelmére tekintettel. A büntetőeljárás és büntetés-végrehajtás jogszabályainak adatvédelmi szempontú vizsgálata.

⁴⁰ Taylor, S. (2017). "Data Protection Laws and Law Enforcement: A Comparative Analysis." *European Journal of Law and Economics*, 28(1), 89-104.

⁴¹Csiszár, Cs. M. (2019.) "Adatvédelem a digitális térben avagy mennyire vagyunk biztonságban." In *Mérleg és Kihívások XI. Nemzetközi Tudományos Konferencia*, szerkesztette Veresné, S. M. és Lipták, K., 62-68. Miskolc, Magyarország: Miskolci Egyetem Gazdaságtudományi Kar.

⁴² Fenyvesi, Csaba.(2019.) "A kriminalisztikai világtendenciák - Különös tekintettel a digitális felderítésre." In *A Bűnügyi Tudományok és az Informatika*, 64–82.

⁴³ Gyaraki, Réka. "A digitális biztonság új kérdései." In *Metaverzum: Az állam requiemje?*, szerkesztette Beer, Miklós; Gyaraki, Eszter; Kondorosi, Ferenc; Sereg, Szabolcs; Virág, Dániel, 33-63. Budapest, Magyarország: Kornétás Kiadó, 2022.

- az online térben elkövetett bűncselekmények és az adatvédelem kapcsolatának feltárása: Az internetes környezetben elkövetett bűncselekmények és az adatvédelmi kérdések összefüggéseinek vizsgálata.
- a személyes adatokkal kapcsolatos bűncselekmények jogi elemzése: A bűncselekmények jogi tárgyának, elkövetési tárgyának, elkövetési magatartásainak, alanyi elemeinek, és a minősített esetek szerinti elemzése.

Ennek alapján hipotéziseim a következőkben fogalmazhatók meg:

1. Az uniós jogharmonizáció és a nemzeti jogrendszerek vonatkozásában feltételezem, hogy az irányelvi fogalmak értelmezésében az egyes tagállamok gyakorlata eltérő lehet. A tagállami átültetés eltérései befolyásolják a bűnügyi adatok védelmének egységes szintjét az Unión belül, így további szabályozási és/vagy pontosítási intézkedések szükségesek, elsősorban a megfelelés kellő szintjének biztosítása érdekében.
2. A személyes adatok védelme területén a büntetőeljárás, valamint a büntetés-végrehajtás jogszabályi feltételei adatvédelmi szempontból megfelelőek, azonban a jelenlegi jogszabályok alapján létrejött gyakorlatok a büntetőeljárás- és végrehajtási folyamatok területén nem mindig biztosítják az érintettek egyes kategóriáinak teljes körű védelmét, így további szabályozásra vagy megoldásokra van szükség a védelem megerősítéséhez.
3. Az internetes környezetben elkövetett bűncselekmények és az adatvédelmi kérdések összefüggéseinek vizsgálata kapcsán feltételezem, hogy az adatvédelmi szabályozás hatékony alkalmazása védelmet biztosít a természetes személyes adatainak tekintetében a kibertámadások ellen.
4. A személyes adatokkal kapcsolatos bűncselekmények büntetőjogi tényállásai és az ehhez szorosan kapcsolódó információs rendszer elleni bűncselekmények tényállásai megfelelnek az uniós keretrendszernek, azonban nem mindig fedik le teljes körűen a digitális térben elkövetett személyes adatokkal kapcsolatos bűncselekményeket a szankciókat illetően.

3. A kutatás módszerei

A disszertáció elkészítése során a témakör szempontjából lényeges nemzetközi, uniós és magyar jogforrások kerülnek felhasználásra. A joganyagok elemzése valamint az adott kérdésköröket tárgyaló, releváns nemzetközi, - többek között angolszász, német, francia, svéd, valamint a hazai jogirodalmat és kutatási eredményeket fogom bemutatni.⁴⁴ Összehasonlítom a különböző szabályozási szinteket és azok rendelkezéseit, illetve a vonatkozó joggyakorlatot, különös figyelemmel azok hasonlóságaira és különbözőségeire. A kutatás során alkalmazom még továbbá a normatív és a dogmatikai megközelítést, valamint egyes részeken a logikai és kritikai elemzéssel kiegészítve

4. Az értekezés tárgya és felépítése

A disszertáció bevezető részében az adatvédelem fogalmával kapcsolatos elméleti megfontolások, az adatvédelmi jog fejlődésének főbb állomásai, és a személyes adatok védelmének aktuális jogi szabályozása kerülnek bemutatásra.

Az értekezés további részeiben a 2016/680/EU irányelv - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv és jogharmonizációja bemutatása során, valamint a bűnügyi célú adatkezelésekkel kapcsolatos probléma felvetés kapcsán elemezni kívánom:

- a bűnügyi adatok védelmének uniós szabályozását és jogharmonizációját figyelemmel a Bizottság és az Európai Adatvédelmi Testület felméréseire. Kiemelt szempontként tekintek az egységes megközelítés vizsgálatára a jogértelmezési kérdéseket illetően, az adatvédelmi felügyelő hatóságok jogköreinek vizsgálatára, az adattovábbítással kapcsolatos megfelelőségi határozatok érvényesítésnek gyakorlatára,
- a bűnügyi irányelv átültetésének gyakorlatát a magyar jogba, bemutatva a magyar jogi szabályozás háttér- és intézményrendszerét, nemzetközi kitekintéssel az egyes tagállamok joggyakorlatára, - a német, a francia és a svéd nemzeti átültetés összehasonlító elemzésével,
- a bűncselekményekhez kapcsolódó személyes adatok védelmét, beleértve a gyanúsított, az áldozat és a tanú személyes adatainak védelmét, a büntetőeljárással és büntetés végrehajtással kapcsolatos adatvédelmi szempontokat, hangsúlyt fektetve a felmerülő nehézségekre, és azzal kapcsolatban a jogalkotó válaszaira,

⁴⁴ Az értekezés tárgyában megjelent tudományos közleményeim, és tanulmányaim felhasználásra kerültek, melyeket az egyes fejezetek elején külön kiemelve megjelöltem.

- a személyes adatokkal kapcsolatos bűncselekményeket, azok jogi tárgyát, elkövetési tárgyát, elkövetési magatartásait, a bűncselekmények alanyait, alanyi elemeit, és a minősített eseteiket, valamint
- a személyes adatokkal kapcsolatos online térben elkövetett bűncselekményeket és az adatvédelem közötti kapcsolódási pontokat.

II. Előzmények

A 2016 májusában elfogadott adatvédelmi reform „csomag” részei, az (EU) 2016/679 rendelete, (General Data Protection Regulation továbbiakban GDPR) az (EU) 2016/680 „bűnügyi adatvédelmi irányelve” (Law Enforcement Directive, továbbiakban LED) és az ezekhez később csatlakozott az (EU) 2018/1725 rendelete⁴⁵ (European Union Data Protection Regulation továbbiakban EUDPR) a természetes személyek védelméről, a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezeléséről, valamint ezen adatok szabad áramlásáról. Tágabb értelemben az adatvédelem tárgykörébe sorolható az elektronikus hírközlési adatvédelmi rendelet (ePrivacy Regulation)⁴⁶

A „2016-os csomag” két fő jogi eszköze a GDPR és a LED. A GDPR általánosan alkalmazandó keretet ad a személyes adatok kezelésére vonatkozóan. A rendelet hatálya alá eső érintettek meghatározott jogokkal rendelkeznek, amelyek sarokköve a személyes adataikhoz való hozzáférés, mely további jogok gyakorlását is lehetővé teszi, mint például a helyesbítéshez vagy a törléshez való jogot. Az adatkezelők - akik meghatározzák a személyes adatok kezelésének célját és eszközét - felelősek a GDPR által meghatározott szabályokkal összhangban történő adatkezelésért. Az adatkezelőknek tiszteletben kell tartaniuk a személyes adatok kezelésével kapcsolatos elveket, és biztosítaniuk kell az adatkezelés jogszerűségét.⁴⁷

Az egyes rendelkezésekre vonatkozó esetleges korlátozások mellett azonban a GDPR teljes mértékben kizár bizonyos egyéb elveket, mint a határellenőrzésre, menekültügyre, a

⁴⁵ (EU) 2018/1725 Rendelet a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről." *Hivatalos Lap* L 295 39–98.

⁴⁶ Európai Bizottság, Javaslat az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről szóló rendeletről (elektronikus hírközlési adatvédelmi rendelet), COM (2017) 10 final.

⁴⁷ (EU) 2016/679, 5-6. cikk.

bevándorlásra, a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre vonatkozó irányelveket, valamint az EU hatályán kívül eső tevékenységek során végzett adatkezelést, továbbá a bűnüldözési célú adatkezelést, beleértve a közbiztonságot fenyegető veszélyek elleni védelmet és azok megelőzését.⁴⁸

A LED iránymutatásként szolgál az illetékes hatóságok számára a bűncselekmények megelőzése, kivizsgálása, felderítése, üldözése vonatkozásában, valamint a bűncselekmények, szankciók végrehajtását - ideértve a közbiztonságot fenyegető veszélyek elleni védelmet és megelőzést – szolgáló adatkezelésre. A bűnüldözési célból történő adatkezelések kifejezett kizárása a GDPR-ból jelzi a két jogi eszköztár eltérő célból történő adatkezelését.⁴⁹

A bűnügyi irányelv alkalmazásai tekintetében a jogharmonizációs kötelezettség a tagállami jogba való törvényi beépítést írta elő.⁵⁰

1. Az adatvédelem fogalmával kapcsolatos megfontolások⁵¹

Az adatok védelme jogi értelemben a természetes személyek, azaz az érintettek adatainak védelmét jelenti.⁵²

A személyes adatok védelme fogalmi- és jogi kategóriáinak értelmezéséhez szükséges az angol privacy fogalom meghatározása, részben történeti előzményként, részben pedig származtatott jogi kategóriaként, tekintettel arra, hogy a magyar „magánélet” fogalma nem fedti le ennek általános fogalmi keretét.

Mint jogi kategória a XIX. század végén jelent meg, az angolszász common law jogrendszerből ered. Warren és Brandeis nevezetes tanulmányához kötődik,⁵³ és a későbbi jogi értelmezések alapjául szolgált. Warren és Brandeis a fogalmat a magánjogi jogviszonyokban vizsgálták, a

⁴⁸ (EU) 2016/679, 2. cikk (2) (d).

⁴⁹ Gáti Balázs. (2022) "Az adatvédelmi szabályozás aktuális tendenciái a büntető igazságszolgáltatás területén." In *IV. PhD konferencia kötet*, szerkesztette Bendes Ákos László, Gáspár Zsolt, Gáti Balázs, Projics Nárcisz, Tóth Dávid, 44. Pécs: PTE-ÁJK, Doktori Iskola

⁵⁰ (EU) 2016/680, 62. cikk (1).

⁵¹ Gáti Balázs. (2022) "Az adatvédelmi jog fejlődésének főbb állomásai." *Studia Iurisprudentiae Doctorandorum Miskolciensium* 23, no.1, 153-168

⁵² Majtényi László: "Az információs jogok," In *Emberi jogok*, szerk. Halmai Gábor és Tóth Gábor Attila, Budapest: Osiris Kiadó, 2008, 579–581.

⁵³ Warren, Samuel and Brandeis, Louis. (1890) "The Right to Privacy," *Harvard Law Review*, IV, (5) 193–220, <https://www.jstor.org/stable/1321160?seq=27> (hozzáférés: 2022.06.25.)

jelen értelmezéshez képest szűkebb mértékben. Értelmezésük szerint a privacy jog arra, hogy „egyedül legyünk” („*right to be alone*”). Javaslatukban megfogalmazták a magánszférához való jog büntetőjogi védelmét is, ezzel is kifejezve annak önálló jogi létjogosultságát.⁵⁴

A XX. század során az amerikai és angolszász jogrendszerekben a fogalom és a kapcsolódó jogszabályi keretek számos fejlődésen és értelmezésen mentek keresztül.

A gyakran idézett Charles Fried a privacy lényegét tekintve azt a „*rólunk szóló tudás feletti ellenőrzés gyakorlásának lehetőségével*” azonosítja (*control over knowledge about oneself*)⁵⁵.

Ez a meghatározás közel áll a személyes adatok védelmének jogi fogalmához. Bár a kontinentális jog a magánszféra fogalomnál szűkebben értelmezi a személyes adatok védelmét, mégis magasabb szintű védelmet biztosít az egyén számára.⁵⁶

Jóri szerint „*Az adatvédelem a magánszféra-védelem sajátos jogi szabályozásban megnyilvánuló módja*”, és egyben célja is.⁵⁷ Bár részletesen elemzi a magánszféra fogalmát és kialakulását a „privacy” fogalmának alapul vételével, az adatvédelem fogalmának meghatározási nehézségeivel, és bizonytalanságaival kapcsolatban Mayer–Schönberger 1997-es véleményét veszi alapul.⁵⁸

A Jóri által megadott definíció olyan értelmezést ad, amely a fejlődést és a történeti kialakulást hordozza magában, ennek alapján jelenleg is aktuális. „*Az adatvédelem jellemzője (...) hogy a magánszféra védelmén belül értelmezhető az alábbiak szerint: a) az adatvédelem minden esetben a személy magánszférájának jogi védelmét jelenti, amely b) az 1970-es évektől az elektronikai forradalom által egyre általánosabbá váló automatizált adatfeldolgozás veszélyeire válaszul jelent meg Európában, és c) az általa nyújtott jogi védelem tartalma a*

⁵⁴ Ibid. p.219.

⁵⁵ Fried, Charles.(1968). "Privacy," *Yale Law Journal* 77 Idézi Szabó ,Máté Dániel.(2005) "Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival," *Információs Társadalom* (5), p.46.

⁵⁶ C-311/18.ítélet. Az Európai Unió Bírósága Schrems II. ügyben hozott ítélete. <http://curia.europa.eu/juris/document/document.jsf?jsessionid=79A9F6D4C441C1B0E1BB674FF3B58578?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=9719131> (hozzáférés: 2021.10.21.)

Az EU-USA közötti adattovábbítást lehetővé tevő megfelelőségi határozat (Privacy Shield) érvénytelensége jól példázza ezt..

⁵⁷ Jóri András. *Adatvédelmi kézikönyv*. Budapest: Osiris, 2005, p.26.

⁵⁸ Ibid. p.27.

fogalom megjelenése óta többször is jelentősen változott, illetőleg jelenleg is folyamatosan változásban van.”⁵⁹

A privacy magyar nyelvű értelmezései többnyire annak egy-egy aspektusát ragadják meg, Szabó Máté Dániel a magyar jogrendszer fogalmaival próbálta annak tartalmát visszaadni.⁶⁰ „Definíciónk szerint a privacy nem más, mint az egyén joga ahhoz, hogy magáról döntsön. A magyar jogirodalomban, alkotmánybírósági gyakorlatban és a jogrendszer más területein is ismert jogról van tehát szó, az önrendelkezés szabadságáról, arról, hogy mindenki maga döntheti el, mi lesz a saját sorsa, mit tesz magával, a testével és a rá vonatkozó ismeretekkel”⁶¹ Későbbiekben a privacy fogalmát, mint információs önrendelkezési jogot veti össze az adatvédelemmel, hivatkozva arra, hogy a magyar jog gyakran azonosítja a kettőt, „a személyes adatok védelméhez való jog nem más, mint az információs önrendelkezési jog.”⁶² Egyetértek azzal a véleményével, mely szerint a személyes adatok védelme több mint önrendelkezési jog, de gyakorlat számára az érintett természetes személyek önrendelkezési jogát, annak hangsúlyozását mind a szabályozás, mind az egyén szempontjából rendkívül fontosnak tartom.. Szőke Gergely László szerint az adatvédelem nem csak a jogi, de a más szabályozási eszközökkel nyújtott védelmet is felöleli.⁶³ Az adatvédelem fogalma leírható azokkal az alapelvekkel, nemzetközi szabályozásokkal is, amelyek a természetes személyeket hivatottak védeni azok önrendelkezési jogának szabályozása által. Ezt támasztja alá többek között Székely Iván definíciója, amely szerint az adatvédelmet „olyan alapelvek, szabályok, eljárások, adatkezelési eszközök és műveletek összességének tekintjük, amelyek az egyénre vonatkozó ismeretek feletti ellenőrzés lehetőségét biztosítják az egyén számára oly módon, hogy a személyes adatok gyűjtését, feldolgozását és felhasználását korlátozzák és ezáltal az egyént védik.”⁶⁴

⁵⁹Jóri András.(2009) "Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése." Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. Pécs, p.16.

⁶⁰ Szabó Máté Dániel.(2005) "Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival." *Információs Társadalom* (59, p.46.

⁶¹ Ibid.

⁶² Az Alkotmánybíróság 15/1991. (IV. 13.) AB-határozata. Ibid. 51.

⁶³ Szőke Gergely László. *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén.* Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., 2014, 118.

⁶⁴ Idézi: Szabó Máté Dániel „Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival.” p.52.

A személyes adatok védelme – véleményem szerint gyakorlati szempontból - nem más, mint a természetes személyek jogainak és szabadságainak védelme a természetes személyek személyes adataihoz fűződő önrendelkezési jog gyakorlási körülményeinek meghatározása által, valamint a természetes személyek személyes adatait kezelő adatkezelőkre vonatkozó adatkezelési feltételek szabályozása által.

2. Az adatvédelmi jog fejlődésének főbb állomásai⁶⁵

Az adatvédelem történeti áttekintése alapján megállapítható, hogy az informatikai szektorban végbement technológiai fejlődés fontos szerepet játszott az adatvédelmi jogszabályok kialakításában és evolúciójában.

A magyar jogirodalomban megjelent jelentős számú adatvédelmi történeti áttekintés alapján - kiemelve Sólyom⁶⁶, Majtényi⁶⁷, Jóri,⁶⁸ Szőke⁶⁹, Péterfalvi⁷⁰ kutatásait - az adatvédelmi szabályozás kezdetei az 1970-es évekre tehetőek.⁷¹

Az elektronikus adatkezelés lehetősége hozta magával az első adatvédelmi törvényt Európában a németországi Hessen népesség nyilvántartó adatbázis terve kapcsán.⁷² 1973 - és 1978 között ehhez hasonló módon Svédországban, Németországban, Norvégiában, Ausztriában és Franciaországban fogadtak el adatvédelmi tárgyú jogszabályokat.⁷³

Az 1980-ban elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló Nemzetközi Gazdasági és Együttműködési Szervezet- OECD – irányelvek egyik legnagyobb érdeme a személyes adatok gyűjtésére és kezelésére vonatkozó alapelvek

⁶⁵ Gáti Balázs. "Az adatvédelmi jog fejlődésének főbb állomásai."

⁶⁶ Sólyom László. "Az adatvédelem és információszabadság előtörténete Magyarországon." In *Az elektronikus információszabadság*, szerk. Majtényi László, 174-183. Budapest: Eötvös Károly Intézet (EKINT), 2004.

⁶⁷ Majtényi László. "Az információs jogok."

⁶⁸ Jóri András. *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.*

⁶⁹ Szőke Gergely László. "Az adatvédelem szabályozásának történeti áttekintése." *Infokommunikáció és Jog* 2013/3, 107–112.

⁷⁰ Péterfalvi Attila. (2020) "Az adatvédelem fejlődésének történeti áttekintése Magyarországon a GDPR hatálybalépéséig." In *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*, szerk. Péterfalvi Attila, 29–78. Budapest: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

⁷¹ Gáti Balázs. "Az adatvédelmi jog fejlődésének főbb állomásai."p. 156.

⁷² Simitis, Spiros. *The Hessian Data Protection Act*. Wiesbaden: The Hessian Data Protection Commissioner, 1987, Idézi: Szőke Gergely László. *Az adatvédelem szabályozásának történeti áttekintése*, p.109.

⁷³ *Ibid.*p.109

lefektetése.⁷⁴ Ilyen például a szándék megjelölés alapelve, amely az adatkezelés céljának meghatározását jelenti. E szerint a „*személyes adatok gyűjtésének szándékát legkésőbb az adatgyűjtéskor meg kell határozni és azok későbbi felhasználását csak ezen célokra, vagy azokkal nem összeegyeztethetetlen célokra kell korlátozni és amint ezek minden egyes szándékváltozás során meghatározásra kerülnek.*”⁷⁵ Az alapelvek a későbbi jogi szabályozás szempontjából irányadó jellegűek voltak, ideértve a korlátozott adatgyűjtés, az adatminőség, a felhasználási korlátozás, a biztonsági garancia, a nyitottság, az egyéni részvétel és a felelősségre vonhatóság alapelveit. Az irányelv alapvetően érintett alapú megközelítést képviselt.

Az első nemzetközi jogilag kötelező erejű dokumentum az adatvédelem területén az Európa Tanács 1981-es adatvédelmi egyezménye volt.⁷⁶ Az egyezmény fő célja az volt, hogy „*garantálja minden egyén számára jogainak és alapvető szabadságainak, különösen a magánélethez való jogának tiszteletben tartását a személyes adatainak gépi feldolgozása során.*”⁷⁷ Biztosítékokat állapított meg a személyes adatok gyűjtésével és feldolgozásával kapcsolatban, és megtiltotta az egyének faji, politikai, egészségi állapotára, vallási meggyőződésére, szexuális életére vagy büntetett előéletére vonatkozó „érzékeny” adatainak kezelését. Az Egyezmény lehetővé tette az érintettek számára, hogy tájékoztatást kapjanak arról, hogy személyes adataik kezelése milyen módon történik, továbbá biztosította az adatok helyesbítésének vagy törlésének jogát az érintettek számára, de nem tartalmazta a hozzájárulást, mint adatkezelési jogalapot. Az Egyezményben szereplő jogok csak abban az esetben voltak korlátozhatók, ha ez az intézkedés az állam biztonságához vagy más alapvető nemzeti érdekekhez kapcsolódott. Emellett bizonyos korlátozásokat írt elő a személyes adatok határokon átnyúló áramlására, különösen arra az esetre, ha a személyes adatok olyan országokba kerültek továbbításra, ahol a szabályozás nem biztosított egyenértékű védelmet.

Az Európai Parlament és az Európai Unió Tanácsa 1995-ben elfogadta az (EU) 95/46/EK adatvédelmi irányelvét, amely kimondta, hogy a tagállamok „*védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a*

⁷⁴ Gazdasági Együttműködési és Fejlesztési Szervezet. "Áttekintés az OECD Irányelvekről a magánélet védelméről és a személyes adatok határokon átvételéről." (hozzáférés 2021. szeptember 10.) <https://www.oecd.org/sti/ieconomy/15590228.pdf>.

⁷⁵ Ibid.p.4

⁷⁶ Treaty No. 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108).

⁷⁷ Ibid. 1.cikk.

személyes adatok feldolgozása során".⁷⁸ Ez az irányelv minden részes félre kötelező érvényű volt. Meghatározta az adatkezelő és az adatfeldolgozó fogalmát, és kiemelte az etikai szabályozás jelentőségét az egyes ágazatokban. Egy további jelentős előrelépés volt, hogy az irányelv előírta a tagállamok számára az előírások független felügyeleti hatóságok általi ellenőrzésének biztosítását.

2001 novemberében az Európa Tanács kiemelkedő mérföldkőként jelentette be az 1981-es adatvédelmi egyezmény Kiegészítő Jegyzőkönyvét, amely jelentősen kibővítette a felügyelő hatóságok szerepkörét és megszabta a személyes adatok nemzetközi áramlásának szabályait.⁷⁹ A Jegyzőkönyv különösen a határokon átívelő, harmadik országokba történő adatáramlás szabályozásában volt előremutató. Az előírások értelmében valamennyi tagállamnak felügyeleti hatóságokat kellett létrehoznia, amelyek felelősek voltak az egyezmény alapján kialakított, személyes adatok védelmére és a határokon átnyúló adatáramlásra vonatkozó jogszabályok és rendeletek betartásának ellenőrzéséért. A dokumentum továbbá kimondta, hogy személyes adatok továbbítása harmadik országokba vagy nemzetközi szervezetek részére csak abban az esetben engedélyezett, ha a fogadó fél garantálja a megfelelő adatvédelmi intézkedések meglétét.

A 45/2001/EK⁸⁰ az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, európai tanácsi és parlamenti rendelet nagy érdeme, hogy létrehozta az uniós intézmények és szervek adatkezelési műveleteit felügyelő Európai Adatvédelmi Biztos intézményét, amely napjainkban is meghatározó szerepet tölt be az uniós adatvédelmi jogszabályok kidolgozásában és alkalmazásában.⁸¹

Az adatvédelem jogi szabályozása a Big Data korszakában újabb kihívások elé érkezett.⁸² A mesterséges intelligencia, a robotika és az úgynevezett negyedik ipari forradalom által

⁷⁸ Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. *Hivatalos Lap* L 281 1995. pp.31–50.

⁷⁹ Council of Europe, Treaty No. 181, Kiegészítő jegyzőkönyv az egyének védelméről a személyes adatok automatikus feldolgozása során, a felügyeleti hatóságokról és a határokon átnyúló adatáramlásról.

⁸⁰ Az Európai Parlament és a Tanács 45/2001/EK rendelete a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról. *Hivatalos Lap* L 8 2001. pp.1–22.

⁸¹ Gáti Balázs. "Az adatvédelmi jog fejlődésének főbb állomásai.", p.158.

⁸² Szőke Gergely László. "Big Data and Algorithms in the Public Sector and Their Impact on the Transparency of Decision-Making." In *Central and Eastern European eDem and eGov Days 2018: Conference proceedings*, szerk. Hansen Hendrik, Müller-Török Robert, Nemeslaki András, Prosser Alexander, Scola Dona, és Szádeczky Tamás, 301–311. Wien, Ausztria: Facultas Verlag, 2018.

előidézett változásokra a jogalkotásnak is meg kellett felelni. Szükségessé vált egy adatvédelmi reform, teret engedve az innovációnak, egyúttal biztosítani a személyes adatok védelmét.

3. Az Európai Unió jelenlegi szabályozása – A személyes adatok védelmének általános jogszabályi háttere és intézményei

3.1. Az adatvédelmi reform

Az adatvédelmi reformot megelőző alapokmányok, az európai uniós szerződések, és kerethatározatok alapvetően meghatározták a fejlődés irányát és jogi feltételeit.

1948-ban fogadták el az Emberi Jogok Egyetemes Nyilatkozatát mely először tesz említést a személyes adatok védelméről, a fogalom tágabb értelmében.⁸³ Két évvel később került elfogadásra az Emberi Jogok Európai Egyezménye (EJEE), amely kimondta a magán- és családi élet tiszteletben tartásához való jogot. „*Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.*”⁸⁴

Az Unió szervei erre reagáltak az Alapjogi Charta kihirdetésével,⁸⁵ ami kötelező erőt csak a Lisszaboni Szerződés 2009. december 1 - i hatályba lépésével nyert.⁸⁶ A Charta 7. és 8. cikkében a magánélet tiszteletben tartása és a személyes adatok védelme egymással szorosan összefüggő, de különálló alapvető jogként nyert elismerést.⁸⁷

A Lisszaboni Szerződéssel módosított Európai Unió Működéséről szóló Szerződés (továbbiakban EUSZ) 16. cikk (2) bekezdése 2008-ban új, önálló jogalapot teremtett az adatvédelmi szabályok elfogadására, az EUSZ felhatalmazta az Európai Parlamentet és Tanácsot, hogy rendes jogalkotási eljárás keretében megalkossa a személyes adatok feldolgozása tekintetében történő védelmére, valamint az ilyen adatok szabad áramlására

⁸³ Emberi jogok egyetemes nyilatkozata, 12. cikk

⁸⁴ Emberi Jogok Európai Egyezménye, 8. cikk

⁸⁵ Az Európai Unió Alapjogi Chartája, 2012/C 326/02.

⁸⁶ Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról, 2007/C 306/01.

⁸⁷ Nagy, Klára. (2010) "Adatvédelem a rendőrségi és bűnügyi együttműködés során a Lisszaboni Szerződés után." In *Tanulmányok "Quo vadis rendvédelem? Szabadságjogok, társadalmi kötelezettségek és a biztonság" című tudományos konferenciáról*, szerkesztette Gaál, Gyula és Hautzinger, Zoltán, 81-88. Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport

vonatkozó szabályokat.⁸⁸ Az Európai Tanács 2009 decemberében a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség vonatkozásában többéves programot hagyott jóvá a 2010–2014-es időszakra. 2014 júniusában az Európai Tanács következtetései meghatározták az elkövetkezendő évekre vonatkozó jogalkotási és operatív programok tervezésére szolgáló stratégiai iránymutatásokat, az EUSZ 68. cikke értelmében. A fő célkitűzések között kiemelendő az Unión belüli személyes adatok hatékonyabb védelmének biztosítása.⁸⁹

A személyes adatok védelméhez való alapvető jogot garantáló uniós keret három pillére közül a GDPR alapelvei a személyes adatok kezelését illetően a jogszerűség, tisztességes eljárás és átláthatóság, a célhoz kötöttség, az adattakarékosság, a pontosság, a korlátozott tárolhatóság, az integritás és bizalmas jelleg, valamint az elszámoltathatóság. A GDPR egyik jelentős újításának tekinthető a korábbi szabályozáshoz képest, hogy a rendelet hatálya az Európai Unió területén kívüli adatkezelésekre is vonatkozik, azokban az esetekben ha az adatkezelőnek a tevékenységi helye az Unióban van, vagy ha az adatkezelés érintette az Unióban tartózkodik. A rendelet az alapfogalmakat és alapelveket nagyrészt az előző 95/46 EK irányelvre alapozta, azonban új elemként bevezette az adatbiztonság követelményét, mint külön alapelvet (integritás és bizalmas jelleg elve), valamint az elszámoltathatóság elvét, amely szerint az adatkezelőnek szükség esetén képesnek kell lennie igazolni, hogy tevékenysége megfelel a jogszabályi előírásoknak.

A GDPR és a LED elfogadását követően is jelentős szerepe van az azt kiegészítő felhatalmazási és végrehajtási aktusoknak.⁹⁰

Az EUDPR kiterjesztette a szabályozást a bünyügyi adatok uniós szervek és hivatalok bünyügyi adatokkal kapcsolatos tevékenységére, az EUSZ harmadik része V. címe 4. vagy 5. fejezetének

⁸⁸ Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata, 2012/C 326/01. *Hivatalos Lap C* 326 2012, pp. 47–390.

⁸⁹ Európai Parlament. "A személyes adatok védelme." (hozzáférés: 2022. június 21) https://www.europarl.europa.eu/ftu/pdf/hu/FTU_4.2.8.pdf

⁹⁰ Bendik Tamás. "A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása." In *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*, szerk. Péterfalvi Attila, 79-109. Budapest, Magyarország: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), 2020. 90.

Ilyenek „, többek között az adatkezelő és az adatfeldolgozó közötti általános szerződési feltételeket, a harmadik országok és nemzetközi szervezetek részére történő adattovábbítások jogszerűsége feltételeit megállapító, illetve a magatartási kódexeket, a tanúsítást érintő, az Európai Bizottság által megalkotott előírásoknak [pl. GDPR 28. cikk (7) bekezdés, 40. cikk (9) bekezdés, 43. cikk (8)-(9) bekezdés, 45. cikk (3) és (5) bekezdés, 46. cikk (2) bekezdés c)-d) pont, 92. cikk, illetve bünyügyi irányelv 36. cikk (3) és (5) bekezdés, 50. cikk (8) bekezdés]”

hatálya alá tartozó tevékenységek végzése során,⁹¹ függetlenül attól hogy, „*e tevékenységeket fő vagy kiegészítő feladataik körében végzik-e bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása érdekében.*”⁹² Felhívja továbbá a figyelmet, hogy a Bizottságnak mindent meg kell tennie a jogalkotási javaslat tekintetében, hogy a személyes adatok kezelésével kapcsolatos szabályozás az Europolra és az Európai Ügyészségre is alkalmazható legyen.^{93,94}

Az e-Privacy javaslat célja az elektronikus hírközlési szektor adatkezelési tevékenységének a GDPR kompatibilis újra szabályozása rendeleti formában.⁹⁵ A tervezet szerint az e-Privacy rendelet kiterjedne az ún. OTT - over the top services -, szolgáltatásokra, mint a Skype, Facebook Messenger, Gmail, iMessage vagy a Whatsapp és az Internet of Things – a dolgok internetére is. A rendelet - az általános adatvédelmi rendelethez hasonlóan - az Unión kívül letelepedett elektronikus hírközlési szolgáltatókra is kiterjed, amennyiben az Unió területén elektronikus hírközlési szolgáltatásokat nyújtanak a végfelhasználók számára. Az Unión kívüli szolgáltatóknak írásban kell képviselőt kijelölniük. A rendeletet nem csak a természetes személy végfelhasználókra, hanem a jogi személyekre is alkalmazni kellene.

Az Európa Tanács 2018. májusában elfogadta, Európa Tanács 108. sz. egyezményének kiegészítő jegyzőkönyvét.⁹⁶ A személyes adatok automatikus feldolgozása tekintetében az egyének védelméről szóló egyezmény, az egyetlen létező, jogilag kötelező erejű nemzetközi egyezmény, amely ezen a területen globális jelentőséggel bír. Foglalkozik az új információs és kommunikációs technológiák használatából adódó, a magánélet védelmével kapcsolatos kihívásokkal, a nemzetbiztonsági adatkezelésekre is alkalmazandó és kiterjeszti alkalmazását olyan területekre is, amelyek nem tartoznak az EU joghatósága alá. Ugyanakkor elegendő mozgásteret hagy a feleknek a rendelkezéseik nemzeti jogban történő végrehajtása tekintetében.

⁹¹ Az EUSZ harmadik rész V. cím. 4. (Igazságügyi együttműködés büntetőügyekben) és 5. (Rendőrségi együttműködés) fejezetei.

⁹² (EU) 2018/1725 Rendelet, 12. bekezdés szerint „(...) azonban az Europolra és az Európai Ügyészségre addig nem alkalmazandó, amíg nem kerül sor az Europol és az Európai Ügyészséget létrehozó jogi aktusok arra irányuló módosítására, hogy ennek a rendeletnek a műveleti vonatkozású személyes adatok kezeléséről szóló fejezete, kiigazított formájában rájuk is alkalmazandó legyen.”

⁹³(EU) 2018/1725, (12)

⁹⁴ Gáti Balázs: "Az adatvédelmi jog fejlődésének főbb állomásai." p.164.

⁹⁵ COM (2017) 10 final.

⁹⁶ Javaslat a TANÁCS HATÁROZATA az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményét (108. sz. egyezmény) módosító jegyzőkönyvnek az Európai Unió érdekében történő megerősítésére a tagállamoknak adott felhatalmazásról, COM(2018) 451 final

Így a kiegészítés lehetővé teszi az egyezményhez való csatlakozást azon – akár Európán kívüli – országok számára is, amelyek az adatvédelmi szabályozásuk megújítását tervezik.

3.2. Az Európai Adatvédelmi Biztos és az Európai Adatvédelmi Testület és az Európai Bíróság szerepe

Az adatvédelmi reform uniós jogszabályainak egységes alkalmazása tekintetében a nemzeti szabályok különbözőségeit is figyelembe véve, jelentős szerepet töltenek be az Európai Adatvédelmi Testület, (EDPB)⁹⁷ és az Európai Adatvédelmi Biztos (EDPS) intézményei jogalkalmazó-jogértelmező tevékenységük folytán. Az egységes jogalkalmazás másik alapját továbbra is az Európai Unió Bírósága (továbbiakban EUB) ítéletei alkotják.

3.2.1. Az Európai Adatvédelmi Testület (EDPB)

Az EDPB az Európai Unió adatvédelmi hatóságainak független testülete. Az EDPB feladata, hogy elősegítse az adatvédelmi jogszabályok egységes értelmezését és alkalmazását az EU-tagállamokban. Feladata többek között iránymutatások, állásfoglalások, véleményezések készítése a GDPR és az a LED megfelelést illetően az uniós jogszabályokkal tervezetekkel kapcsolatosan, a tagállami állásfoglalások véleményezése, a tudományos kutatás, a technológiai fejlődések általi iránymutatások felülvizsgálata. A tagállamok adatvédelmi hatóságaival együttműködve többek között koordinálja a határokon átnyúló adatvédelmi ügyeket.⁹⁸

A GDPR rendelkezett az Európai Adatvédelmi Testület létrehozásáról, egyúttal rendelkezett a Testület feladatairól, az elnökről és az elnökhelyettesekről, valamint a titkárságról.⁹⁹

Az (EU) 2016/680 irányelve további feladatokat határozott meg a Testület, az elnök és az elnökhelyettesek, valamint a titkárság számára.¹⁰⁰

⁹⁷ Jogelődje a 29. cikk szerinti Adatvédelmi Munkacsoport (European Union Agency for Fundamental Rights FRA 2018, 199.)

⁹⁸ Európai Adatvédelmi Testület. "Eljárási Szabályzat, 8. változat." Elfogadva: 2018. május 25.

Legutóbb módosítva és elfogadva: 2022. április 6.

Preambulum.https://edpb.europa.eu/system/files/202208/edpb_rules_of_procedure_version_8_adopted_20220406_hu.pdf.

⁹⁹ „(EU) 2016/6799” 68. cikk (1)-(2).

¹⁰⁰ „(EU) 2016/680” , 51. cikk.

Az Európai Adatvédelmi Testület a GDPR 51. cikke értelmében a következő főbb feladatokat látja el:

- Tanácsadás a Bizottságnak a személyes adatok védelmére vonatkozó uniós jogszabályokkal kapcsolatosan, beleértve az irányelv módosításait is.
- Az irányelv alkalmazásával kapcsolatos kérdések elemzése és az egységes alkalmazás elősegítése céljából iránymutatások, ajánlások és legjobb gyakorlatok kidolgozása.¹⁰¹
- Felügyeleti hatóságok számára iránymutatások készítése különösen az adatvédelmi incidensek kezelésével és az érintetti jogok érvényesítésével kapcsolatban.
- Harmadik országok adatvédelmi szintjének értékelése a Bizottság számára, döntéstámogatás az adatáramlás biztonságos kereteinek megállapításában.
- Az adatvédelmi gyakorlatok egységes alkalmazását és a felügyeleti hatóságok közötti együttműködést elősegítő tevékenységek támogatása

A 2018/1725 rendelet is meghatároz szabályokat a Testület számára.¹⁰² Az uniós jog egyéb rendelkezései is további feladatokat róhatnak a Testületre. Az általános adatvédelmi rendeletet belefoglalták az EGT-megállapodásba, amely előírja, hogy az Európai Gazdasági Térség (továbbiakban EGT) tag EFTA-államok¹⁰³ felügyeleti hatóságainak és az EFTA Felügyeleti Hatóságnak részt kell venniük a Testület tevékenységeiben, amelyet az EDPB Eljárási Szabályzata is előír. Bár szavazati joguk nincs, az EGT-tag EFTA-államok felügyeleti hatóságainak jogukban áll kifejtetni álláspontjukat minden megvitatott kérdésben vagy szavazásra terjesztett témában.¹⁰⁴ Az Európai Bizottság nem tagja a Testületnek, de annak ülésein, tevékenységeiben és értekezletein részt vehet, szavazati joggal nem rendelkezik.¹⁰⁵

¹⁰¹ „(EU) 2016/6799” 12.cikk.1.” Az általános adatvédelmi rendelet 70. cikke (1) bekezdésének d), e), f), g), h), i), j), k), m), p), q), r), s) és x) pontjaiban és a rendőri és büntető igazságszolgáltatási adatvédelmi irányelv 51. cikkében foglalt esetekben”

¹⁰² „(EU) 2018/1725 „, 42.cikk, 52- 57. cikk

¹⁰³ Az EFTA (European Free Trade Association) vagyis az Európai Szabadkereskedelmi Társulás egy regionális kereskedelmi szervezet és szabadkereskedelmi övezet, amely néhány európai országot tömörít. Az EFTA nem része az Európai Uniónak, de tagjai szoros gazdasági és kereskedelmi kapcsolatokat ápolnak az EU-val, különösen az EGT megállapodás révén, amely lehetővé teszi az EFTA néhány tagjának, hogy részt vegyen az EU egységes piacán.

¹⁰⁴ EUDPR. 3. cikk

¹⁰⁵ A Bizottságnak kiemelkedő szerepe van a rendelet működésének és hatékonyságának felülvizsgálatában. A GDPR 97. cikke szerint a Bizottság 2020. május 25-ig és minden azt követő negyedik évben jelentést terjeszt az Európai Parlament és a Tanács elé a rendelet értékeléséről és felülvizsgálatáról.

A GDPR 69. cikkében rögzített függetlenségi elv szerint a Testület pártatlanul és teljes függetlenséggel jár el feladatainak elvégzésében és jogköreinek gyakorlásában. A Testület az egyes tagállamok és az EGT-tag EFTA-államok részéről egy felügyeleti hatóság vezetőjéből vagy az általános adatvédelmi rendelet szerinti közös képviselőből és az európai adatvédelmi biztosból vagy ezek megfelelő képviselőiből áll.¹⁰⁶

Az EDPB adatvédelmi reformmal kapcsolatos legfontosabb iránymutatásai a következők:

Iránymutatás az adathordozhatósághoz való jogról¹⁰⁷, Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához¹⁰⁸, Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról¹⁰⁹, 5/2019 iránymutatás az elfeledtetéshez való jog kritériumairól az általános adatvédelmi rendelet hatálya alá eső, keresőmotorokkal kapcsolatos ügyekben¹¹⁰, 10/2020 sz. iránymutatás az általános adatvédelmi rendelet 23. cikke szerinti korlátozásokról,¹¹¹ 01/2022. sz. iránymutatás az érintettek jogairól – hozzáférési jog.¹¹²

Az Európai Adatvédelmi Testület továbbá iránymutatás-tervezetet nyújtott be a Schrems II utáni adattovábbítási mechanizmusokról a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében az adattovábbítási eszközöket kiegészítő intézkedésekről szóló 01/2020. sz. ajánlásában.¹¹³ Ez az ajánlás tartalmazza a harmadik országokba történő adattovábbításra alkalmazandó kiegészítő intézkedések listáját, úgymint technikai intézkedések, pl. erős titkosítás, szerződéses intézkedések, beleértve egy olyan új szerződéses rendelkezés végrehajtását, amely arra kötelezi az átadó és fogadó feleket, hogy jogorvoslati

¹⁰⁶ GDPR . 68. cikkének (4), és 4. cikk (1).

¹⁰⁷ 16/HU WP 242 rev.01, https://www.adatvedelmirendelet.hu/wp-content/uploads/wp242rev01_hu.pdf

¹⁰⁸ 17/HU WP251rev.01, https://www.naih.hu/files/wp251rev01_hu.pdf

¹⁰⁹ 17/HU WP260 rev.01, https://www.naih.hu/files/wp260rev01_hu.pdf

¹¹⁰ EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_hu

¹¹¹EDPB,https://www.edpb.europa.eu/system/files/202307/edpb_guidelines_202010_art23_adopted_afterpublicconsultation_hu.pdf

¹¹²EDPB,https://www.edpb.europa.eu/system/files/202404/edpb_guidelines_202201_data_subject_rights_access_v2_hu.pdf

¹¹³EDPB,https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_hu

mechanizmusok révén segítsék az érintetteket jogaik harmadik országban történő gyakorlásában.¹¹⁴

3.2.2. Európai Adatvédelmi Biztos (EDPS)

Az EDPS az Európai Unió intézményeinek és szerveinek független adatvédelmi tisztviselője. Az (EU) 2018/725 rendelet VI. fejezete rendelkezik az európai adatvédelmi biztosról.¹¹⁵ Az EDPS felügyeli az EU intézmények által végzett adatkezelést, és biztosítja az adatvédelmi jogszabályok betartását. Az EDPS véleményeket ad ki, javaslatokat tesz az adatvédelmi szabályzatok és gyakorlat fejlesztésére, valamint tájékoztatást nyújt az uniós polgároknak az adatvédelemmel kapcsolatos kérdésekben.

Az EDPS a közérdeket szem előtt tartva szakértőként, valamint a magánélet és az adatvédelem területén működő független, proaktív és hiteles szervként jár el.¹¹⁶ Feladatköre széleskörű, ideértve a panaszok felülvizsgálatát és bírósági jogorvoslatokat,¹¹⁷ a jogalkotási konzultációt, technológia monitoringot, kutatási projekteket, és a bírósági eljárásokba való beavatkozás lehetőségét az Unió Bírósága elé terjesztett ügyekben.¹¹⁸ Feladat továbbá az együttműködés a nemzeti felügyeleti hatóságokkal és a nemzetközi együttműködés.¹¹⁹

Jogalkotási konzultációt végez, a Bizottság kérésére az EDPS a GDPR 42. cikkének (1) bekezdése alapján véleményeket vagy hivatalos észrevételeket ad ki. Az EDPS megtagadhatja a válaszadást a konzultációra, ha a rendelet 42. cikkében meghatározott feltételek nem teljesülnek, beleértve azokat a helyzeteket is, amikor az adatvédelmi intézkedések nem gyakorolnak közvetlen hatást az egyének jogaira és szabadságaira. Amennyiben az EDPS és az

¹¹⁴ Gáti, Balázs.(2022) "A Schrems II ítélet lehetséges hatásai a nemzetközi jogalkotásra." In *Az internet és a közösségi média jogi kihívásai – Konferenciakötet*, szerkesztette Tóth, Dávid, 18-35. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

¹¹⁵ (EU)2018/1725, 52.- 60 cikk, és 61.- 69.cikk

¹¹⁶Az Európai Adatvédelmi Biztos Határozata (2020. május 15.) az európai adatvédelmi biztos eljárási szabályzatának elfogadásáról, II. fejezet, 3.cikk (1). https://edps.europa.eu/sites/default/files/publication/20-06-26_edps_rules_of_procedure_hu.pdf

¹¹⁷ Ibid. 18. cikk

¹¹⁸ Ibid. III.cím

¹¹⁹ Ibid. IV.cím

EDPB a rendelet 42. cikkének (2) bekezdése szerinti közös véleményét nem tudják kiadni a meghatározott határidőn belül, az EDPS önállóan véleményt adhat ki ugyanebben az ügyben.¹²⁰ Az EDPS korrekciós jogkört vehet igénybe, figyelmeztetheti az EU azon intézményét, amely jogellenesen vagy tisztességtelenül dolgozza fel a személyes adatokat, kötelezi az intézményt, hogy tegyen eleget az érintett jogainak gyakorlására irányuló kéréseknek (pl. hozzáférés a saját adataihoz), ideiglenes vagy végleges tilalmat rendelhet el egy adott adatkezelési műveletre, közigazgatási bírságot szabhat ki az uniós intézményekre, az ügyet az Európai Unió Bírósága elé utalhatja. Az EUDPR 58. cikke az európai adatvédelmi biztost széleskörű hatáskörrel bízta meg, ezenkívül Europol-rendelet¹²¹, az EPPO rendelet¹²² és az Eurojust-rendelet¹²³ is adatvédelmi hatásköröket ruháztak az európai adatvédelmi biztosra.

3.2.3 Bűnüldözésű célú releváns irányelvek az EDPB és EDPS gyakorlatában

A bűnügyi irányelv következetes alkalmazása kulcsfontosságú a büntetőügyekben folytatott hatékony igazságügyi együttműködés és a rendőrségi együttműködés biztosításához¹²⁴ Az EDPB-nek az általános adatvédelmi rendeletről szóló több iránymutatása a bűnüldözési célú adatvédelemről szóló irányelv szempontjából is releváns. Ezek közé tartozik az adatkezelő és az adatfeldolgozó fogalmáról¹²⁵ az érintettek jogairól,¹²⁶ az adatvédelmi incidensről

¹²⁰ Ibid. 20.cikk.(1),(2),(3),(4)

¹²¹ Az Európai Parlament és a Tanács (EU) 2016/794 rendelete a Bűnüldözési Együttműködés Európai Uniósi Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről. *Hivatalos Lap* L 135, 2016. pp.53—114.

¹²² Az Európai Parlament és a Tanács (EU) 2018/1727 rendelete az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről. *Hivatalos Lap* L 295, 2018. pp. 138—183.

¹²³ (EU) 2018/1727 Rendelet az Európai Unió ügynökségeként működő Eurojustról, lásd még : 01/2020 EDPB ajánlás, 24.,31.,39. oldalak

¹²⁴ (EU) 2016/680 , Preambulum (7)

¹²⁵ EDPB Guideline 07/2020 on the concepts of data controller and processor in the GDPR, adopted on 7 July 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf .

¹²⁶ EDPB Guideline 01/2022 on data subject rights - right of access, adopted on 18 January 2022, version for public consultation, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

értésítésről,¹²⁷ az adatvédelmi hatásvizsgálatról,¹²⁸ beépített és az alapértelmezett adatvédelemről¹²⁹ és az egyedi automatizált döntéshozatalról szóló iránymutatások.¹³⁰

Az EDPB iránymutatásokat fogalmazott meg a bűnügyi adatvédelmi irányelvvel kapcsolatosan is. Ezek közül az irányelv V. fejezetével kapcsolatos - nemzetközi adattovábbítások - szempontjából specifikus iránymutatást¹³¹, az arcfelismerő technológiák használatára vonatkozó iránymutatást¹³² részletesebben ismertetem.

- A bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti megfelelőségi referenciáról szóló ajánlás:

Az irányelv szabályokat állapít meg a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítására, az irányelv V. fejezete és a 35-39. cikkei alapján. Személyes adatokat csak akkor lehet harmadik országba vagy nemzetközi szervezet részére továbbítani, ha a megfelelő védelmi szintet biztosítanak, azaz megfelelnek az uniós szabályoknak. A Bizottság szerint ez az elv a LED 35. cikkével összhangban értelmezendő, amely megállapítja, hogy az irányelv valamennyi rendelkezését alkalmazniuk kell annak érdekében, hogy a természetes személyek számára biztosított védelmi szint ne sérüljön. Személyes adatokat harmadik országba, területre, ágazatba vagy nemzetközi szervezetbe engedély nélkül lehet továbbítani, ha a Bizottság nyilatkozott a megfelelőségről. A harmadik ország védelmi szintjének lényegében egyenértékűnek kell lennie az EU-ban garantált védelmi szinttel, azonban a

¹²⁷ Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01), <https://ec.europa.eu/newsroom/article29/items/612052>

01/2021. számú iránymutatás Az adatvédelmi incidensek bejelentésével kapcsolatos példákra, https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adapted_hu.pdf

¹²⁸ Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), <https://ec.europa.eu/newsroom/article29/items/611236/en>

¹²⁹ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

¹³⁰ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), <https://ec.europa.eu/newsroom/article29/items/612053/en>

¹³¹ 01/2021 ajánlás a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti megfelelőségi referenciáról https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf

¹³² Az Európai Adatvédelmi Testület 2022. május 12-én elfogadott, az arcfelismerő technológiának a bűnüldözés területén történő használatáról szóló, 05/2022. számú iránymutatása, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frlawenforcement_en_1.pdf

harmadik ország által e célból igénybe vett eszközök eltérhetnek az Európai Unióban alkalmazottaktól. A megfeleléségi normának nem kell pontról pontra tükröznie az uniós jogszabályokat, hanem az említett jogszabályok alapvető követelményeit kell megállapítaniuk.¹³³ A Bizottságnak a megfeleléségi határozatában minden releváns megállapítást tartalmaznia kell arra vonatkozóan, hogy a harmadik országban működő szabályozás korlátozza-e azon személyek alapvető jogainak gyakorlását, akiknek személyes adatait az Unióból az adott harmadik ország területére továbbítják. Ez magában foglalja azokat az eseteket is, amikor a harmadik ország közhatalmi szervei jogosultak beavatkozni az egyének alapvető jogainak gyakorlásába, amennyiben e beavatkozás jogos célokat, például a nemzetbiztonság védelmét szolgálja.^{134,135}

Az adatvédelmi szabályok azonban csak akkor hatékonyak, ha végrehajthatók és a gyakorlatban is betartják őket. Ezért az EDPB szerint nem csak a harmadik országba vagy nemzetközi szervezetekhez történő adatátvitelre vonatkozó szabályok tartalmát kell megvizsgálni, hanem az ilyen szabályok hatékonyságát biztosító rendszert is.

Az értékelés során az érintett harmadik országok törvényeinek teljes körű értékelésére van szükség a LED 36. cikkében meghatározott kritériumok alapján. Figyelembe kell venni az adott ország vagy szervezet jogállamiságát, az emberi jogok és alapvető szabadságok tiszteletben tartását, a vonatkozó jogszabályokat, az érintett jogait és jogorvoslati lehetőségeit, valamint a független felügyeleti hatóságok meglétét és hatékony működését. A Bizottság feladata a szabályok gyakorlati hatékonyságának rendszeres ellenőrzése.

¹³³ Schrems I ügy, 72–74. pont és a Bíróság 2017. július 26-i 1/15. sz. véleménye a Kanada és az Európai Unió közötti megállapodás tervezetéről, ECLI:EU:C:2017:592 (1/15. sz. vélemény), 134. pont: „A személyes adatok védelméhez való e jog megköveteli többek között, hogy a személyes adatoknak az Unióból valamely harmadik országba történő továbbítása esetén érvényesüljön az alapvető szabadságok és jogok tekintetében az uniós jog által biztosított magas szintű védelem folytonossága. Még ha az ilyen szintű védelem biztosítására irányuló eszközök különbözhetnek is azoktól, amelyeket az uniós jogból eredő követelmények tiszteletben tartásának biztosítása érdekében az Unión belül kialakítottak, ezen eszközöknek a gyakorlatban akkor is hatékonyak kell lenniük ahhoz, hogy az Unióban biztosított védelemmel lényegében egyenértékű védelmet biztosítsanak”.

¹³⁴ Schrems I. ügy, 52. pont

¹³⁵ (EU) 2016/680, 47. cikk (5) és Preambulum (82)

- Az arcfelismerő technológia (FRT)¹³⁶ használatának iránymutatása a bűnüldözés területén a kritikus jogi kereteket és a technológia alapvető jellemzőit hivatott tisztázni. Az olyan technológiák alkalmazása, amelyek lehetővé teszik az egyének azonosítását vagy hitelesítését viselkedésük alapján különböző médiumokon keresztül, mint például zárt láncú televíziós rendszerek (CCTV)¹³⁷ felvételei vagy fényképek, egyre inkább gyakorlattá válnak bűnüldözés területén is. Ez a technológia alkalmas többek között a körözési listákban szereplő személyek azonosítására vagy egyének közterületeken történő mozgásának nyomon követésére. Az FRT alkalmazása biometrikus adatok kezelésén alapul, ami a személyes adatok különleges kategóriáinak feldolgozását jelenti, és mesterséges intelligencia (AI) vagy gépi tanulás (ML¹³⁸) algoritmusokra épül. Bár az FRT nagy adatmennyiségek feldolgozására ad lehetőséget, magában hordozza a diszkrimináció és az esetleges téves azonosítások kockázatát is. Az FRT alkalmazható kontrollált egy-az-egyhez¹³⁹ helyzetekben, de alkalmas nagy tömegek és fontos

¹³⁶ Gáti, Balázs. (2022)"A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései." In *FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI: KONFERENCIAKÖTET – VÁLOGATOTT TANULMÁNYOK*, szerkesztette Bujtár, Zsolt; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond; Ferencz, Barnabás; Ázsoth, Szilvia; Szívós, Alexander Roland; Martin, Márton, 59-78. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar.

FRT (Facial Recognition Technology).Az FRT számos adatvédelmi és etikai kérdést vet fel , különösen a személyes adatok gyűjtése, tárolása és feldolgozása terén, valamint abban, hogy miként biztosítható a jogosulatlan hozzáférés elleni védelem és az egyének magánéletének tiszteletben tartása.

¹³⁷ A CCTV (Closed-Circuit Television) egy zárt televíziós rendszer, amelyet elsősorban megfigyelési és biztonsági célokra használnak. A CCTV rendszereket olyan helyeken telepítik, ahol szükség van a terület vagy az ott tartózkodó emberek folyamatos megfigyelésére, például bankokban, bevásárlóközpontokban, közterületeken, iskolákban, és egyéb létesítményekben. A rendszer kamerákból, monitorokból és rögzítő eszközökből áll, amelyek lehetővé teszik a vizuális felvételek élő közvetítését vagy későbbi visszanezését.

¹³⁸ Az ML, vagyis a gépi tanulás (Machine Learning) egy olyan mesterséges intelligencia (AI) alapú gépi tanulás, ahol az algoritmusok elemzik az adatokat, tanulnak belőlük, és képesek önálló döntéseket hozni vagy előrejelzéseket készíteni az adott adathalmaz alapján.

¹³⁹ Az ellenőrzött 1:1 helyzetek olyan specifikus alkalmazási területeket jelentenek, ahol az arcfelismerő rendszert egyetlen személy azonosítására vagy ellenőrzésére használják. Ebben a kontextusban az FRT célja az, hogy egy adott személy arcát összevethesse egy előre meghatározott, ellenőrzött adatbázisban szereplő arcképpel, annak érdekében, hogy igazolja az illető személyazonosságát. Ez a fajta alkalmazás gyakori például biztonsági ellenőrzéseknél, ahol az arcfelismerő rendszert azonosító dokumentumok – útlevél, személyi igazolvány – ellenőrzése során használják a hatóságok, vagy beléptető rendszereknél, ahol a hozzáférés engedélyezéséhez szükséges a személy azonosítása.

közlekedési csomópontok megfigyelésére is, így szükségszerűen jogi és etikai szempontok szigorú mérlegelését igényli.

A személyes adatok bűnüldözési kontextusban történő védelme érdekében meg kell felelnie a LED követelményeinek,¹⁴⁰ de alkalmazása azonban számos más alapvető jogot is érinthet, úgy mint a Charta 8. cikkében foglalt személyes adatok védelméhez való jogot, és a Charta 7. cikkében foglalt magánélethez való jogot.¹⁴¹ A különleges adatkategóriák, például a biometrikus adatok feldolgozása csak akkor tekinthető *"feltétlenül szükségesnek"* a LED 10. cikke értelmében, ha a személyes adatok kezelése és annak korlátozása erre korlátozódik, és kizár minden általános vagy rendszerszintű feldolgozást.¹⁴² A LED 11. cikke az automatizált egyedi döntéshozatal kereteit határozza meg. Az uniós joggal és a LED 11. cikkének (3) bekezdésével összhangban minden esetben tilos az olyan profilalkotás, amely a személyes adatok különleges kategóriái alapján természetes személyekkel szembeni megkülönböztetést eredményezne. Az adatminimalizálás elve - a LED 4. cikke (1) bekezdésének e) pontja - azt is megköveteli, hogy az adatfeldolgozás célja szempontjából nem releváns videoanyagot a felhasználás előtt mindig el kell távolítani vagy anonimizálni kell (pl. az adatok visszamenőlegesen visszaállíthatatlan elmosásával).

Az adatkezelőknek gondosan meg kell fontolniuk, hogy hogyan tudnak megfelelni az érintettek jogaira vonatkozó követelményeknek, mielőtt elkezdenek bármilyen arcfelismerő technológiával kapcsolatos adatkezelést végezni. Az érintettek jogainak hatékony gyakorlása attól függ, hogy az adatkezelő teljesíti-e a tájékoztatási kötelezettségeit. Az érintettek hatékony joggyakorlása érdekében az adatkezelőnek tájékoztatnia kell őket az automatizált döntéshozatal jellemzőiről, amennyiben csak az

¹⁴⁰ Az FRT használatára vonatkozóan a LED bizonyos keretet biztosít, különösen a LED 3. cikkének (13) bekezdése a "biometrikus adatok", a 4. cikke a személyes adatok feldolgozására vonatkozó elvek, a 8. cikke a feldolgozás jogszerűsége, a 10. cikke a személyes adatok különleges kategóriáinak feldolgozása és a 11. cikke az automatizált egyedi döntéshozatal kapcsán..

¹⁴¹ Ebers Martin: Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act In :The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, (2021) <https://ssrn.com/abstract=3900378> or <http://dx.doi.org/10.2139/ssrn.3900378>

¹⁴² Az a tény, hogy egy fényképet az érintett egyértelműen nyilvánosságra hozott nem jelenti azt, hogy a fényképből különleges technikai eszközökkel kinyerhető kapcsolódó biometrikus adatok is egyértelműen nyilvánosságra hozottak minősülnek. Egy szolgáltatás alapértelmezett beállításai, a sablonok nyilvános hozzáférhetővé tétele, választás lehetősége nélkül, anélkül, hogy a felhasználó megváltoztathatná ezt a beállítást, semmiképpen sem tekinthetők egyértelműen nyilvánosságra hozott adatoknak.

arcfelismerő technológia alapján hoznak döntéseket.¹⁴³ A korlátozáshoz való jog különösen fontossá válik - az algoritmuson alapuló arcfelismerő technológia esetében, ha nagy mennyiségű adatot gyűjtenek, és az azonosítás pontossága és minősége változhat.

Az adatvédelmi hatásvizsgálat (DPIA) kötelező előírás az arcfelismerő technológia alkalmazása előtt, a GDPR 27. cikkével összhangban. A DPIA eredményeinek vagy legalább a főbb megállapításainak és a következtetéseknek a nyilvánosságra hozatalát javasolja az EDPB, a bizalom és az átláthatóság növelése érdekében. Az FRT-t bevezető hatóságnak konzultálnia kell az illetékes felügyeleti hatósággal a rendszer bevezetése előtt. A biometrikus adatok egyedi jellege miatt különös figyelmet kell fordítani a biztonsági intézkedésekre az FRT-t bevezető és/vagy használó hatóság részéről a GDPR 29. cikke értelmében. A bűnüldöző hatóságnak biztosítania kell, hogy a rendszer megfeleljen a vonatkozó szabványoknak, és biometrikus sablonvédelmi intézkedéseket hajtson végre. Az adatvédelmi elveket és biztosítékokat a technológiába kell beépíteni még a személyes adatok feldolgozása előtt – a beépített adatvédelem elve alapján. A naplózás kiemelt jelentőséggel bír az adatkezelési folyamatok jogosságának biztosításában, mind az adatkezelő belső auditjai, mind a külső, felügyeleti szervek általi ellenőrzések terén. Az arcfelismerő technológiák alkalmazásánál ajánlott az olyan naplózási gyakorlat bevezetése, amely magában foglalja a referenciaként szolgáló adatbázisok módosításait és az azonosítási folyamatokat. Az EDPB és az EDPBS szükségesnek tartja bizonyos típusú feldolgozási eljárások tiltását, úgymint az emberek távolról történő biometrikus azonosítását (nyilvános helyeken), a mesterséges intelligenciával támogatott arcfelismerő rendszereknek az etnikai hovatartozás, nemek, valamint politikai vagy szexuális irányultság vagy más megkülönböztető okok szerinti felhasználását, az arcfelismerésből következtetéseket levonni kívánó technológiák használatát, valamint a személyes adatok bűnüldözési célú nagy adatbázisokban történő tömeges és megkülönböztetés nélküli gyűjtését. Ez az iránymutatás vonatkozik az uniós és nemzeti jogalkotókra, a bűnüldöző hatóságokra, az egyénekre az érintetti jogokat

¹⁴³ Ha biometrikus adatokat tárolnak és azokat összekapcsolják az alfanumerikus adatokkal, a hozzáférési kérelmeket az alfanumerikus adatok alapján kell ellenőrizni, hogy ne kezdeményezzenek további biometrikus adat feldolgozást. Az érintetteket súlyos kockázatok érhetik, ha pontatlan adatokat tárolnak és megosztanak róluk rendőrségi adatbázisokban vagy más szervezeteknél. Az adatkezelőnek élniük kell a helyesbítés lehetőségével az adatok és az arcfelismerő rendszerek, különösen az algoritmuson alapuló arcfelismerő technológia esetén, a LED erre vonatkozó (47) preambulumbekzdése alapján.

illetően. Az iránymutatás eszköz , egy adott felhasználási eset érzékenységének első osztályozásához, gyakorlati útmutatást ad azon helyi hatóságok számára, amelyek FRT-rendszert kívánnak beszerezni és működtetni és számos tipikus felhasználási esetet is bemutat, különösen a szükségesség és az arányosság vizsgálata tekintetében.¹⁴⁴

3.2.4. Az Európai Unió Bírósága (EUB)

Az Európai Bíróság az adatvédelem terén döntéseket hozhat az adatvédelmi jogszabályok értelmezésével és alkalmazásával kapcsolatos vitás kérdésekben, döntései irányt mutathatnak az adatvédelmi gyakorlat számára.

Az EUB ismertebb adatvédelemmel kapcsolatos ügyei: Schrems II. ügy (C-311/18, Tele2/Watson ügy (C-203/15 és C-698/15),¹⁴⁵ Digital Rights Ireland (C-293/12),¹⁴⁶ Weltimmo (C-230/14) ügy.¹⁴⁷

A bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel kapcsolatos ítélkezési gyakorlat során az EUB előtt előzetes döntéshozatali eljárások keretében a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv értelmezéséről több ügy is folyamatban van, mint

¹⁴⁴ EDPB 05/2022, Annex I.II.III.

¹⁴⁵ Az ítélet alapján a Bíróság megállapította, hogy a tömeges adatgyűjtés és -megőrzés csak akkor engedélyezhető, ha az arányos és szükséges a súlyos bűncselekmények megelőzése vagy felderítése érdekében. Az adatgyűjtésnek konkrét célokkal -, mint például a terrorizmus elleni küzdelem - kell történnie. Az ítéletben a Bíróság hangsúlyozta, hogy az adatgyűjtés csak akkor megengedett, ha az az egyének magánéletének és adatvédelmének alapvető elveivel összeegyeztethető.

¹⁴⁶ Az ítéletben az Európai Bíróság kimondta, hogy az Európai Unió adatmegőrzési irányelve, amely a kommunikációs adatok hosszabb távú megőrzését rendelte el a bűnüldözési célokra, sérti az alapvető jogokat, különösen az adatvédelmet és a magánéletet.

¹⁴⁷ Az ítéletben az Európai Bíróság kifejtette, hogy egy vállalkozás a saját tagállamán kívülre történő adatkezelés esetén is alkalmaznia kell az adatvédelmi jogszabályokat, ha az adatkezelés az adatok tárolására, kezelésére vagy feldolgozására irányul.

Egy vállalatot azon tagállam jogszabályai szerint kell elszámoltatni -, az adott esetben az online ingatlanhirdetések közzétételéért - ahol a tevékenysége hatással van a az ott élő emberekre, még akkor is, ha a vállalat fizikailag egy másik tagállamban van bejegyezve.

például a WS kontra Bundesrepublik Deutschland¹⁴⁸ és a B kontra Latvijas Republikas Saeima¹⁴⁹ ügyek. Az egyes ügyeket az irányelv jogértelmezéseivel kapcsolatban ismertetem.

III. A Bűnügyi Adatvédelmi Irányelv (LED) - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv és jogharmonizációja

1. A bűnügyi adatvédelmi irányelv bemutatása¹⁵⁰

Az Európai Parlament 2016. április 27-i (EU) 2016/680 irányelve 2016. május 4-én került kihirdetésre, egyúttal hatályon kívül helyezve a 2008/977/IB tanácsi kerethatározat.

Jelentős előrelépés a korábbi kerethatározattal szemben, hogy egyrészt teljes körű szabályokat határoz meg a személyes adatok bűnüldözési célú, határokon átnyúló és belföldi kezelésére egyaránt, míg a tanácsi kerethatározat csak a határokon átnyúló adatkezelésre vonatkozott. Másrészt átfogó horizontális szabályrendszert határoz meg, míg korábban minden olyan ágazati jogi szabályozásra, mely a bűnüldözési célú adatok kezelését írta elő, a saját adatvédelmi szabályai voltak irányadók. Példaként említhető, hogy a Schengeni Információs Rendszer működését és a schengeni vívmányokhoz kapcsolódó egyéb eszközöket szabályozó jogszabályok tartalmazznak olyan specifikus rendelkezéseket, amelyek az érintett személyek jogait szabályozzák.

Az irányelv célja, hogy garantálja az egyének személyes adataik védelméhez való jogát, emellett a bűnüldözési célból kezelt személyes adatok belföldi kezelésére és határokon átnyúló továbbítására vonatkozó szabályok egységesítésével elősegíteni a tagállamok közötti együttműködést, és a közbiztonság magas szintjét is kívánja biztosítani.

¹⁴⁸ C-505/19, WS kontra Bundesrepublik Deutschland, ECLI:EU:C:2021:376. Az ügy többek között a személyes adatok kezelésének jogszerűségére vonatkozott (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 4. cikke (1) bekezdésének a) pontja és 8. cikke) az Interpol által kiadott piros sarkos körözéssel összefüggésben. A Bíróság nem zárta ki az Interpol által kiadott piros sarkos körözésben szereplő személyes adatok jogszerű kezelését mindaddig, amíg jogerős bírósági határozat nem állapítja meg, hogy a ne bis in idem elve alkalmazandó az említett értesítés alapjául szolgáló cselekményekre.

¹⁴⁹ C-439/19, B kontra Latvijas Republikas Saeima, ECLI:EU:C:2021:504. Az EUB értelmezte a 3. cikk (7) bekezdése szerinti illetékes hatóság meghatározását és a bűncselekmény fogalmát.

¹⁵⁰ Gáti Balázs. „Az adatvédelmi szabályozás aktuális tendenciái a büntető igazságszolgáltatás területén” p. 46.

A jogirodalomban az irányelv számos értelmezése és bemutatása lelhető fel.^{151,152,153}

Az értelmezési kérdésekkel kapcsolatos jelentősebb források az irányelv egyes pontjainál kerülnek ismertetésre.

Az Irányelv preambulumból és tíz fejezetből épül fel. A preambulum hivatkozik az Alapjogi Charta és az EUSZ. 16. cikkének (1) bekezdésére, amelyek rögzítik, hogy „*mindenkinek joga van a rá vonatkozó személyes adatok védelméhez*”^{154,155}, megállapítja, hogy ezen jogok állampolgárságtól és lakhelytől függetlenek^{156,157}, azokat minden tagállamban azonos módon szükséges kezelni. A bűncselekmények megelőzése, felderítése és nyomozása a közbiztonságot fenyegető veszélyekkel szembeni védelemre és e veszélyek megelőzésére is kiterjed.¹⁵⁸

Az irányelv tárgyi hatálya bűnüldözési célból végzett adatkezelésekre terjed ki.¹⁵⁹ Ez az értelmezés tágabban azt jelenti, hogy a LED az adatkezelési tevékenységekre akkor alkalmazandó, ha két kumulatív feltétel teljesül: az adatkezelés az 1. cikk (1) bekezdésében¹⁶⁰ meghatározott célok valamelyikét szolgálja, és azt a 3. cikk (7) bekezdésében¹⁶¹ meghatározott illetékes hatóságok végzik. Ha e feltételek egyike sem teljesül, akkor a GDPR alkalmazandó.

¹⁵¹ Nagy Zoltán András, Mezei Kitti (2018). "Az Európai Unió Bűnügyi Adatvédelmi Irányelvről." In *A XXI. század biztonsági kihívásai*, szerk. Gaál, Gyula; Hautzinger, Zoltán. Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport pp. 229-234.

¹⁵² Eszteri Dániel. (2018) "A bűnügyi adatvédelmi irányelv." In *Magyarázat a GDPR-ról*, szerk. Buzás, Péter; Péterfalvi, Attila; Révész, Balázs. Budapest, Magyarország: Wolters Kluwer, pp. 385-401.

¹⁵³ Eszteri Dániel. (2021)"A bűnügyi adatvédelmi irányelv az Infotv. kontextusában." In *Magyarázat a GDPR-ról: második, bővített kiadás*, szerk. Bendik, Tamás; Árvay, Viktor; Bojnár, Katinka; Eszteri, Dániel; Majsa, Ágnes; Osztopáni, Krisztián; Sziklay, Júlia - Péterfalvi, Attila; Buzás, Péter; Révész, Balázs. Budapest, Magyarország: Wolters Kluwer Hungary, pp. 489-506.

¹⁵⁴(EU) 2016/680 Preambulum (1)

¹⁵⁵ Szinte szó szerint ezt adja vissza a magyar Alaptörvény. „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.”, Alaptörvény VI. cikk 3.

¹⁵⁶(EU) 2016/680 Preambulum (2).

¹⁵⁷(EU) 2016/680 Preambulum (17).

¹⁵⁸(EU) 2016/680 Preambulum (12).

¹⁵⁹ (EU) 2016/680 Preambulum (11).

¹⁶⁰ „a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – így többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából”

¹⁶¹ „illetékes hatóság”: a) olyan közhatalmi szerv, amely a bűncselekmények megelőzését, nyomozását, felderítését vagy üldözését, illetve büntetőjogi szankciók végrehajtását illetően eljárni jogosult beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését; vagy b) bármely egyéb, olyan szerv vagy

A bűnügyi irányelv kimondja, hogy előírásai nem alkalmazandók a személyes adatoknak az uniós jog hatályán kívül eső tevékenységek keretében végzett kezelésére, a nemzetbiztonsággal kapcsolatos tevékenységek, a nemzetbiztonsági ügyekkel foglalkozó ügynökségek vagy egységek tevékenységei, valamint a tagállamok által az EUSZ. V. címe 2. fejezetének - a közös kül- és biztonságpolitikára vonatkozó különös rendelkezések - hatálya alá tartozó tevékenységek során végzett személyes adatkezelésekre.¹⁶²

A nemzetbiztonság fogalmának értelmezése további jogértelmezési problémákat vet fel, hagyományosan az állami szuverenitáshoz kapcsolódik, az állam alapvető funkcióihoz és a társadalom alapvető érdekeihez kapcsolódik.¹⁶³

A bűncselekmény fogalmának meghatározása¹⁶⁴ az irányelv szerint értelmezendő, „*az Európai Unió Bírósága (...) általi értelmezésnek megfelelő, önálló uniós jogi fogalomnak minősül*”.^{165,166} Meghatározza azokat az illetékes hatóságokat, - személyi hatály - akikre vonatkozik az irányelv, amelyek körébe nem csak olyan közhatalmi szervek tartozhatnak mint az igazságügyi hatóságok, a rendőrség vagy egyéb bűnüldöző hatóságok, hanem bármely egyéb olyan szerv vagy jogalany is, amely a tagállami jog alapján ezen irányelv alkalmazása céljából közfeladatokat lát el és közhatalmi jogosítványokat gyakorol. A LED 3. cikke (7) bekezdésének b) pontja szerint továbbá illetékes hatóság lehet bármely más szerv vagy szervezet, amelyet a tagállam joga megbízott azzal, hogy ugyanezen bűnüldözési célokból közhatalmat és közhatalmat gyakoroljon.¹⁶⁷

más jogalany, amely a tagállami jog alapján közfeladatokat lát el és közhatalmi jogosítványokat gyakorol a bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása céljából, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését

¹⁶² (EU) 2016/680, Preambulum (14)

¹⁶³ Latvijas Republikas Saeima, C-439/19. sz. 2021. június 22-i ítélet, ECLI:EU:C:2021:504, 67. pont.

¹⁶⁴ (EU) 2016/680, Preambulum (13).

¹⁶⁵ C-439/19, EU:C:2021:504, 87. pont.: Ennek megfelelően annak megítélése, hogy egy bűncselekmény büntetőjogi természetű-e, három tényezőtől függ: attól, hogy a bűncselekményt a nemzeti jog ekként minősíti-e, a bűncselekmény „belső” jellegétől, valamint az érintett személyre kiszabható büntetés súlyosságának mértékétől.

¹⁶⁶ A bűncselekmény fogalmának az EUB és az EJEB vonatkozó esetjogának elemzése kapcsán a fogalom lefedti a szabálysértési eljárás során és céljából kezelt személyes adatokat, így azok kezelése is az irányelv hatálya alá tartozik. Lásd. Eszteri Dániel: „Bűnügyi adatvédelmi irányelv az Infotv. kontextusában”

¹⁶⁷ Latvijas Republikas Saeima, C-439/19, 2021. június 22-i ítélet, ECLI:EU:C:2021:504, 70. pont.: Az EUB szerint az illetékes hatóságot "a személyes adatok védelme tekintetében a büntetőügyekben folytatott igazságügyi

Az irányelvtől eltérő cél tekintetében az (EU) 2016/679 rendeletet kell alkalmazni. Ilyen tevékenység például a hatósági jogkör gyakorlása, valamint ha például bűncselekmények nyomozása, felderítése és a vádeljárás lefolytatása céljából a pénzügyi intézmények bizonyos általuk kezelt személyes adatokat megőriznek, és azokat kizárólag meghatározott esetekben és a tagállami joggal összhangban az illetékes nemzeti hatóságok részére szolgáltatják.¹⁶⁸

A személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelésére a 45/2001/EK európai parlamenti és tanácsi rendelet alkalmazandó¹⁶⁹, amely rendeletet az (EU) 2018/1725 rendelet – EUDPR - váltotta fel.

Az irányelv a preambulumban utal a személyes adatok kezelésének alapelveire, ezzel kapcsolatban a jogszerű, tisztességes és átlátható adatkezelés elvével kapcsolatosan – a Charta 47. cikke, és az EJEE 6. cikkében meghatározott fogalomtól elkülöníti azt.¹⁷⁰ Kiemeli az irányelv a tájékoztatáshoz való jogot, valamint az ehhez kapcsolódó korlátokat, a jogszerű, átlátható,¹⁷¹ és tisztességes adatkezelés, a megfelelő szintű biztonság és bizalmas kezelés elvét, a célhoz kötöttség, szükségesség és arányosság elvét, a pontosság elvét.¹⁷²

A GDPR és LED elvek bizonyos értelemben különböznek egymástól, példa erre átláthatóság elve, amelyről a 4. cikk nem rendelkezik kifejezetten. A büntető igazságszolgáltatás és a bűnüldözés szükségleteinek jellege azonban olyan, hogy a bűnügyi nyomozások és a biztonsági érdekek védelme érdekében az átláthatóság különböző szintjeit követeli meg.¹⁷³

A célhoz kötöttség és az adatminimalizálás elvei is másképpen jelennek meg mint a GDPR-ban. A LED külön rendelkezéseket vezet be a tárolási határidőkre, valamint az érintettek és az adatok különböző kategóriái közötti különbségtételre vonatkozóan. Az adatminimalizálási

együttműködés és a rendőrségi együttműködés területén kell érteni, tekintettel azokra a rendelkezésekre, amelyek e tekintetben e területek sajátos jellege miatt szükségesnek bizonyulhatnak".

¹⁶⁸ (EU) 2016/680, Preambulum (11) és 3.cikk. (2).

¹⁶⁹ Az Európai Parlament és Tanács. 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról. *Hivatalos Lap* L 8 2001.1.

¹⁷⁰ (EU) 2016/680, Preambulum (26)

¹⁷¹ WP258, Vélemény a bűnüldözési irányelv (EU 2016/680) néhány kulcskérdéséről.

.A WP29 azt állítja, hogy az átláthatóságot a LED III. fejezete szerinti érintettek jogai biztosítják.

¹⁷² (EU) 2016/680, Preambulum (26) – (30).

¹⁷³ Leiser, M., Custers, B. (2019) "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680", *European Data Protection Law Review*, Vol. 5, (3), pp. 367-78.

elvek megfogalmazás is a bűnüldözés sajátos igényeinek figyelembevételére és a személyes adatok védelme mellett a tisztességes eljárás tiszteletben tartásának biztosítására is törekszik.¹⁷⁴ A LED az érintettek különböző kategóriáihoz tartozó személyes adatok elkülönítését a büntetőügyekben különösen fontosnak tartja, így a bűncselekmények elkövetésével gyanúsított vagy amiatt elítélt személyek, az áldozatok, illetve egyéb érintett felek, például tanúk vagy a gyanúsítottak és az elítélt bűnelkövetők kapcsolataira és bűntársaira vonatkozó személyes adatok közötti elkülönítést.¹⁷⁵

Az érintett hozzájárulása önmagában sohasem képezheti a jogalapját a különleges személyes adatok kezelésének a bűnügyi irányelv kontextusában. Ez egy jelentős eltérés a GDPR-hoz képest.¹⁷⁶ Eszerint a bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása az illetékes hatóságok feladata, amelyek elrendelhetik vagy megkövetelhetik a természetes személyektől kérésük teljesítését. Ebben az összefüggésben az érintettek hozzájárulása, amint azt a GDPR meghatározza, nem képezheti a személyes adatok kezelésének jogalapját az illetékes hatóságok részéről. Ha az érintett jogi kötelezettségek alapján cselekszik, nem áll fenn szabad választás lehetősége, ezért az ilyen típusú hozzájárulás nem értelmezhető az akarat szabad megnyilvánulásaként.¹⁷⁷

Az irányelv kötelezi a tagállamokat, hogy közérthető tájékoztatást jogának biztosításához¹⁷⁸, valamint az érintett hozzáférési jogának biztosításához¹⁷⁹, illetve a jogokat a helyesbítéshez, törléshez stb.¹⁸⁰, korlátozásokat is előír, lehetővé téve a tagállamok számára, hogy e jogokat korlátozó jogalkotási intézkedéseket fogadjanak el. *„Ez az irányelv nem zárja ki, hogy a tagállamok a személyes adatok bíróságok és más igazságügyi hatóságok általi feldolgozásával*

¹⁷⁴ Quezada-Tavárez, K., Vogiatzoglou, P. and Royer, S. (2021) "Legal Challenges in Bringing AI Evidence to the Criminal Courtroom", *New Journal of European Criminal Law*, Vol. 12, (4) pp.531-551.

¹⁷⁵(EU) 2016/680, Preambulum (31).

¹⁷⁶ (EU) 2016/680, Preambulum (35).

Eszerint a bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása feladatának ellátását az irányelv intézményesen átruházza az illetékes hatóságokra, melyek elrendelhetik vagy megkövetelhetik a természetes személyektől az adatszolgáltatás teljesítését. Ebben az esetben az érintettnek a GDPR-ban meghatározott értelemben vett hozzájárulása nem szolgálhat jogalapul a személyes adatok illetékes hatóságok általi kezeléséhez. Ha az érintett jogi kötelezettséget teljesít, nincs valós és szabad választási lehetősége, ezért az érintett hozzájárulása nem tekinthető akarata szabad kinyilvánításának

¹⁷⁷ (EU) 2016/679 6.cikk.(1) e)

¹⁷⁸ (EU) 2016/680, Preambulum (38), (39).

¹⁷⁹ (EU) 2016/680, Preambulum (43), (44), és 13. cikk.

¹⁸⁰ (EU) 2016/680, 13. cikk. (e).

*kapcsolatos büntetőeljárásokra vonatkozó nemzeti szabályokban meghatározzák az adatkezelési műveleteket és eljárásokat, különösen a bírósági határozatokban vagy a bírósági nyilvántartásokban szereplő személyes adatok tekintetében. a büntetőeljárásokkal kapcsolatban.”*¹⁸¹.

Az érintett tevékenyen közreműködhet az adatai kezelésében, amennyiben az érintett rendelkezésére kell bocsátani legalább a következő információkat: „*az adatkezelő kilétét, az adatkezelési művelet tényét, az adatkezelés céljait, tájékoztatást a panasz benyújtásának jogáról, valamint az ahhoz való jogról, hogy az érintett az adatokhoz való hozzáférést, az adatok helyesbítését, törlését, illetve az adatkezelés korlátozását kérje az adatkezelőtől.*”¹⁸² Az érintetti jogok gyakorlását lehetővé kell tenni a felügyeleti hatósághoz történő panasztétel jogával és a hatóság elérhetőségével.¹⁸³

Kiemelendő, hogy az érintettek jogai önmagukban nem akadályozzák a bűnüldöző szerveket abban, hogy olyan tevékenységeket folytassanak, mint a titkos nyomozás vagy a videó megfigyelés¹⁸⁴.

Az automatizált adatkezelés alapján történő döntéshozatal esetében az irányelv rendelkezik arról, hogy az érintetteknek jogot kell biztosítani arra, hogy az ilyen döntés ne érinthesse őket hátrányosan. Megfelelő garanciákat kell nyújtani az érintettek számára, beleértve a tájékoztatáshoz való jogot, az emberi beavatkozás lehetőségét, valamint a döntések megtámadásának jogát. A profilalkotás, amely alapvető jogokat sértő megkülönböztetést eredményez, különösen érzékeny adatok esetében, tilos.¹⁸⁵

A preambulum szabályozza továbbá a megfelelőség, a felügyeleti hatóságok¹⁸⁶, és a harmadik országba történő továbbításra vonatkozó rendelkezéseket.¹⁸⁷

A szabályozás a kötelező kölcsönös segítségnyújtás szabályait is rögzíti, és általános együttműködési kötelezettséget ír elő¹⁸⁸. Kimondja továbbá, hogy az EDPB hatásköre kiterjed

¹⁸¹ (EU) 2016/680, Preambulum (20).

¹⁸² (EU) 2016/680, Preambulum (42).

¹⁸³ (EU) 2016/680, Preambulum (52) (55), 13. cikk (1). Ennek alapján az érintettnek joga van ahhoz, hogy személyes adataihoz hozzáférjen.

¹⁸⁴ (EU) 2016/680, Preambulum (26).

¹⁸⁵ EU) 2016/680, Preambulum (38)

¹⁸⁶ EU) 2016/680, Preambulum (48), (54), (56) (59) (61) (62) (72), (74),(76),(77),(78),(79), (81)- (87),(90), (91) (96)

¹⁸⁷ (EU) 2016/680, Preambulum (67)- (75)

¹⁸⁸ (EU) 2016/680, Preambulum (77), 40. cikk (b).

az ezen irányelv hatálya alá tartozó adatkezelési tevékenységekre¹⁸⁹. Az irányelv ezenkívül kártérítési jogot biztosít az érintettek részére abban az esetben, ha jogsértés, vagy jogellenes adatkezelés következtében kár érte őket¹⁹⁰.

A harmadik országba történő továbbítással kapcsolatban megállapítja, hogy az adatok harmadik országba csak akkor továbbíthatók, ha az bűnüldözési célból szükséges, és a Bizottság megfelelési határozatot fogadott el az érintett harmadik országban nyújtott védelemi szintjéről¹⁹¹. Megfelelési határozat hiányában az adattovábbítás csak megfelelő biztosítékok alapján lehetséges,¹⁹² azonban különleges körülmények fennállása esetén is előírja az adatok továbbítását¹⁹³.

Az I. fejezet – az általános rendelkezések - a tárgyat és célokat, a hatályt, és a fogalom meghatározásokat tartalmazza.¹⁹⁴ A tagállamok ezen irányelvvel összhangban „*védik a természetes személyek alapvető jogait és szabadságait, különösen a személyes adatok védelméhez való jogukat, és biztosítják, hogy a személyes adatok illetékes hatóságok közötti, Unión belüli cseréje (...) ne legyen korlátozás vagy tiltás tárgya*”¹⁹⁵

Az irányelv 3. cikke a „Fogalom meghatározások” tizenhat fogalmat határoz meg, köztük a profilalkotás, az illetékes hatóság, az adatkezelő, adatfeldolgozó és a címzett fogalmát.¹⁹⁶

A II. fejezet - az Elvek - a személyes adatok kezelésére vonatkozó elveket a tárolásra és a felülvizsgálatra vonatkozó határidőket, az érintettek különböző kategóriái közötti különbségtételt, a személyes adatok és a személyes adatok minőségének ellenőrzése közötti különbségtételt, az adatkezelés jogszerűségét, a különös adatkezelési feltételeket, valamint a személyes adatok különleges kategóriáinak kezelését és az egyedi ügyekben történő automatizált döntéshozatalt szabályozza.¹⁹⁷

¹⁸⁹ (EU) 2016/680, Preambulum (84) 51.cikk.

¹⁹⁰ (EU) 2016/680, Preambulum (88) 56. cikk.

¹⁹¹ (EU) 2016/680, Preambulum (64), 36. cikk (1).

¹⁹² (EU) 2016/680, Preambulum (70) (71), (72) 35. – 37.cikk.

¹⁹³ (EU) 2016/680, 38.cikk.

¹⁹⁴ (EU) 2016/680, 1 cikk– (2) a), b).

¹⁹⁵ (EU) 2016/680, 1 cikk– (2) a), b).

¹⁹⁶ (EU) 2016/680, 7.–10. pont.

¹⁹⁷ (EU) 2016/680, 4.– 11. cikk.

Az alapelvek közül a személyes adatok különleges kategóriáinak¹⁹⁸ kezelésével kapcsolatos elveket emelném ki. Az irányelv kimondja, hogy az ilyen adatok csak akkor kezelhetők, ha azt,

- „az uniós vagy tagállami jog lehetővé teszi;
 - az érintett vagy más természetes személy létfontosságú érdekeinek védelmét szolgálja;
- vagy
- az ilyen adatkezelés olyan adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott”¹⁹⁹

A tárolásra és a felülvizsgálatra vonatkozó határidőkkel kapcsolatban az irányelv előírja, hogy azok betartását eljárásjogi intézkedésekkel kell biztosítani.²⁰⁰

Az érintettek különböző kategóriái közötti különbségtételről a preambulumban már volt szó.²⁰¹ Ennek jelentősége lehet az adattárolás időtartama szempontjából is, tekintettel arra, hogy az adatkezelés célja az egyes különböző kategóriák esetében különböző ideig maradhat fenn, melynek megszűnése után az adatok nem tárolhatók a célhoz kötöttség elve alapján.²⁰² Az EJEB és az EUB ítélkezési gyakorlatára, valamint a LED (26) preambulumbekzdésére való hivatkozással az adatminimalizálás elvének való megfelelés többek között azt követeli meg, hogy az adatokat ne tárolják tovább, mint amennyi az elérni kívánt célhoz szükséges, és csak akkor, ha az adatkezelés célja ésszerűen nem teljesíthető más eszközökkel.²⁰³

¹⁹⁸ „(...) faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok”

¹⁹⁹ (EU) 2016/680, 10. cikk. A Preambulum (37) pontja a személyes adatok különleges kategóriáinak kezelésével kapcsolatos biztosítékokat sorolja fel.

²⁰⁰ (EU) 2016/680, 5. cikk.

²⁰¹ (EU) 2016/680, 6. cikk.

²⁰² C-205/21. számú Ministerstvo na vatreshnite raboti kontra B. C, „Előzetes döntéshozatal – A természetes személyek védelme a személyes adatok kezelése vonatkozásában – (EU) 2016/680 irányelv – 4., 5., 8., 10. és 16. cikk – Szándékos bűncselekmény miatt elítélt természetes személy adatainak a haláláig történő tárolása – Jogerős ítélettel elítélt, majd mentesítésben részesült természetes személy – Törlés iránti kérelem elutasítása – Az Európai Unió Alapjogi Chartájának 7. és 8. cikkében foglalt alapvető jogokba való beavatkozás szükségessége és arányossága”

²⁰³ C-205/21, Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2022:507, 54-55. pont.

A LED újdonsága a tárolási határidőkre és a tárolás szükségességének időszakos felülvizsgálatára vonatkozó külön rendelkezés²⁰⁴ amely megerősíti a tárolás korlátozásának elvét.²⁰⁵

A LED átültetés értelmezése kapcsán a jogirodalomban a kategorizálásra vonatkozó LED-rendeletek aggályokat is felvetettek azzal kapcsolatban, hogy a szabályok statikusak. Ugyanis döntéseket kell hozni a bűncselekmény szereplőinek tipizálására vonatkozóan, a büntetőeljárás korai szakaszában, miközben ezek a döntések gyakran még tévesek lehetnek.²⁰⁶

A bűnügyi nyomozásokat a változékonyság jellemzi, tekintettel arra, hogy a szerepek idővel változhatnak, (pl. tanúból terhelt stb.) mivel a kategóriákra vonatkozó bizonyítékok gyarapodnak és frissülnek. A szerepek átfedhetik egymást, vagy tovább oszthatók alkategóriákra vagy a bűncselekményben való részvétel spektrumára.²⁰⁷ Ezt teszi megfontolás tárgyává Pálvölgyi is, önmagában az a körülmény, hogy megváltozik az eljárásjogi helyzete valakinek, például terheltből tanú lesz, nem jelent sérelmes helyzetet. Azonban, ha ezt a körülményt, mint személyes adatot, az azt kezelő nem veszi figyelembe, akkor jogsérelmes helyzet alakulhat ki.²⁰⁸

Az irányelv 8. cikkének (2) bekezdése szerint a tagállamoknak kell meghatározniuk az adatkezelés jogalapját, azaz meg kell határozniuk, hogy melyik hatóság rendelkezik hatáskörrel a személyes adatok kezelésére, az adatkezelést indokoló közfeladatokra, valamint az adatkezelés célját illetően is. Az adatkezelési tevékenységet az illetékes hatóság által a LED céljaira végzett feladat végrehajtásához, az uniós vagy nemzeti jog alapján kell végrehajtani. Az illetékes hatóságoknak kell meghatározniuk az adatkezelés jogalapját sajátos feladatkörük alapján, a hozzájárulás vagy a szerződés, nem elfogadható jogalapok. A tagállamok jelentős

²⁰⁴ (EU) 2016/680, 5. cikk,

²⁰⁵ (EU) 2016/680, 4. cikk (1)

²⁰⁶ Leiser, M. and Custers, B. " The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680" p.369

²⁰⁷ Winter, H.B. et al, (2020) „De verwerking van politiegegevens in vijf Europese landen, Rijksuniversiteit Groningen - Pro facto” , WODC rapport 3031

²⁰⁸ Pálvölgyi, Ákos.(2014) "A hírérték margóján: személyhez fűződő jogok védelméhez való jog a büntetőeljárásban különös tekintettel a személyes adatok védelmére." *Büntetőjog Szemle*, (3) pp. 41-45.

mérlegelési mozgástérrel rendelkeznek az adatkezelés indokairól való döntés során, azonban az alapjogokra tekintettel kell lenniük.²⁰⁹

A LED tartalmaz egy "különleges adatkezelési feltételek" elnevezésű rendelkezést, amely tovább pontosítja a célhoz kötöttség elvét, amikor a bűnüldözési célokból kezelt személyes adatok nem bűnüldözési célokra, azaz a LED-ből a GDPR- vagy az EUDPR keretrendszerébe kerülnek át. A 9. cikk (1) bekezdése szerint az eredetileg az illetékes hatóságok által és bűnüldözési célból gyűjtött személyes adatok csak akkor dolgozhatók fel nem bűnüldözési célokra, ha a feldolgozást az uniós vagy nemzeti jog engedélyezi.²¹⁰ Ez a záradék különösen fontossá vált a bűnüldözési eszközökkel kapcsolatos tudományos kutatás során, amely gyakran valós adatok felhasználását teszi szükségessé.²¹¹

Az irányelv 10. cikke a személyes adatok különleges kategóriáinak kezelésével kapcsolatosan a jogszabály által engedélyezett adatkezelést, az érintett vagy egy másik személy létfontosságú érdekeinek védelmét, vagy az érintett által nyilvánvalóan nyilvánosságra hozott adatokra vonatkozó adatkezelést irányozza elő jogalapként. Tehát a LED nem tiltja a személyes adatok különleges kategóriáinak feldolgozását önmagában, ellentétben az általános adatvédelmi rendelet 9.cikkével.²¹²

Az olyan automatizált döntéshozatal, amely a profilalkotást is érinti, és az érintettre hátrányos, vagy a személyes adatok különleges kategóriáira vonatkozik tilos, kivéve, ha „*olyan uniós vagy tagállami jog teszi lehetővé, amely az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciákról is rendelkezik, ideértve legalább az érintett jogát arra, hogy az adatkezelőtől*

²⁰⁹ Bäcker, M. és Hornung, (2012) "Data Processing by Police and Criminal Justice Authorities in Europe - The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure", *Computer Law & Security Review*, Vol 28. (6) pp. 627-33.

²¹⁰ (EU) 2016/680, 9. cikk

²¹¹ Bolognini, L., A. (2020) „Proposal for the EU Privacy Law Simplification, Supporting Data-Driven Research in the Law Enforcement Field” Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP), <https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven>,

²¹² Együtt értelmezendő a 10. cikk a (37) preambulum bekezdéssel, amely szerint "[...] személyes adatok (különleges kategóriái) nem dolgozhatók fel, kivéve, ha az adatkezelésre az érintett jogainak és szabadságainak megfelelő, jogszabályban meghatározott garanciái vonatkoznak, és azt törvény által engedélyezett esetekben engedélyezik”

emberi beavatkozást kérjen".²¹³ Az érintett jogosult tájékoztatást, és magyarázatot kapni a az automatizált adatkezelés során hozott döntésről, valamint joga van, hogy megtámadja a döntést. A III. fejezet - Az érintett jogai – szabályozza a tájékoztatás és az érintett jogainak gyakorlására vonatkozó módokat, az érintett rendelkezésére bocsátandó vagy számára nyújtandó információkat, az érintett hozzáférési jogát, a hozzáférési jog korlátozását, a személyes adatok helyesbítéséhez, törléséhez és kezelésének korlátozásához való jogot, az érintett jogainak gyakorlását és a felügyeleti hatóság általi ellenőrzését és az érintettet a bünyügyi nyomozások és büntetőeljárások során megillető jogokat²¹⁴.

Az automatizált döntéshozatali információkra vonatkozó tilalom az egyéni döntéshozatalra összpontosít, a kollektív vagy csoportos profilalkotást figyelmen kívül hagyva. Ez a szabályozás bizonyos esetekben problémát okozhat, mint például a prediktív rendőri technológiák esetében. Bűnözési célpontok azonosítása esetén megnehezíti annak megkülönböztetését, hogy egy adott terület lakosai közül az egyén vagy a lakosok egy csoportja az érintett.²¹⁵ Kérdéseket vet fel az, hogy hogy mi minősül automatizált döntésnek, milyen mértékű és jellegű emberi beavatkozásra van szükség.^{216•217}

A hozzáférési jog korlátozása szükséges és arányos intézkedés annak érdekében, hogy „*ne gördüljenek akadályok a hivatalos vagy jogi vizsgálatok, nyomozások vagy eljárások elé; ne szenvedjen sérelmet a bűncselekmények megelőzése, felderítése, nyomozása vagy a vádeljárás lefolytatása, illetve a büntetőjogi szankciók végrehajtása; biztosított legyen a közbiztonság védelme, biztosított legyen a nemzetbiztonság védelme, biztosított legyen mások jogainak és szabadságainak védelme*”.²¹⁸

A 17. cikk előírja, hogy az érintettek az adatvédelmi felügyeleti hatóságon keresztül gyakorolhassák jogaikat. Az érintettek jogainak a felügyeleti hatóság általi gyakorlását

²¹³ (EU) 2016/680, 11. cikk és Preambulum (38). Az érintett jogosult tájékoztatást, és magyarázatot kapni a az automatizált adatkezelés során hozott döntésről, valamint joga van, hogy megtámadja a döntést.

²¹⁴ (EU) 2016/680, 12.– 18. cikk.

²¹⁵ Lynskey, Orla. 2019. "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection Against Predictive Policing." *International Journal of Law in Context* 15, (2) pp. 162-176.

²¹⁶ Oswald, Marion, Jennifer Grace, Stephanie Urwin, and Geoffrey Barnes. (2018.) "Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality." *Information & Communications Technology Law* 27, no. 2: pp. 223-250.

²¹⁷ Sajfert, J., and T. Quintel. (2016): "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities." *European Data Protection Law Review* 2, no. 3 pp.397-408

²¹⁸ (EU) 2016/680, 15. cikk (1) a) – e)

szabályozó 17. cikk biztonsági hálót jelent mind az illetékes hatóságok, mind az érintettek számára.²¹⁹ Az illetékes hatóságok dönthetnek úgy, hogy a folyamatban lévő vizsgálatok²²⁰ védelme érdekében nem teszik lehetővé az érintettek számára az adatkezelés ellenőrzését, míg az érintettek lehetőséget kapnak arra, hogy a felügyeleti hatóság legalább az adatkezelés jogszerűségét ellenőrizze.²²¹

A WP29 szerint a 17. cikkben meghatározott úgynevezett "közvetett" hozzáférési jogot meg kell különböztetni az 52. cikk szerinti, a felügyeleti hatóságnál történő panasztételhez való jogtól, amely a LED keretében további jognak minősül²²². A WP29 megállapítása szerint, a LED nem egyértelmű megfogalmazása ellenére a felügyeleti hatóságokat a nemzeti jogban fel kell hatalmazni arra, hogy ne csak a hozzáférési jogot, hanem a helyesbítés, törlés és korlátozás további jogait is gyakorolják az érintettek nevében.²²³ Ugyanezt a felfogást fogadja el a szakirodalom, amely a felügyeleti hatóságok e hatáskörét az adatkezelés jogszerűségének egyfajta független felügyeletként fogja fel, összhangban az EJEB ítélkezési gyakorlatával.^{224,225}

Az irányelv tehát biztosítja a jogot a tagállamok részére, hogy az érintett rendelkezésére bocsátandó jogok - úgymint az érintett hozzáférési joga, a személyes adatok helyesbítéséhez, törléséhez és kezelésének korlátozásához való jog tekintetében a tagállami jogokkal összhangban gyakorolják azt „*ha a személyes adatokat büntügyi nyomozás vagy büntetőeljárás során kezelt bírósági határozat, vagy jegyzőkönyv vagy ügyirat tartalmazza*”²²⁶. A 18. cikk a LED szerint – az érintettek jogainak jelentős korlátozását írja elő, és lehetővé teszi a tagállamok számára, hogy a jogok gyakorlására alkalmazandó keretként a nemzeti jogot jelöljék ki, "*amennyiben a személyes adatokat büntetőeljárás vagy büntetőeljárás során feldolgozott bírósági határozat, nyilvántartás vagy ügyiratok tartalmazzák*".

²¹⁹ Drechsler, L. (2020) "Comparing LED and GDPR Adequacy: One Standard Two Systems", *Global Privacy Law Review*, Vol.1, No. 2, pp. 93-103.

²²⁰ (EU) 2016/680 13. cikk (3), 15. cikk (3) és 16. cikk (4)

²²¹ (EU) 2016/680 17. cikk (3),

²²² "Vélemény a bűnüldözési irányelv (EU 2016/680) néhány kulcskérdéséről", WP258, 2017. november 29., 23-24. o.

²²³ Ibid. pp. 23-24.

²²⁴ Roman Zakharov kontra Oroszország, App. no. 47143/06, 2015. december 11., 272-285. pont; Szabó és Vissy kontra Magyarország, App. no. 37138/14, 2016. január 12., 75-77. pontok.

²²⁵ Sajfert, J., and T. Quintel. "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities." p.340

²²⁶ (EU) 2016/680, 18. cikk.

A IV. fejezet - Adatkezelő és adatfeldolgozó, az általános kötelezettségek, a személyes adatok biztonsága, és az adatvédelmi tisztviselő szakaszokból épül fel²²⁷. Ezen részletes szabályok meghatározzák az adatkezelő kötelezettségeit, az adatkezelés, adatfeldolgozás folyamatát, a felügyeleti hatósággal való együttműködést, az adatkezelés biztonságát, az adatvédelmi incidens bejelentését, az érintett tájékoztatását az adatvédelmi incidensről, az adatvédelmi tisztviselő feladatát, jogállását. Az adatvédelmi incidenst azonnal, de legkésőbb 72 órán belül jelenteni kell a felügyeleti hatóságnak.²²⁸

A beépített adatvédelem elve szerint az adatkezelőnek a kockázat figyelembevételével olyan „technikai és szervezési intézkedéseket – például álnevesítést – kell végrehajtani, amelyek célja egyrészt adatvédelmi elvek, (...) megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.”²²⁹ Ilyen elvek például a WP 29 ajánlása szerint a szükségesség és arányosság elvei, ha a rendszer automatikusan korlátozza az adatokhoz való hozzáférést²³⁰

A LED 21. cikke számos szabályt állapít meg arra az esetre, ha két vagy több adatkezelő közösen határozza meg az adatkezelési műveletek céljait és eszközeit. A bűnüldözés és a büntető igazságszolgáltatás területén működő hatóságoknak a bűncselekmények hatékony felderítése, megelőzése és üldözése érdekében gyakran együtt kell működniük különböző szervezetekkel. Az együttműködés ilyen esetei előfordulhatnak mind ugyanazon szervezeten belüli különálló osztályok között, mind pedig külső szereplőkkel, ügynökségekkel vagy intézményekkel. Ilyen helyzetben megállapodás útján kell meghatározniuk a jogi megfeleléssel kapcsolatos felelősségeiket, kivéve, ha e felelősségeket ehelyett jogi aktus állapítja meg, és ki kell jelölniük egy, az érintettek számára egyetlen kapcsolattartási pontot.

24. cikk értelmében az adatkezelőknek és - kisebb mértékben - az adatfeldolgozóknak nyilvántartást kell vezetniük a felelősségi körükbe tartozó valamennyi adatkezelési kategóriáról. Ezeknek a nyilvántartásoknak többek között a következőket kell tartalmazniuk: tájékoztatás az adatkezelés céljairól, a vonatkozó jogalapról, az adatok megőrzéséről és biztonságáról, az egyéb címzettek részére történő továbbításról, valamint az érintett érintettek

²²⁷ (EU) 2016/680, 19 – 34. cikk.

²²⁸ (EU) 2016/680, Preambulum (61), (62).

²²⁹ (EU) 2016/680, 20. cikk.

²³⁰ WP 258, Vélemény a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv ((EU) 2016/680) egyes kulcsfontosságú kérdéseiről– 17., <https://ec.europa.eu/newsroom/article29/items/610178/en> (2022.07.02.)

és személyes adatok kategóriáiról. Ez a rendelkezés tehát megköveteli, hogy az illetékes hatóságok dokumentálják tevékenységüket, és kérésre képesek legyenek ezeket az információkat a felügyeleti hatóságok rendelkezésére bocsátani.

25. cikk értelmében a tagállamoknak naplózást kell előírniuk az automatizált feldolgozási rendszerekben végzett különböző feldolgozási műveletekről, beleértve legalább a személyes adatok számítógépes rendszerekben történő gyűjtését, módosítását, betekintését, közzétételét, összekapcsolását és törlését. Különösen fontosak a naplóbejegyzések, mivel lehetővé kell tenniük a feldolgozás indoklásának, dátumának és időpontjának megállapítását, valamint - amennyiben lehetséges - azon személyek azonosítását, akik az adatokat megtekintették, közzétették vagy megkapták. Ezeket az információkat kérésre az illetékes hatóságok rendelkezésére kell bocsátani, és kizárólag a feldolgozás jogszerűségének ellenőrzésére, önellenőrzésre, a személyes adatok integritásának és biztonságának biztosítására, valamint büntetőeljárásokhoz használhatók fel. A naplózás egyúttal a bűnüldözési adatfeldolgozás elszámoltathatóságának jelentős eleme és központi szerepet játszik az adatokkal való visszaélések megelőzése érdekében, a megfelelő jogosultsággal rendelkező személyek azonosításában.²³¹

A LED 27. cikke meghatározza az adatvédelmi hatásvizsgálat elvégzésének a hatályát, részleteit és követelményeit a bűnüldözés és a büntető igazságszolgáltatás kontextusában. Előírja, hogy az adatfeldolgozással kapcsolatos hatásvizsgálatra akkor van szükség, ha az adatfeldolgozás típusa - különösen, ha az új technológiák alkalmazásával jár - az adatfeldolgozás jellegét, hatályát, összefüggéseit és céljait figyelembe véve valószínűleg magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Azzal, hogy előírja, hogy erre a vizsgálatra az adatfeldolgozás előtt kerüljön sor, kiegészíti a beépített adatvédelem általános elvét,²³² és mind az adatkezelőknek, mind a rendszerfejlesztőknek egyértelmű lehetőséget biztosít arra, hogy a jövőbeli adatfeldolgozási műveletek kidolgozásának és tervezésének korai szakaszában biztosítékokat építsenek be.

Az V. fejezet - A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása - személyes adatok továbbításaira vonatkozó általános elveket, az

²³¹ Sajfert, J. and Quintel, T. "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities", p.342

²³² Naudts, L. "The Data Protection Impact Assessment for Law Enforcement Agencies" (Adatvédelmi hatásvizsgálat a bűnüldöző szervek számára), előadás a 12. Nemzetközi Kommunikációs Konferencián, Bukarest, Románia, 2018. június 15. Idézi: Assessment of the implementation of the Law Enforcement Directive 2022, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU\(2022\)740209_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf), p.72

adattovábbítást megfelelőségi határozat alapján, az adattovábbítás megfelelő garanciáit, a kivételes esetekben biztosított eltéréseket, a személyes adatok továbbítását harmadik országbeli címzettek részére és a személyes adatok védelmével kapcsolatos nemzetközi együttműködés részletes szabályait fekteti le²³³.

A harmadik országba történő adattovábbítás kritikus kérdése, az adott ország védelmi szintjének megfelelőségi értékelése. A megfelelőséget a Bizottság értékeli az adott ország általános jogszabályrendszere, joggyakorlata, és ítélkezési, jogorvoslati gyakorlata alapján, ideértve a közigazgatási és bírósági jogorvoslatot is.²³⁴ A Bizottság az Európai Unió Hivatalos Lapjában és annak weboldalán teszi közzé a megfelelőségi határozatról szóló jegyzéket.²³⁵ A LED 61. cikkét követően a korábban megkötött nemzetközi megállapodások mindaddig hatályban maradhatnak, amíg azokat nem módosítják, fel nem váltják vagy vissza nem vonják. Amint azt a LED (71) preambulumbekzdése tovább pontosítja, ez magában foglalja azokat a *"jogilag kötelező erejű kétoldalú megállapodásokat"* is, amelyek alapján a tagállamok közvetlen együttműködést folytatnak a külföldi bűnüldöző szervekkel.²³⁶

Kivételes helyzetekben azonban az illetékes hatóságok megállapíthatják, hogy a személyes adatok harmadik országbeli, nem illetékes címzettekkel történő megosztását olyan nyomós közérdek teszi szükségessé, amely indokolja az érintettek jogainak megsértését közvetlen fenyegetés elhárítása vagy bűncselekményre való reagálás érdekében. A LED 39. cikke meghatározza az ilyen aszimmetrikus adattovábbítások általános keretét, és minimumszabályokat állapít meg azon tagállamok számára, amelyek lehetővé teszik illetékes hatóságaik számára az ilyen adatcserét. Ezek az adattovábbítások csak akkor jogszerűek, ha közvetlen fenyegetés elhárításához vagy bűncselekményre való reagáláshoz szükségesek, és ha az adatoknak a helyi illetékes hatóság részére történő továbbítása nem lenne megfelelő.

A VI. fejezet - Független felügyeleti hatóságok – első szakasza a független jogállással, a második szakasza az illetékesség, feladatok és hatáskörök részletes szabályaival foglalkozik, ideértve a kinevezés átláthatóságát, a felügyeleti hatóság létrehozásának általános feltételeit,

²³³ (EU) 2016/680, 35– 40. cikk.

²³⁴ (EU) 2016/680, 36. cikk (1) a), b), c).

²³⁵(EU) 2016/680, 36. cikk (8).

²³⁶ COM (2020) 262 final.

annak szabályait, illetékességét, hatásköreit, tevékenységi jelentéseit.²³⁷ Ezek a feladatok egyúttal a tagállamokra rótt kötelezettségek is a felügyeleti hatóságokkal kapcsolatban.²³⁸

Az adatvédelmi felügyeleti hatóságoknak az EU-ban azonos hatáskörrel kell rendelkezniük ahhoz, hogy a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvben előírt feladataikat el tudják látni. A LED 45. cikkének (2) bekezdése szerint a tagállamoknak ki kell zárniuk a felügyeleti hatóságok hatásköréből a bíróságok által igazságszolgáltatási minőségükben végzett adatkezelési műveleteket. A 80. preambulumbekzdés további betekintést nyújt az előbbi rendelkezés mögött meghúzódó indoklásba, és tisztázza, hogy az a bírák függetlenségének védelmét szolgálja. Az egyéb független igazságügyi hatóságokkal kapcsolatban a preambulumbekzdés megjegyzi, hogy ez olyan szervekre is vonatkozhat, mint az ügyészség.²³⁹

A VII. fejezetben – Együttműködés – a kölcsönös segítségnyújtás és a Testület feladatai kerülnek tárgyalásra. A Testületet az (EU) 2016/679 rendelete hozta létre, mely együttműködik a Bizottsággal, tanácsot ad a személyes adatok Unión belüli védelmével kapcsolatosan, az irányelvvel kapcsolatos feladatai az iránymutatások, módosítások, ajánlások és a legjobb gyakorlat kidolgozása a felügyeleti hatóságok részére.²⁴⁰

A VIII. fejezet - Jogorvoslat, felelősség és szankciók, a IX. fejezet - Végrehajtási jogi aktusok - a X. fejezet - Záró rendelkezéseket tartalmazza.

A jogorvoslat a felügyeleti hatóságnál történő panasztételi jog, a felügyeleti hatósággal szemben bírósági jogorvoslathoz való jog, és az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog.²⁴¹ Az érintettek képviselőt a tagállami

²³⁷(EU) 2016/680, 41– 49. cikk.

²³⁸ A megfelelés adatvédelmi felügyeleti hatóságok általi felügyelete alapvető fontosságú, és a Charta 8. cikkének (3) bekezdésében is szerepel.

²³⁹ A bíróságokkal szemben bírói minőségükben fennálló hatáskörök ugyanilyen korlátozását írja elő a GDPR a rendelet 55. cikkének (3) bekezdése alapján.

A C-245/20. sz. ügyben az EUB úgy ítélte meg, hogy a bíróságok kommunikációs tevékenységével összefüggésben végzett személyes adatok kezelése - ebben az esetben bizonyos dokumentumok újságírók rendelkezésére bocsátása - igazságszolgáltatási jogkörük gyakorlásának minősül, és így nem tartozik a felügyeleti hatóságok hatáskörébe. Bár ezt az ítéletet a GDPR-rel kapcsolatban hozták, értelemszerűen ez az értelmezés a LED-re is ugyanúgy vonatkozik. lásd még: X és Z kontra Autoriteit Persoonsgegevens, 2022. március 24-i ítélet, C-245/20, ECLI:EU:C:2022:216. „Bírósági eljárásból származó, személyes adatokat tartalmazó iratoknak egy újságíró rendelkezésére bocsátása”

²⁴⁰ (EU) 2016/680, 51. cikk.

²⁴¹(EU) 2016/680, 52–54 cikk.

rendeletnek megfelelően létrehozott nonprofit jellegű szerv, szervezet vagy egyesület láthatja el, mely az érintettek jogainak és szabadságainak a személyes adataik vonatkozásában biztosított védelme területén tevékenykedik.²⁴²

A záró rendelkezések fogalmazzák meg a tagállami jogba való átültetés vonatkozó szabályait.²⁴³

„A tagállamok 2018. május 6-ig elfogadják és kihirdetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek.(...)(4) A tagállamok közlik a Bizottsággal a nemzeti jog azon főbb rendelkezéseit, amelyeket az ezen irányelv által szabályozott területen fogadnak el”

2. A bűnügyi irányelv jogharmonizációja

Az Európai Bizottság 2022. július 25-én tette közzé a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv alkalmazásáról és működéséről szóló jelentését.²⁴⁴ Ezt követően értékelő tanulmány készült az Állampolgári Jogi, Bel- és Igazságügyi Bizottság (LIBE) megbízásából, amely a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásának kritikai értékelését tartalmazta²⁴⁵

Az irányelv jogharmonizációs értékeléséről szóló átfogó jelentések áttekintése mellett, a magyar, a német, a francia és svéd jogba történő átültetés példáin keresztül ismertetem az egyes nemzeti jogszabályokba történő átültetés konkrét gyakorlatát, beleértve az adott nemzeti jogrendszerek adatvédelmi történetéhez kapcsolódó összefüggéseket.

A GDPR, az EUDPR és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv hasonló fogalmakon és elveken alapul, ami az uniós adatvédelmi szabályok következetes értelmezését és alkalmazását eredményezi. A LED 62. cikke alapján az Európai Bizottság felülvizsgálati célja annak értékelése volt, hogy szükséges-e a tagállamokba átültetett jogi aktusoknak a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel való további összehangolása. A Bizottság ennek alapján 2020-ban elfogadta „A korábbi harmadik pillérhez tartozó vívmányok adatvédelmi szabályokkal való összehangolásának további lépései” című

²⁴²(EU) 2016/680, 55.cikk.

²⁴³(EU) 2016/680, 63.cikk.

²⁴⁴ Bizottság közleménye az Európai Parlamentnek és a Tanácsnak - Első jelentés a bűnüldözésben érvényesítendő adatvédelemről szóló (EU) 2016/680 irányelv alkalmazásáról és működéséről. COM/2022/364 final.

²⁴⁵ Vogiatzoglou, P. et al. "Assessment of the implementation of the Law Enforcement Directive" Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.209 - December 2022

közleményt²⁴⁶ Ez a közlemény tíz olyan jogi aktust azonosított, amelyeket össze kell hangolni a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel, mert olyan, a személyes adatok védelmére vonatkozó különös rendelkezéseket tartalmaznak, amelyeket a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 60. cikke értelmében a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv nem érint (szerzett jogként elismer), vagy amelyeket nem ismer el szerzett jogként, de nincsenek teljes mértékben összhangban a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel.

A 2022-s bizottsági jelentést,²⁴⁷ az uniós intézmények, a nemzeti felügyeleti hatóságok és a civil társadalmi szervezetek különböző forrásai alapján készítették, az EUDPR alkalmazásáról szóló bizottsági jelentéssel párhuzamosan készült el. Ez utóbbinak fontos eleme a IX. fejezetben meghatározott, a műveleti vonatkozású személyes adatoknak az uniós szervek, hivatalok vagy ügynökségek által a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés hatálya alá tartozó tevékenységek végzése során történő kezelésére vonatkozó szabályok felülvizsgálata is. Ennek keretében a Bizottság jogalkotási javaslatokat tehet, különösen az Europolra és az Európai Ügyészségre vonatkozóan.²⁴⁸

A már említett LIBE kérésére készült tanulmány megállapításai - mely részben a Bizottság jelentésén és más kapcsolódó anyagokon alapulnak²⁴⁹ foglalkozik a LED hatályával, az alapelvekkel, az érintetti jogokkal, az adatkezelői kötelezettségekkel, és a harmadik országokba való továbbításával a jogharmonizáció kapcsán.

A tanulmányok ajánlásokat fogalmazott meg a tagállamok részére,²⁵⁰ valamint a nemzeti illetékes hatóságok és a nemzeti felügyeleti hatóságok részére is. Általánosságban a LED szorosán vett értelmezése korlátozza az érintettek jogait, azonban bizonyos esetekben szükségessé válhat az ettől való eltérés. Fontosnak tartják az információk hozzáférhetőségét és az érintettek jogainak megkönnyítését célzó intézkedések megvalósítását.

Ajánlásokat fogalmazott meg a Bizottság, az EDPB részére is, iránymutatások és ajánlások készítését illetően, számos ezek közül már megvalósult.

²⁴⁶ A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – A korábbi harmadik pillérhez tartozó vívmányok adatvédelmi szabályokkal való összehangolásának további lépései. COM(2020) 262 final, 2020, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A52020DC02622020>. június 24.

²⁴⁷ COM (2022) 364 final, Brüsszel, 2022.7.25.

²⁴⁸ (EU) 2018/ 1725, 98. cikk (2)

²⁴⁹ Vogiatzoglou, P. et al. "Assessment of the implementation of the Law Enforcement Directive," pp. 9-10..

²⁵⁰ Ibid.pp. 9-10.

2.1. A bűnügyi irányelv átültetése a magyar nemzeti jogba

2.1.1. Előzmények ²⁵¹

Magyarországon az 1992. évi LXIII. törvény²⁵² - volt az első adatvédelmi törvény. Előzménye a személyes adatok védelméhez valamint a közérdekű adatok megismeréséhez fűződő jog 1989-es Alkotmány által történő beiktatása az alapjogok sorába. Az 1981-es Európa Tanács egyezmény hazai kihirdetése az 1998. évi VI. törvény²⁵³ - révén történt meg.

A 95/46/EK irányelv magyar jogrendszerbe való átültetése több lépcsőben, első alkalommal 1995-ben valósult meg. Ebben az évben lépett érvénybe az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény, valamint a köziratokról, közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény. Az adatvédelmi törvény második módosítása az 1999. évi LXXII. törvény²⁵⁴ megalkotásával jött létre.

Az Unió 95/46/EK irányelve megfelelésének érdekében, szükségessé vált az adatvédelmi törvény további harmadik módosítása, melyet a 2003. évi XLVIII. törvény valósított meg.²⁵⁵ Ez a módosítás kiterjesztette a személyes adatok kezelésére vonatkozó szabályokat, valamint az adatvédelmi biztos feladatait és jogkörét meghatározó rendelkezéseket, új fogalmakkal bővítve azokat.²⁵⁶

²⁵¹ Gáti Balázs: "Az adatvédelmi jog fejlődésének főbb állomásai."

²⁵² 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

„E törvény célja annak biztosítása, hogy – ha e törvényben meghatározott jogszabály kivételt nem tesz – személyes adatával mindenki maga rendelkezzen, és a közérdekű adatokat mindenki megismerhesse.”

²⁵³ 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

²⁵⁴ 1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

²⁵⁵ 2003. évi XLVIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról

²⁵⁶ Péterfalvi Attila. "Az adatvédelem fejlődésének történeti áttekintése Magyarországon a GDPR hatálybalépéséig." In: Péterfalvi, Attila (szerk.) Szemelvények az információs jogok felügyeletének elmúlt 25 évéből, Budapest, Magyarország: Nemzeti Adatvédelmi és Információs szabadság Hatóság (NAIH), 2020, 29–78. p.50 „A törvény hatálya minden Magyarországon folytatott adatkezelésre és adatfeldolgozásra kiterjed, függetlenül az adatkezelő/feldolgozó állampolgárságára, lakó- vagy székhelyére. A törvény rendelkezéseit a számítástechnikai eszközzel és a manuális módon végzett adatkezelésekre egyaránt alkalmazni kell, nem terjed ki a hatálya azonban a természetes személyeknek a saját céljait szolgáló adatkezeléseire.”

2011-ben az Alaptörvény kimondta a független adatvédelmi felügyeleti hatóság létrehozásának szükségességét, amely az „Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény” (Infotv.)²⁵⁷ alapjául szolgált. Ez a törvény és annak későbbi módosításai integrálták az adatvédelmi jog harmadik generációjának kulcsfontosságú elemeit.

2.1.2. Implementálás a 2011. évi CXII. törvénybe²⁵⁸

A bűnügyi irányelv kötelezettséget teremtett a tagállamok számára a nemzeti jogba történő implementálására meghatározott alkotmányossági és nemzetközi jogi keretek figyelembevételével. Mindezen feltételeknek való megfelelést hivatott biztosítani az Infotv. Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvény (Módtv.)²⁵⁹ A módosító jogszabály 2018. július 26-án hatályba lépett, míg a Nemzeti Adatvédelmi Hatóság (NAIH) adatkezelési engedélyezési eljárására vonatkozó és akkreditációval kapcsolatos módosító rendelkezések 2018. augusztus 25-én léptek hatályba.

Az Infotv. implementálja az általános adatvédelmi rendeletet, amely mindenféle adatkezelési műveletre vonatkozik, kivéve a személyes adatok természetes személy általi kizárólag saját személyes céljait szolgáló adatkezelésekre.²⁶⁰ A GDPR harmonizációja során az ágazati jogszabályokat is módosítani kellett, úgy, mint a Munka Törvénykönyvéről szóló 2012. évi I. törvény, az egészségügyi adatokról szóló 1997. évi XLVII. törvény, a munkabiztonságról szóló 1993. évi XCIII. törvény²⁶¹, az emberi genetikai adatok védelméről szóló 2008. évi XXI. törvény, az állampolgárok személyi adatairól és lakcímnnyilvántartásáról szóló 1992. évi LXVI. törvény, a biztonsági szolgálatokról és a magánnyomozói tevékenységről szóló 2005. évi CXXXIII. törvény, valamint a név- és lakcímadatok kutatási és direkt marketing célú

²⁵⁷ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

²⁵⁸ Gáti Balázs: "Az adatvédelmi jog fejlődésének főbb állomásai."

²⁵⁹ 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról.

²⁶⁰ 2018. évi XXXVIII. törvény 1. §., Infotv. 2. §. 6.

²⁶¹ 1993. évi XCIII. törvény a munkavédelemről

felhasználásáról szóló törvény²⁶², az 1995. évi CXIX. törvény a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok felhasználásáról²⁶³ és a panaszokról és a közérdekű bejelentésekről szóló törvényt.²⁶⁴

A törvény akkor alkalmazandó, ha az adatkezelőnek a tevékenységi központja vagy az Unión belüli egyetlen tevékenységi helye Magyarországon van, vagy ha az adatkezelőnek a tevékenységi központja vagy az Unión belüli egyetlen tevékenységi helye nem Magyarországon van, de az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési művelet meghatározott feltételei fennállnak.²⁶⁵

A 2011. évi CXII. törvény hat fejezetből épül fel, ezek az általános rendelkezések, a személyes adatok védelmére vonatkozó követelmények, az érintett jogai, az adatkezelő és az adatfeldolgozó kötelezettségei, a közérdekű adatok megismerése, a közérdekű adatok közzététele, a Nemzeti Adatvédelmi és Információszabadság Hatóság, a hatóság eljárásai, a bírósági adatkezelési műveletek ellenőrzése és a záró rendelkezések.

A bünyügyi adatok kezelését a törvény második fejezetének a személyes adatok védelmére vonatkozó követelmények 5. pontja alatt az adatkezelés jogalapja és általános feltételei 5. szakaszának (7) bekezdése határozza meg az alábbiak szerint:

„Bűnyügyi személyes adatok kezelése esetén - ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik - a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni”

A törvény hatályával kapcsolatban a 1. szakasz (2) bekezdése sorolja fel az általános adatvédelmi rendelet azon fejezeteit, amellyel kiegészült az Infotv. A (3) bekezdés megállapítja, hogy *„a személyes adatok bűnyildözési, nemzetbiztonsági és honvédelmi célú kezelésére is e törvényt kell alkalmazni.”*

A nemzetbiztonsági és honvédelmi célú adatkezelés tágabb értelemezést jelent az irányelvi meghatározáshoz képest.

²⁶² 1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről. Az Országgyűlés a kutatás célját szolgáló név- és lakcímadatok kezeléséről a következő törvényt alkotja ezzel a törvénnyel.

²⁶³ 1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

²⁶⁴ 2013. évi CLXV. törvény a panaszokról és a közérdekű bejelentésekről, a törvényt a 2023.évi XXV.törvény, 73.§-a hatályon kívül helyezte, és az hatályos 2023.0.25-től.

²⁶⁵ Infotv. 2. § (5) b).

A módosított törvény a további fejezeteiben a kiegészítésekkel a GDPR és a korábbi szabályozás elemeit is tartalmazza,²⁶⁶ valamint a személyes adatok védelmén túl, az információ biztonságot, a felügyeleti hatóságokkal kapcsolatos garanciákat, az eljárási szabályokat is jogszabályba foglalja, ahogy erre a fejezet címe is utalnak.²⁶⁷

A NAIH –l kapcsolatos jogszabályok²⁶⁸ a bírósági adatkezelési műveletek ellenőrzése²⁶⁹ az Infotv.-ben külön fejezetet kapott.²⁷⁰

A bűnüldözési célú adatkezelés fogalmát az alábbiak szerint határozza meg:

„ a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából - ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is - (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése ”²⁷¹

Az Infotv. tehát a bűnügyi személyes adatok kezelésére vonatkozóan főszabály szerint továbbra is a különleges adatok kezelésének feltételeire vonatkozó szabályokat alkalmazza.²⁷²

²⁶⁶ 2018. évi XXXVIII. törvény, 1. § (5) – 5. § (1) – (3), Infotv. 2. § (2)

²⁶⁷ 2018. évi XXXVIII. törvény, 19. § (2a)(2b).

²⁶⁸ Infotv. V. FEJEZET

²⁶⁹ Infotv. VI/A. FEJEZET

²⁷⁰ 2018. évi XXXVIII. törvény, 29. § . Az Infotv. a VI/A. Fejezettel egészült ki, a bírósági adatkezelési műveletek ellenőrzése címmel.

²⁷¹ 2018. évi XXXVIII. törvény, 2. § (6) , Infotv. 3. § 10. a.

²⁷² Bendik Tamás "A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása." p.104. „Ennek indoka, hogy noha az általános adatvédelmi rendelet a „büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatokat” (GDPR 10. cikk) nem a „személyes adatok különleges kategóriáiba” (GDPR 9. cikk) tartozó személyes adatként szabályozza, azok kezelése tekintetében „megfelelő garanciákat nyújtó” tagállami jogi előírások megalkotását írja elő feltételként. Ezen garanciák jellegét és tartalmát azonban a GDPR maga nem határozza meg, így azt az Infotv. - összhangban az ET adatvédelmi

A bűnügyi irányelv adatkezelése az Infotv.-ben a bűnüldözési célú adatkezelések²⁷³ szerint szerepel a korábbi alkalmazásnak megfelelően, elkülönítve azt a személyes adatok büntetőjogi védelmétől.²⁷⁴

A bűnüldözési célú adatkezelés fogalma alatt tehát együttesen határozza meg azokat tevékenységi célokat, melyekhez kapcsolódó adatkezelések az irányelvvel összhangban végezhetők. Kiterjed az adatkezelési cél a szabálysértéssel kapcsolatos tevékenységekre is, valamint az adatkezelést folytató szerv kapcsán külön nevesíti, hogy az adott „személy” is lehet: *(...) a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy*²⁷⁵

A bűnüldözési célú adatkezelésekkel kapcsolatosan az olyan személyes adatok kezelését, amelyeket az érintett kifejezetten nyilvánosságra hozott lehetővé teszi abban az esetben, ha adatkezelés céljának megvalósulásához szükséges és azzal arányos.²⁷⁶

A bűnügyi irányelv az érintettek különböző kategóriához tartozó Preambulum 31.pontjának megfelelő személyes adatainak elkülönítését, a törvény a személyes adatok rendszerezésének kötelezettségével szabályozza:

„Bűnüldözési célú adatkezelés esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó - (...) az általa kezelt személyes adatokat (...) rendszerezi”, akiknél „(...) feltételezhető hogy bűncselekményt vagy szabálysértést követtek el vagy bűncselekményt készülnek elkövetni, (...) akik büntetőjogi vagy szabálysértési felelősségét jogerősen megállapították, (...) akik bűncselekmény vagy szabálysértés sértettjei voltak (...)” és olyan érintettek akik a fentiekkel kapcsolatba hozhatók és ezekről információval szolgálnak.²⁷⁷

egyezmény 6. cikkében meghatározottakkal - lényegét tekintve az adatvédelmi reformot megelőző szabályozással megegyező tartalommal rendezi”

²⁷³ Infotv. 3. § (10) a.)

²⁷⁴ A személyes adatok büntetőjogi védelme elleni bűncselekményeket nem az Infotv., hanem a Büntető Törvénykönyvről szóló 2012. évi C. törvény rendeli büntetni.

²⁷⁵ Infotv. 3. § (10). a.) A bűnügyi irányelv 3. cikk. 7. pont alatt az illetékes hatóságok között meghatározott „egyéb jogalany” fogalmának megfelelően.

²⁷⁶ Infotv. 5. § (1) d). Az érintettnek tisztában kell lennie, azzal, hogy ezek az adatok nyilvánosak, és bárki számára elérhetők.

²⁷⁷ 2018. évi XXXVIII. törvény, 5. §, Infotv. 7. § (1).

Az érintetti jogokkal kapcsolatban a továbbiakban kiemelném azokat a jogokat, melyben az Infotv. konkrétan megjeleníti azokat a korlátozásokat, amelyek a bűnüldözési célú adatkezelésekkel kapcsolatosak, és amelyeket az Irányelv 23. cikke együttesen tárgyal.²⁷⁸

A tájékozódáshoz való jog: a törvény 14. szakaszának a) pontja rendelkezik az "*előzetes tájékoztatáshoz való jogról*". Az érintettek jogainak megkönnyítésére vonatkozó általános követelményeket a törvény 15. szakasza, míg az előzetes tájékoztatáshoz való jogra vonatkozó különös követelményeket a törvény 16. szakasza tartalmazza.²⁷⁹

A tájékoztatás teljesítését az elérni kívánt céllal arányosan azonban az adatkezelő késleltetheti, a tájékoztatás tartalmát korlátozhatja vagy a tájékoztatást mellőzheti, ha ezen intézkedése elengedhetetlenül szükséges:

- az adatkezelő által vagy részvételével lefolytatott vizsgálatok, különösen büntetőeljárások hatékony és eredményes lefolytatása,
- a bűncselekmények hatékony és eredményes megelőzése és felderítése,
- a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtása
- a közbiztonság hatékony és eredményes védelme,
- az állam külső és belső biztonságának, különösen a honvédelemnek és a nemzetbiztonságnak a hatékony és eredményes védelme, vagy
- harmadik felek alapvető jogainak védelme érdekében.²⁸⁰

A törvény 14. szakaszának b) pontja a hozzáférési jogról rendelkezik. Az érintettek jogainak megkönnyítésére vonatkozó általános követelményeket a törvény 15. szakasza, míg a hozzáférési jogra vonatkozó konkrét követelményeket a törvény 17. szakasza tartalmazza. (mint a tájékoztatási joggal kapcsolatban is) Az adatkezelő a kívánt céllal arányosan korlátozhatja vagy elutasíthatja a hozzáférési jog érvényesítését, ha ez az intézkedés feltétlenül

²⁷⁸ (EU) 2016/680 5.szakasz, 23.cikk, (1) : Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az (...) szükséges és arányos intézkedés egy demokratikus társadalomban.

²⁷⁹ 2018. évi XXXVIII. törvény, 9. §, Infotv. 16. § (1)

²⁸⁰ Infotv. 16. § (3)

szükséges annak biztosításához. A feltételek azonosak a tájékoztatási joggal kapcsolatban leírtakkal.²⁸¹

A törvény 14. szakaszának e) pontja rendelkezik a törléshez való jogról. Az érintettek jogainak megkönnyítésére vonatkozó általános követelményeket szintén a törvény 15. szakasza, míg a törléshez való jogra vonatkozó konkrét követelményeket a törvény 20. szakasza tartalmazza. A törléshez való jog korlátozása esetében ugyanúgy a már felsorolt korlátozások, így köztük, a bűncselekmények hatékony és eredményes megelőzése és felderítése, és a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtása szerepelnek. Az adatkezelés tartama a cél elérésének szükségessége.²⁸²

Ha az adatkezelő elutasítja az érintettnek az általa vagy az adatkezelő nevében eljáró vagy általa utasított adatfeldolgozó által kezelt személyes adatok helyesbítésére, törlésére vagy kezelésének korlátozására irányuló kérelmét, haladéktalanul írásban értesítenie kell az érintettet.²⁸³ Az elérni kívánt céllal arányosan az adatkezelő késleltetheti a felmondásról szóló tájékoztatás teljesítését, valamint a jogi és ténybeli okokat, korlátozhatja a tájékoztatás tartalmát, vagy eltekinthet a tájékoztatás nyújtásától, ha ez elengedhetetlen.²⁸⁴

A törvény 6. szakasza előírja a kizárólag automatizált feldolgozáson alapuló döntésekre vonatkozó követelményeket. Kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés, amely az érintett személyére vagy jogos érdekeire nézve hátrányos következményekkel jár, vagy őt jelentős mértékben érintő joghatással jár, csak akkor hozható meg, ha törvényben vagy az Európai Unió kötelező erejű jogi aktusában erre kifejezett felhatalmazás rendelkezik.²⁸⁵ Ezenkívül feltétel, hogy nem sérti az egyenlő bánásmód követelményét, az adatkezelő vagy az adatkezelő nevében eljáró vagy általa utasított

²⁸¹ Infotv. 17. § (3), E törvény alkalmazása esetén, esetén az adatkezelő haladéktalanul írásban tájékoztatja az érintettet arról, hogy (Törvény 17. § (4) bekezdés): a hozzáférés korlátozásának vagy megtagadásának ténye, valamint annak jogi és ténybeli indokai, ha az érintett tájékoztatása nem hátráltatja a meghatározott érdek érvényesítését; és az érintettet a törvény alapján megillető jogokat, valamint azok érvényesítésének módját, így különösen az érintettnek a NAIH-n keresztül történő hozzáférési jog gyakorlásához való jogát.

²⁸² „Főszabályként, a személyes adatokat addig lehet kezelni, ameddig a kezelésük megfelel annak a célnak, amelyből gyűjtötték azokat. Amennyiben az adatkezelés célja megszűnik, a személyes adatokat törölni kell, kivéve, ha a további kezelésüket törvény előírásai teszik szükségessé, és az összeegyeztethető a kezelésük a felvételük eredeti céljaival is. Ezek az előírások megfelelnek a magyar Infotv. általános adatvédelmi szabályozásának is a célhoz kötöttség szempontjából.” Lásd: Magyarázat a GDPR-ról 392.o

²⁸³ Infotv. 21. § (1).

²⁸⁴ Infotv. 21. § (2). A 16. § (3) bekezdés a)–f) pontjában meghatározott valamely érdek biztosításához.

²⁸⁵ Infotv. 6. §

adattfeldolgozó kérésére tájékoztatja az érintettet a döntéshozatali mechanizmus során alkalmazott módszerről és kritériumokról valamint az érintett kérésére emberi beavatkozás alkalmazásával felülvizsgálja a döntés eredményét. Ugyancsak kritérium, hogy Európai Unió törvénye vagy kötelező erejű jogi aktusa másként nem rendelkezik, és a döntéshozatal során nem használnak fel különleges adatokat.

Az adattovábbítás feltételei²⁸⁶ között részletesen szabályozza a bűnüldözési célú adatkezelés esetén nemzetközi adattovábbítás feltételeit a korlátozásokkal együtt.²⁸⁷ Az EU/EGT valamely tagállamába történő adattovábbítás nem igényel további megfelelő biztosítékokra vagy eltérésekre való szabályozást.

A GDPR-ral összhangban az adatkezelők vagy adattfeldolgozók személyes adatokat továbbíthatnak harmadik országbeli adatkezelőknek vagy adattfeldolgozóknak, ha: az adattovábbítás az Európai Bizottság megfelelőségi határozatán alapul²⁸⁸, az adattovábbításra megfelelő biztosíték vonatkozik (pl. kötelező erejű vállalati szabályok ("BCR"), az átruházó és a kedvezményezett által kötött általános szerződési feltételek, ez nem foglalhatja magában az ismétlődő adatkezelési műveleteket, és csak korlátozott számú érintettet érinthet.

Bűnüldözési célú adatkezelés esetén nemzetközi adattovábbításra a 10. szakasz (1) bekezdésben meghatározott feltételek teljesülése esetében is csak akkor kerülhet sor, amennyiben:

- *„az bűnüldözési célból szükséges, annak címzettje bűnüldözési adatkezelést folytató szerv,*
- *vagy nem bűnüldözési adatkezelést folytató szerv és meghatározott feltételek teljesülnek²⁸⁹,*
- *valamint nemzetközi adattovábbítással érintett személyes adatnak valamely EGT-állam adatkezelőjétől történő átvétele esetén, akkor, ha azt a nemzetközi adattovábbítást, ezen személyes adatok tekintetében az EGT-állam adatkezelője vagy képviselőjében eljáró más szerv vagy személy előzetesen jóváhagyta, vagy a közvetett*

²⁸⁶ Infotv. 8. § - 13. §, 13. §,(2) : Nemzetközi adattovábbítás az általános adatvédelmi rendelet 96. cikkében, valamint a 2016/680 (EU) irányelv 61. cikkében meghatározott nemzetközi szerződések alapján az azokban meghatározott célokból, feltételekkel és adatkörben – azok módosításáig, megszüntetéséig, megszűnéséig vagy alkalmazásuk felfüggesztéséig – az e törvényben meghatározott feltételek hiányában is végezhető.

²⁸⁷ 2018. évi XXXVIII. törvény, 6. § , Infotv. 10. § (2) -12. § (2)

²⁸⁸ Az Európai Bizottság az (EU) 2016/679 rendelet 45. cikke alapján jogosult meghatározni, hogy egy EU-n kívüli ország megfelelő szintű adatvédelmet biztosít-e.

²⁸⁹ Infotv. 11. § (3).szerint

adattovábbítás kivételével – a nemzetközi adattovábbítás Magyarország vagy valamely más EGT-állam alapvető érdekeit vagy ezen államok vagy harmadik ország közbiztonságát fenyegető súlyos és közvetlen veszély megelőzése érdekében szükséges és az előzetes jóváhagyás beszerzése²⁹⁰ ezen érdekek sérelme nélkül a nemzetközi adattovábbítást megelőzően nem lehetséges.²⁹¹”

Az Infotv. a hetedik fejezet záró rendelkezések alatt szabályozza a 2018. évi XXXVIII. törvény 31. szakasz alapján az (EU) 2016/680 európai parlamenti és tanácsi irányelvnek való megfelelést, a 77. § d) pont alatt. Ugyanitt szabályozza a 2018. évi XXXVIII. törvény 32. szakasza alapján az (EU) 2016/679 rendelet szerint az ezzel kapcsolatban az Infotv. 77/A. §-a helyébe lépő új rendelkezéseket.²⁹²

Összefoglalva a bűnügyi irányelv alkalmazásai tekintetében a jogharmonizációs kötelezettség a tagállami jogba való törvényi beépítést írta elő, a jogalkotó a korábbi szabályozási megközelítést megtartotta, a bűnügyi irányelv rendelkezéseit beépítette az Infotv. – be, az általános adatvédelmi rendelettel együtt. Az Infotv. tételesen azonban nem különíti el, hanem egységes szerkezet alatt tárgyalja a bűnügyi irányelv rendelkezéseit.

Az Infotv. ilyen módon teljes körűen implementálja az adatvédelmi csomagot és átfogó szabályozásra törekszik, háttérszabályokat is biztosítva.

2.2. A bűnügyi irányelv átültetése a német nemzeti jogba

A bűnügyi irányelv szabályait a tagállami jogalkotóknak a nemzeti jogba át kell ültetniük, azok közvetlenül nem alkalmazandók. Az irányelv - a GDPR-ral szemben - nem a teljes jogegységesítésre, hanem a tagállami jogok harmonizációjára törekszik. *„Ez az irányelv nem akadályozza meg a tagállamokat abban, hogy az érintettek jogainak és szabadságainak védelme érdekében a személyes adatok illetékes hatóságok által végzett kezelésére az ezen irányelvben megállapítottnál magasabb védelmi szintet biztosító garanciákról rendelkezzenek.”²⁹³*

²⁹⁰ Infotv. 10. § (2). ca.)

²⁹¹ Infotv. 10. § (2).

²⁹² Megállapította: 2018. évi XXXVIII. törvény 32. §. Hatályos: 2018. VII. 26-tól

²⁹³ (EU) 2016/680, 1. cikk (3).

Németország volt az első EU-tagállam, amely a GDPR-t a német szövetségi adatvédelmi törvény keretén belül - Bundesdatenschutzgesetz²⁹⁴ (BDSG) – a nemzeti jogszabályába foglalta, amely 2018. május 25-én lépett hatályba, és amely a bűnüldözésre vonatkozó adatvédelmi irányelvet is átültette, és ennek kapcsán módosított a BDSG-ben felsorolt számos más vagy egyéb szövetségi törvényt.

2.2.1. Előzmények

Németország, pontosabban Hessen tartomány is adatvédelmi történelmet írt. Mint ismeretes a világ első adatvédelmi törvénye itt jött létre.²⁹⁵ 1970. október 13-án lépett hatályba, és válasz volt az állami szervek egyre hatékonyabb automatizált információ feldolgozására. Hessen számítógéppel támogatott adatgyűjtést tervezett a kórházakban és iskolákban. A felelősök számára gyorsan világhírűvé vált: ahol annyi személyes adatot gyűjtenek össze, az egyes polgárok gyorsan úgy érezhetik, hogy megfigyelik és ellenőrzik őket. Az azóta többszörösen felülvizsgált hesseni tartományi adatvédelmi törvény többek között azt írta elő, hogy az elektronikusan feldolgozott adatokat védeni kell az illetéktelen hozzáféréstől. Kötelezte az adatkezelésben részt vevőket az adatok tartalmának titokban tartására, és lehetővé tette a téves adatok helyesbítését. Az adatvédelmi tisztviselő kinevezése is hesseni „találmány”.

Körülbelül hat évvel a hesseni adatvédelmi törvény után a szövetségi kormány követte a példáját. A német szövetségi adatvédelmi törvény első változatát 1977. január 27-én fogadták el „Die erste Fassung des deutschen Bundesdatenschutzgesetzes”²⁹⁶ (BDSG) - (Törvény az adatfeldolgozás során a személyes adatokkal való visszaélés elleni védelemről²⁹⁷) címmel. Célja, hogy megakadályozza a kormányzati szervek, és a vállalatok korlátozás nélkül felhasználhassák a személyes adatokat. Ezért megállapították, hogy az ilyen adatok

²⁹⁴ "Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU)," Deutscher Bundestag, <https://dip.bundestag.de/vorgang/gesetz-zur-anpassung-des-datenschutzrechts-an-die-verordnung-eu-2016-679/79680>.

²⁹⁵Das Hessische Beamtenengesetz in der Fassung vom 16. Februar 1970. URL: <http://starweb.hessen.de/cache/GVBL/1970/00041.pdf>.

²⁹⁶Bundesgesetzblatt, hatályba lépett 1978. január 1-én. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl177s0201.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl177s0201.pdf%27%5D__1708963582035.

²⁹⁷ saját fordítás

feldolgozása csak akkor engedélyezett, ha az érintett ehhez hozzájárult, vagy a szövetségi adatvédelmi törvény vagy más jogszabály ezt lehetővé teszi. Ezen túlmenően az adatkezelés során a szükségesség elvét kell követni, ezentúl csak olyan személyes adat kezelhető, amely a feladatok ellátásához elengedhetetlen. 1977-ben büntetendő volt a személyes adatok jogosulatlan továbbítása, módosítása, visszakeresése. Egy év börtönbüntetést vagy pénzbüntetést is kiszabhattak. Ha azonban az elkövető szándékosan cselekedett, a börtönbüntetés két évre meghosszabbítható volt, vagy ismételten pénzbírsággal sújtható volt. 1978. január 1-én hatályba lépett szövetségi adatvédelmi törvény 17. szakasza előírja az adatvédelmi szövetségi biztos kinevezését.

1981-ig Németország összes régi szövetségi állama fokozatosan felzárkózott, és hatályba léptette saját állami adatvédelmi törvényeit. Az adatvédelem mérföldköve volt az 1983-as népszámlálási határozat, amellyel a Szövetségi Alkotmánybíróság részben alkotmányellenesnek nyilvánította a tervezett népszámlálást.²⁹⁸ Garanciákat tartott szükségesnek ahhoz, hogy az egyén alapvetően maga dönthesse el, hogyan használja fel adatait. A korábbi adatvédelmi törvények már nem feleltek meg ennek a követelménynek, 1990-ben a módosítások megtörténtek.

A 95/46/EK adatvédelmi irányelv átültetése is tartományi szinten kezdődött meg. Hessen és Brandenburg tartomány reagált először, 1998-ban, illetve 1999-ben adatvédelmi törvényeiket az EU követelményeihez igazították. 2001 májusától hatályba léphetett a felülvizsgált szövetségi adatvédelmi törvény. 2006. január 1-én pedig hatályba lépett az információszabadságról szóló törvény, amely feltétlen jogot biztosít minden személynek az összes szövetségi hatóság hivatalos információinak megtekintésére. A Szövetségi Adatvédelmi Biztos²⁹⁹ egyben az Információszabadság Szövetségi Biztosa is, és gondoskodik e törvény rendelkezéseinek betartásáról.

²⁹⁸ A Német Szövetségi Alkotmánybíróság ítéletében (Volkszählungsurteil) alkotmányellenesnek mondta ki a népszámlálási törvényt. A népszámlálási-ítélet deklarálta az ún. információs önrendelkezési jogot, azaz a polgárok azon jogát, hogy az adataik felhasználhatósága, kezelése kapcsán maguk rendelkezhetnek.

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

²⁹⁹ Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

https://www.bfdi.bund.de/DE/Home/home_node.html

2.2.2. A német szövetségi adatvédelmi törvény az adatvédelmi reform után ³⁰⁰

Az új német szövetségi adatvédelmi törvény (*Bundesdatenschutzgesetz* – "BDSG") elfogadásával hozzáigazították a korábbi német jogi keretet a GDPR-hoz. A BDSG a GDPR-ral együtt lépett hatályba 2018. május 25-én.

2019. november 26-án hatályba lépett az adatvédelmi törvénynek az (EU) 2016/679 rendelethez és az (EU) 2016/680 végrehajtási irányelvhez történő hozzáigazításáról szóló második törvény (a második adatvédelmi kiigazítási törvény)³⁰¹. A második adatvédelmi kiigazítási törvény tovább módosította a BDSG-t, és módosított 154 másik szövetségi törvényt - mindegyik szerepel a második adatvédelmi kiigazítási törvényben - hogy összeegyeztesse azokat a GDPR-ral, és a LED-el. A 16 tartomány mindegyike új állami adatvédelmi törvényt fogadott el a GDPR szerint, és számos ágazatspecifikus adatvédelmi kötelezettséget módosított más állami törvényekben, például a kórházi törvényekben.

A BDSG-n kívül több más adatvédelmi szabály létezik a területspecifikus törvényekben, például a pénzügyi kereskedelmet vagy az energiaszektort szabályozó jogszabályokban. 2021. december 1-jétől a távközlési-telemédia-adatvédelmi törvény (*Telekommunikation-Telemedien-Datenschutzgesetz* – "TTDSG ") olyan adatvédelmi szabályozást ír elő a távközlési és telemédia-szolgáltatók számára, amelyek célja, hogy kiküszöböljék a régóta fennálló jogbizonytalanságot a távközlési és telemédia-szolgáltatók számára. A német távközlési törvény (*Telekommunikationsgesetz* – "TKG ") és a német telemédiatörvény (*Telemediengesetz* – "TMG") adatvédelmi előírásai a GDPR-ral kölcsönhatásban értelmezendők.

A TTDSG az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése szerinti „cookie-hoz való hozzájárulás” követelményét is átülteti a német jogba.

A német szövetségi adatvédelmi törvény IV. részből, és 7 fejezetből és 86 szakaszból épül fel. Az I. rész Közös rendelkezések címszó alatt a törvény hatályát, és a fogalommeghatározásokat tartalmazza az első fejezetben ³⁰², a második fejezet a személyes adatok feldolgozásának

³⁰⁰ Version information: "The English translation includes the amendments to the Act by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045)."

³⁰¹ Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU), Gesetz vom 20.11.2019 – BGBl. I 2019, Nr. 41 vom 25.11.2019, S. 1626

³⁰² BDSG 1. § (1), (2)

jogalapját, ezen belül a személyes adatok állami szervek általi feldolgozását, és a nyilvánosan hozzáférhető helyek videó megfigyelését tárgyalja.³⁰³

A törvény személyi hatálya kiterjed a Szövetség állami szerveire, a tartományok állami szerveire, különösen azokra az esetekre, amikor a tartományi jogszabályok nem szabályozzák az adatvédelmet. Ezen felül magában foglalja azokat az állami szerveket is, amelyek szövetségi törvények végrehajtásával foglalkoznak, vagy igazságügyi szervként működnek a közigazgatási ügyektől eltérő esetekben, valamint azon magánszervezeteket, amelyek igazságügyi szervként járnak el.³⁰⁴

A törvény területi hatálya az állami szervekre terjed ki, továbbá érinti a magánszervezeteket is abban az esetben, ha az adatkezelő vagy adatfeldolgozó a személyes adatokat Németország területén kezeli. Ezenfelül alkalmazandó azokra a helyzetekre is, amikor a személyes adatok feldolgozása az adatkezelő vagy adatfeldolgozó németországi tevékenységével áll kapcsolatban, illetve akkor is, ha az adatkezelő vagy adatfeldolgozó nem rendelkezik telephellyel az Unió vagy az EGT valamely tagállamában, de a tevékenysége az GDPR hatálya alá esik.³⁰⁵

Az adatkezelés jogalapjáról a törvény 3. szakasza rendelkezik. Az állami szervek abban az esetben jogosultak személyes adatokat kezelni, amennyiben az ilyen típusú adatkezelés szükséges az adatkezelő által ellátott feladatok végrehajtásához vagy a rájuk ruházott hivatalos hatáskör gyakorlásához.³⁰⁶

A fogalommeghatározások alatt a Szövetség köztestületeinek, a tartományok köztestületeinek, a magánszerv, és a magánszervezet fogalmait értelmezi.

A nyilvánosan hozzáférhető területek optikai-elektronikai eszközökkel történő megfigyelése esetében³⁰⁷ a törvény értelmezése szerint a gyűjtött adatok tárolása vagy felhasználása akkor megengedett, ha az a cél eléréséhez szükséges, és ha semmi nem utal az érintettek jogos nyomós érdekére. Az adatok más célból csak akkor kezelhetők tovább, ha az állam- és közbiztonság veszélyeztetésének megelőzése, valamint a bűncselekmények üldözése érdekében szükséges. Ha a videokamerás megfigyelés során gyűjtött adatokat egy adott személyhez kötik, az érintett

³⁰³ BDSG 1. § (3), (4)

³⁰⁴ BDSG 1. § (1)

³⁰⁵ BDSG 1. § (4)

³⁰⁶ BDSG 3. §

³⁰⁷ BDSG 3. § (1),(3)

személyt az (EU) 2016/679 rendelet 13. és 14. cikkének megfelelően tájékoztatni kell az adatkezelésről, e törvény 32. §-a megfelelően alkalmazandó.^{308,309}

A harmadik fejezet részletesen foglalkozik a közttestületek adatvédelmi tisztviselőinek kijelölésével, szerepkörének meghatározásával és feladatainak körülírásával. E fejezet különös hangsúlyt fektet az adatvédelmi tisztviselők feladatbővítésére, és utal a törvény 67. és 69. szakaszaira. Ezek a szakaszok az adatvédelmi hatásvizsgálat elvégzését és a felügyeleti hatósággal történő egyeztetési kötelezettségeket részletezik.

A negyedik fejezetben a törvény az adatvédelemért és az információszabadságért felelős szövetségi biztos (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) – mint legfelsőbb szövetségi hatóság kompetenciáit, kinevezését, hivatali idejét, jogait, kötelezettséget, és feladatait határozza meg, valamint a tevékenységi jelentéseket és a hatáskörét³¹⁰. A 14. szakasz kiemeli, hogy a szövetségi biztos az (EU) 2016/680 irányelv hatálya alatt a 60. cikke szerinti feladatot is ellátja.³¹¹

A Szövetségi Biztos döntései ellen vagy abban az esetben, ha eljárási kötelezettségének nem tesz eleget az alábbiak szerint élhetnek jogorvoslattal az érintettek:

- A BDSG 61.§ (1) bekezdése szerint más jogorvoslati lehetőségek érintetlenségének megőrzése mellett minden természetes vagy jogi személynek joga van jogorvoslattal élni a Szövetségi Biztos által hozott jogerős döntés ellen.³¹²
- A BDSG 61§ (1) bekezdése megfelelően alkalmazandó az adatalanyokra is, ha a Szövetségi Biztos nem foglalkozik a panasszal a 60. cikk értelmében, vagy nem

³⁰⁸ BDSG (3. § 4)

³⁰⁹ A magánszervezetek videó megfigyelését illetően is kötelező a német Szövetségi Közigazgatási Bíróság döntése alapján a GDPR 6. cikke (1) bekezdésének f) pontjának alkalmazása. A vitatott BDSG 4. szakasz (1) bekezdése szerint: videós megfigyeléshez a nagy, nyilvánosan hozzáférhető létesítmények, például sportlétesítmények, gyülekező- és szórakozóhelyek, bevásárlóközpontok és parkolók, vagy járművek és nagy, nyilvánosan hozzáférhető vasúti, hajó- vagy autóbuzsközlekedési létesítmények esetében a jelenlévő személyek életének, egészségének és szabadságának védelmét nagyon fontos érdeknek kell tekinteni.

³¹⁰ BDSG 5. § – 16. §

³¹¹ (EU) 2016/680 a 60.§. „Változatlanul hatályban maradnak a büntetőügyekben folytatott igazságügyi együttműködés és a rendőrségi együttműködés területén 2016. május 6-án vagy azt megelőzően hatályba lépett, a személyes adatok védelmére vonatkozó uniós jogi aktusok olyan különös rendelkezései, amelyek a tagállamok közötti adatkezelést és a kijelölt tagállami hatóságoknak a Szerződések alapján létrehozott, ezen irányelv hatálya alá tartozó információs rendszerekhez való hozzáférését szabályozzák.”

³¹² BDSG 61.§ (1)

tájékoztatja az adatalanyt a panasz előre haladásáról vagy eredményéről három hónapon belül.³¹³

Az ötödik fejezet az Európai Adatvédelmi Testületben történő képviselétről szól,³¹⁴ a hatodik fejezet a jogorvoslati lehetőségeket szabályozza.³¹⁵

Németországnak szövetségi adatvédelmi hatósága és 16 állami adatvédelmi hatósága is van, amelyek mindegyike a GDPR hatálya alá tartozik. Az adatvédelmi szövetségi szabályozás fő szerve továbbra is a bonni BfDI marad. A BfDI hatáskörébe tartozik a Szövetség állami szerveinek és a távközlési szolgáltatóknak a felügyelete, és közös képviselőként és egyetlen kapcsolattartóként Németországot képviseli az Európai Adatvédelmi Testületben. Ezen túlmenően mindegyik német tartomány továbbra is rendelkezik egy szabályozó hatósággal, amely az adatvédelmi jogszabályok magánszervezetek általi alkalmazásának ellenőrzéséért felelős a területén³¹⁶ A magánszervezetek szemszögéből a „fő szabályozó” az az illetékes állami hatóság, amely a GDPR-nak való megfelelés szerinti ellenőrzésre illetékes.³¹⁷

A BfDI feladatait illetően kiemelném az (EU) 2016/680 irányelv végrehajtására elfogadott jogszabályokat.³¹⁸ Ez vonatkozik az érintett tájékoztatására, az érintett, illetve az 2016/680 irányelv 55. cikkével összhangban valamely szerv, szervezet vagy egyesület által benyújtott panaszok kezelése, valamint a panasz tárgyának a megfelelő mértékben történő kivizsgálására, a megfelelő hatóságokkal kapcsolatos együttműködésre.

A jogkörök, kötelezettségek és felelőségekkel kapcsolatban a BfDI hatáskörébe tartozik a Szövetség állami szerveinek felügyelete.³¹⁹ A BDSG 16. szakasza előírja, hogy a BfDI rendelkezik a GDPR 58. cikkében említett hatáskörökkel.³²⁰

³¹³ BDSG 61.§ (2)

³¹⁴ BDSG 17 .§ – 19.§

³¹⁵ BDSG 20.§ – 21.§

³¹⁶ BDSG 40. §

³¹⁷ A fő telephelyet a GDPR 4. cikkének (16) bekezdése szerint kell meghatározni, amely fő telephelyként a központi ügyintézés helyét jelöli ki, kivéve, ha az adatkezelés céljaira vagy módjaira vonatkozó döntéseket egy másik telephelyen hozzák meg, amely szintén rendelkezik határozatok végrehajtására vonatkozó hatáskörrel, amely esetben az a telephely a fő telephely.

³¹⁸ BDSG 14. §.(5) (6) (7) (8)

³¹⁹ BDSG 9. §.

³²⁰ BDSG 16.§.Ha szövetségi biztos arra a következtetésre jut, hogy az adatvédelmi jogszabályokat megsértették, vagy a személyes adatok feldolgozásával kapcsolatban egyéb problémák merülnek fel, erről tájékoztatja az illetékes hatóságot. Az (EU) 2016/679 rendelet 58. (2) b)–g), i) és j) pontja alapján lehetőséget kell biztosítani

A BDSG 14. szakasza a BfDI feladatainak hosszú listáját sorolja fel, és tisztázza, hogy ezek kiegészítik a GDPR-ban foglalt feladatokat.

A BDSG II. része Az (EU) 2016/679 rendelet 2. cikkének megfelelő célú adatkezelésre vonatkozó végrehajtási rendelkezéseket tartalmazza.³²¹ A törvény 6 fejezet cím alatt tárgyalja ezeket: a személyes adatok kezelésének jogalapja, (két alfejezettel: 1. alfejezet - a személyes adatok különleges kategóriáinak feldolgozása és egyéb célú feldolgozás, 2. alfejezet-különleges feldolgozási helyzetek), az érintett jogai, adatkezelők és adatfeldolgozók kötelezettségei, felügyeleti hatóságok a magánszervezetek által végzett adatkezelések esetében a büntetések és a jogorvoslat.

A kulcsfogalmak, a jogalapok, a beleegyezés, az érintettel történő szerződés, a jogi kötelezettségek, az érintett érdekei, a közérdek, az adatkezelő jogos érdekeit illetően nincs eltérés a GDPR-tól.

A magánszervezetekre vonatkozó jogalapokkal kapcsolatban a személyes adatokat az adatgyűjtés céljától eltérő célból kezelhetik, ha: az adatkezelés az állam- vagy közbiztonságot fenyegető veszélyek megelőzése vagy a bűncselekmények üldözése érdekében szükséges, vagy a feldolgozás polgári jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges, kivéve, ha az érintettnek nyomós érdeke fűződik ahhoz, hogy az adatokat ne kezeljék.³²²

A munkavállalói adatok feldolgozása esetében a német jogalkotó a GDPR 88. cikkében foglalt nyitózáradékot használta, és meghatározta a munkavállalói adatok feldolgozásának jogalapját.³²³ A „munkavállaló” fogalmát a BDSG 26. § (8) bekezdése határozza meg, a további szabályozás nem teljesen feleltethető meg a GDPR 88.cikkének.³²⁴

ennek a hatóságnak, hogy ésszerű határidőn belül véleményt nyilvánítson az adatkezelő részére. A véleményezési lehetőség mellőzhető, ha az azonnali döntés közvetlen veszély vagy közérdek miatt szükségesnek tűnik, vagy kényszerítő közérdekbe ütközne. A véleménynek tartalmaznia kell a szövetségi biztos tájékoztatása alapján hozott intézkedések leírását is.

³²¹ BDSG 22. § - 44.§

³²² BDSG 24. §

³²³ BDSG 26. §. (1)- (2)

³²⁴ 2023 márciusában az EUB a Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium kontra Minister des Hessischen Kultusministeriums ügyben (C-34/21) hozott ítéletében úgy határozott, hogy a személyes adatok feldolgozására vonatkozó nemzeti jogszabályok a munkavállalók foglalkoztatási vonatkozású adatainak továbbra is alkalmazhatatlanok, ha nem felelnek meg a GDPR 88. cikkének (1) és 88. cikkének (2) bekezdésében meghatározott feltételeknek és korlátoknak

A személyes adatok különleges kategóriáinak kezelése során az (EU) 2016/679 rendelet 9. cikkének (1) bekezdésétől eltérve a személyes adatok különleges kategóriáinak kezelése engedélyezett meghatározott feltételek esetén.^{325,326} A különleges adatkategóriák és a büntetőítéletre vonatkozó adatok kezelésére vonatkozó nemzeti szabályozás esetében a BDSG nem tartalmaz szabályokat a büntetőítéletre vonatkozó adatok kezelésére.

A BDSG számos eltérést tartalmaz a GDPR 9. cikkében meghatározott speciális adatkategóriák feldolgozásának általános tilalma alól. Ezeket a következő kategóriába lehet sorolni: általános eltérések és a tudományos vagy történelmi kutatási, statisztikai, közérdekű archiválási és foglalkoztatási célú adatkezeléssel kapcsolatos különleges eltérések. A BDSG, a GDPR 9. cikkétől eltérve úgy rendelkezik, hogy a személyes adatok különleges kategóriáinak tudományos vagy történelmi kutatási vagy statisztikai célú hozzájárulás nélkül történő feldolgozása megengedett, ha az ilyen feldolgozás ezekhez a célokhoz szükséges, és az adatkezelőnek az adatkezeléssel kapcsolatos érdekei lényegesen felülmúlják az érintettek adatkezelésének mellőzésével kapcsolatos érdekeit, bizonyos szigorú feltételek mellett.³²⁷

Az érintetti jogokkal kapcsolatban a német jogalkotó az alábbiak szerint élt a GDPR 89. cikkének (2) és (3) bekezdésében biztosított eltérési lehetőséggel. A BDSG 27. § (2) bekezdése előírja, hogy tudományos vagy történelmi kutatási vagy statisztikai célú adatkezelés esetén az érintettek alábbi jogai olyan mértékben korlátozottak, amennyiben ezek a jogok valószínűleg lehetetlenné teszik vagy súlyosan sértik az adatkezelést: hozzáférési jog (GDPR 15. cikk), helyesbítéshez való jog (GDPR 16. cikk), az adatkezelés korlátozásához való jog (GDPR 18. cikk) és a tiltakozás joga (GDPR 21. cikk). A korlátozás csak oly mértékben szükséges, amely a kutatási vagy statisztikai célok elérése, és a kutatási vagy statisztikai célok teljesítéséhez szükségesek. Ugyanez vonatkozik a BDSG 28. § (2-4) bekezdése alapján a közérdekű archiválási célú adatkezelés bizonyos körülmények közötti eseteire.

A tájékoztatási joggal kapcsolatban a törvény felsorolja azokat a körülményeket, amikor a GDPR 13. illetve 14. cikke értelmében nem kell információt szolgáltatni az érintetteknek. Ezek a körülmények nagyon specifikusak és korlátozottak.³²⁸

³²⁵ BDSG 22. §,(1)

³²⁶ BDSG 22. § (1) : általános eltérésként rendelkezik arról, hogy a személyes adatok különleges kategóriáinak feldolgozását állami és magánjogi szervek is engedélyezik.

³²⁷ BDSG 27. §, 28. §.

³²⁸ BDSG 29 . §, 32. §, és 33. §, A GDPR 13. cikkével kapcsolatban az ilyen korlátozások csak azokra az esetekre vonatkoznak, amikor az adatkezelő az adatokat az adatgyűjtés eredeti céljától eltérő célból kívánja feldolgozni. A

Az adatokhoz való hozzáférést illetően a német szövetségi törvény további korlátozásokat ír elő a GDPR 15. cikkével kapcsolatban.³²⁹

A törlési joggal kapcsolatban a BDSG előírja, hogy az érintettet nem illeti meg törlési jog a nem automatizált adatkezelés esetén, ha a törlés a tárolás módjából adódóan lehetetlen vagy aránytalan erőfeszítéssel járna, feltéve, hogy az érintett érdeke a törlést illetően minimálisnak tekinthető, és az adatok kezelése jogszerűen történt. Ekkor a törlési jog helyett a feldolgozás korlátozása érvényesül.³³⁰

A BDSG a GDPR 21. cikke értelmében az érintettek tiltakozási jogát korlátozza, amennyiben előírja, hogy a közérdekű archiválási célú adatkezelés esetén nem áll fenn az adatkezelés elleni tiltakozás, amennyiben az az archiválási cél elérését lehetetlenné teszi vagy súlyosan akadályozza, és a korlátozás szükség az adathordozhatósághoz való jogról

Az adathordozhatósághoz való joggal kapcsolatban megállapítja, hogy a közérdekű archiválási célú adatkezelés esetén a GDPR 20. cikke alapján biztosított adathordozhatósághoz való jog nem áll fenn, amennyiben az lehetetlenné teszi vagy súlyosan csorbítja az adatkezelést, az archiválási célok elérése érdekében, és a korlátozás e célok teljesítéséhez szükséges.³³¹

A szankciókkal kapcsolatban általános szabályként a GDPR szerinti szankciókat kell alkalmazni, azonban büntető rendelkezéseket is tartalmaz. A büntető rendelkezéseket a törvény a 42. szakaszban tételesen szabályozza beleértve a szabadságvesztés tényét is, nem csak a pénzbüntetést.

A szövetségi adatvédelmi törvény III. része az (EU) 2016/680 irányelv 1. cikkének (1) bekezdése szerinti célból történő adatfeldolgozásra vonatkozó végrehajtási rendelkezéseket tartalmazza.

GDPR 14. cikkével kapcsolatban a BDSG 29. szakaszának (1) bekezdése előírja, hogy a tájékoztatási kötelezettség nem áll fenn, amennyiben e kötelezettség teljesítése olyan információt hozna nyilvánosságra, amelyet természeténél fogva titokban kell tartani, különösen harmadik fél nyomós jogos érdekei miatt. A BDSG 33. §-a kimondja, hogy a tájékoztatási kötelezettség nem vonatkozik arra az esetre, ha az információs szolgáltatás akadályozná a jogi igények előterjesztését, érvényesítését vagy védelmét, vagy a feldolgozás magánjogi szerződésekből származó adatokat tartalmaz, és célja a bűncselekményekből eredő károk megelőzése, kivéve, ha az érintettnek nyomós jogos érdeke fűződik az információ megszerzéséhez.

³²⁹ BDSG 34. § (1)

³³⁰ BDSG 35. § (1). Ezeket a korlátozásokat bírálta az Európai Bizottság a jogalkotási folyamat során, de a vonatkozó német rendelkezések csak annyiban minősíthetők GDPR eltérésnek, amennyiben a a GDPR nem automatizált feldolgozás szerinti tárgyi hatálya alá tartoznak.

³³¹ BDSG 28. § (4)

Az 1. fejezet a személyes adatok feldolgozásának hatálya, fogalommeghatározásai és általános elveit, a 2. fejezet a személyes adatok feldolgozásának jogalapját, a 3. fejezet az érintett jogait a 4. fejezet az adatkezelők és adatfeldolgozók kötelezettségeit, 5. fejezet az adattovábbítás harmadik országoknak és nemzetközi szervezeteknek, a 6. fejezet a felügyeleti hatóságok közötti együttműködést, a 7. fejezet a felelősség és szankciókat szabályozza.³³²

A német BDSG a 45. szakasza (EU) 2016/680 irányelv hatályával kacsoltban egyértelműen megjelöli az irányelv szerinti bűnügyi adatkezelési célt: *„E rész rendelkezéseit kell alkalmazni a személyes adatoknak a bűncselekmények megelőzésére, kivizsgálására, felderítésére vagy büntetőeljárás alá vonására, illetve büntetőjogi vagy közigazgatási szankciók végrehajtására illetékes állami szervek által végzett adatkezelésre, amennyiben az adatkezelés célja ezeknek a feladatoknak a végrehajtása. Ebben az esetben az állami szerveket adatkezelőnek kell tekinteni. Az első mondatban említett bűncselekmények megelőzése magában foglalja a közbiztonságot fenyegető veszélyek elleni védelmet és azok megelőzését.”*

Arról is rendelkezik, hogy ez a hatály a szövetségi adatvédelmi biztosra és hivatalára is vonatkozik, tehát - *„a 11. § (1) bekezdésében említett szankciók, intézkedések végrehajtásáért felelős állami szervekre is vonatkozik”*³³³. A LED németországi végrehajtásakor például az úgynevezett Ordnungswidrigkeitenre³³⁴ is alkalmazhatóvá vált, amely nem büntetőjogi szabálysértésnek minősül, és csak pénzbírság formájában kiszabott közigazgatási szankciókkal sújtható.

A német jogalkotó követi a bűnügyi irányelv megfelelő kategóriáit, az egyes fejezetek tartalmazzák az uniós normákat, a GDPR- nál említett korlátozásokkal és kiegészítésekkel, a büntető rendelkezéseknél visszautalva szintén az ott megadott szabályozásra.

Az adattovábbítás általános követelményeit a törvény 78. szakasza szabályozza, az alábbi módon. Ha az adattovábbításra vonatkozó minden egyéb feltétel teljesül, a személyes adatok harmadik országbeli szervnek vagy nemzetközi szervezetnek történő továbbítása megengedett, ha

- a Testület vagy nemzetközi szervezet felelős a 45. szakaszban említett célokért³³⁵ és

³³² BDSG 45.§ - 86.§

³³³ Ezt kell alkalmazni azokra az állami szervekre is, amelyek a büntetések, a Büntető Törvénykönyv 11. § (1) bekezdésének 8. pontjában említett intézkedések, a fiatalkorúak bíróságáról szóló törvényben említett nevelési vagy fegyelmi intézkedések vagy pénzbírságok végrehajtásáért felelősek.

³³⁴ közigazgatási szabálysértés

³³⁵ EDPB, Európai Bizottság

- az Európai Bizottság az (EU) 2016/680 irányelv 36. cikkének (3) bekezdése alapján megfelelési határozatot fogadott el.³³⁶
- A személyes adatok továbbítása megfelelési határozat ellenére sem megengedett, ha - a BDSG 2. szakaszát, valamint az adattovábbításhoz fűződő közérdeket kell figyelembe véve - az egyedi esetben nem biztosítható, hogy az adatokat az adatvédelmi jogszabályoknak megfelelően és az alapvető emberi jogokkal összhangban kezeljék.^{337,338}

Adattovábbítás megfelelő biztosítékokkal³³⁹ és az adattovábbítás megfelelő biztosítékok nélkül³⁴⁰ megfelelnek az (EU) 2016/680 irányelv 37. és 38. cikkeinek. Az egyéb adattovábbítás harmadik országbeli címzettek részére megfelel az irányelv 39. cikkének, a BDSG 81. szakasz (4) rögzíti azonban, hogy az (1) bekezdés szerinti adattovábbítás esetén az átadó adatkezelő kötelezi a címzettet, hogy az átadott személyes adatokat az adatkezelő hozzájárulása nélkül csak abból a célból kezelje, amelyből azokat továbbították.

A LED 40. cikkével kapcsolatos elveket pontosítja és részletezi a német jogalkotó a kölcsönös segítségnyújtás kapcsán³⁴¹ az alábbi módon:

A szövetségi biztos az (EU) 2016/680 irányelv következetes végrehajtásához és alkalmazásához,

- szükséges mértékben tájékoztatást és kölcsönös segítségnyújtást nyújt az Európai Unió többi tagállamának felügyeleti hatóságai számára. A kölcsönös segítségnyújtás kiterjed különösen az információ kérésekre és a felügyeleti intézkedésekre, mint például a konzultációk, vizsgálatok és vizsgálatok lefolytatására irányuló megkeresésekre,³⁴²

³³⁶ BDSG 45.§ (1)

³³⁷ BDSG 45.§ (2)

³³⁸ BDSG 45.§ (3)-(4) (3) Ha az (1) bekezdés szerint az Európai Unió másik tagállamából továbbított vagy hozzáférhetővé tett személyes adatot kell továbbítani, a másik tagállam illetékes szervének előzetesen engedélyeznie kell az továbbítást. Az előzetes engedély nélküli továbbítás csak akkor engedélyezhető, ha az átadás egy ország közbiztonságát vagy valamely tagállam alapvető érdekeit fenyegető közvetlen és súlyos fenyegetés megelőzése érdekében szükséges, és az előzetes engedély nem szerezhető be időben.

³³⁹ BDSG 80.§

³⁴⁰ BDSG 81.§

³⁴¹ BDSG 82.§

³⁴² BDSG 82.§ (1)

- minden szükséges intézkedést megtesz annak érdekében, hogy a kölcsönös segítségnyújtás iránti megkeresésre haladéktalanul, de legkésőbb a kérelem kézhezvételétől számított egy hónapon belül válaszoljon,³⁴³
- csak akkor tagadhatja meg a kérelem teljesítését, ha nem illetékes a megkeresés tárgyára vagy az általa végrehajtandó intézkedésekre, vagy a felszólítás teljesítése jogszabályba ütközne,³⁴⁴
- tájékoztatja a másik állam megkereső felügyeleti hatóságát az eredményekről, illetve adott esetben a kérelemre válaszul hozott intézkedések előre haladásáról. A kérelem teljesítésének megtagadását indokolnia kell,³⁴⁵
- a másik állam felügyeleti hatósága által kért információkat rendszerint elektronikus úton, szabványos formátumban adja meg,³⁴⁶
- a kölcsönös segítségnyújtás megkeresése alapján tett intézkedésért nem számít fel díjat, kivéve, ha a másik állam felügyeleti hatóságával az egyedi ügyben a felmerült költségek megtérítésében megállapodott,³⁴⁷ és a
- segítségnyújtás iránti kérelmének tartalmaznia kell minden szükséges információt, beleértve különösen a megkeresés célját és indokait. A kicserélt információ csak arra a célra használható fel, amelyre azt kérték.³⁴⁸

A felelősség és szankciók tekintetében a kártérítésre a német polgári törvénykönyv. szabályait³⁴⁹ kell alkalmazni.³⁵⁰

A BDSG 86. szakasza előírja, hogy a köz- és magánszervezetek személyes (beleértve az érzékeny) adatokat nemzeti kitüntetések és kitüntetések céljára az érintett tájékoztatása nélkül is feldolgozhatnak.

Összefoglalva a német szövetségi adatvédelmi törvény második módosítása együttesen implementálja az uniós jog két fő pillérét, az általános adatvédelmi rendeletet és a bűnügyi adatvédelmi irányelvet, a GDPR tekintetében néhány eltéréssel, mely a LED-re is ugyanúgy vonatkozik.

³⁴³ BDSG 82.§ (2)

³⁴⁴ BDSG 82.§ (3)

³⁴⁵ BDSG 82.§ (4)

³⁴⁶ BDSG 82.§(5)

³⁴⁷ BDSG 82.§ (6)

³⁴⁸ BDSG 82.§ (7)

³⁴⁹ Bürgerliches Gesetzbuch (BGB), Gesetze im Internet, <https://www.gesetze-im-internet.de/bgb/>

³⁵⁰ BDSG 83.§

2.3 A bűnügyi irányelv átültetése a francia nemzeti jogba³⁵¹

Franciaországban 2018 júniusban hirdették ki, és lépett hatályba a 2018. június 20-i 2018-493. számú törvény³⁵², a francia adatvédelmi jogszabály módosítása.

A jogszabály szintén együttesen rendelkezik a GDPR, és a bűnügyi irányelv átültetéséről. A francia törvény- a magyar jogszabályhoz hasonlóan - elsősorban a GPDR nemzeti végrehajtásával kapcsolatos rendelkezéseket tartalmazza, és ehhez képest különíti el a bűnügyi célú adatkezelést.

2.3.1 Előzmények

Történetileg Franciaországban az 1978-as adatvédelmi törvény az első, amely egyúttal létrehozta a francia adatvédelmi hatóságot, a „la Commission Nationale de l'Informatique et des Libertés (CNIL) - t.”³⁵³ Az 1974-ben az úgynevezett „SAFARI” botrányt követően léptették életbe a francia közigazgatás azon terve kapcsán, hogy társadalombiztosítási számon keresztül összekapcsolják a névleges fájlokat, így szükség volt a személyes adatok felhasználásának szabályozására.³⁵⁴

Ez a francia adatvédelmi törvény az 1978. január 6-i 78-17. számú törvény „Az adatkezelésről, a fájlokról és a szabadságjogokról”³⁵⁵, melyek egyes cikkeit, rendelkezéseit már az uniós adatvédelmi reform előtt is módosították, többek között a személyes adatok védelméről szóló 95/46/EK irányelv végrehajtásáról szóló 2004. augusztus 6-i 2004-801 számú törvénnyel.³⁵⁶

³⁵¹ Gáti Balázs. "A bűnügyi adatvédelmi irányelv átültetése a tagállami jogrendszerekbe." Szakdolgozat, Eötvös Loránd Tudományegyetem, Állam- és Jogtudományi Kar, Jogi Továbbképző Intézet, 2022.

³⁵² LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1)

³⁵³ A Számítástechnikai és Szabadságjogok Nemzeti Bizottsága (saját fordítás)

³⁵⁴ "France - Data Protection Overview," DataGuidance, <https://www.dataguidance.com/notes/france-data-protection-overview> (hozzáférés: 2022.07.12.).

³⁵⁵ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (a magyar cím saját fordítás), <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/> (2022.07.04)

³⁵⁶ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1), <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676/> (2022.07.12.)

Franciaországban a 2016-1321 számú „A digitális köztársaságról szóló törvény”³⁵⁷ előrevetítette az általános adatvédelmi rendeletet, az elektronikus szolgáltatásokra vonatkozó az adatgazdaság, az online adatok védelmének, és a digitális hozzáférés jogszabályainak megalkotásával.³⁵⁸

A személyes adatok védelméről szóló, 2018-493 számú törvény módosította - az Alkotmánytanács 2018-765 DC határozata alapján, a 78-17. számú törvényt, mely az adatvédelmi uniós reform végrehajtása érdekében jött létre.

A törvény szerkezeti felépítése szerint öt címmel bővült, melyek közül az első kettő az (EU) 2016/679 Rendeletéhez kapcsolódik, a III. Cím alatt (EU) 2016/680 Irányelvének hatékony végrehajtásáról szóló rendelkezések találhatók a 29 – 30 cikk alatt.

Maga a törvény szakaszonként tartalmazza az egyes fejezeteket kiegészítő szövegeket, így ezek épültek be a korábbi szabályozásba. A módosított törvény együtt volt értelmezendő a GDPR rendelkezéseivel mivel több, a GPDR-ral kapcsolatos rendelkezést ekkor még nem ültetett át, úgy mint az adathordozhatósághoz való jog, adatvédelmi hatásvizsgálatok elvégzésének kötelezettsége, illetve a tengerentúli területek esetében eltérő hatállyal rendelkezett a nemzeti jogszabály. A módosító törvény 32. cikke felhatalmazta a kormányt, hogy rendelettel folytassa annak általános átírását annak érdekében, hogy javítsa az érthetőséget és a személyes adatok védelmével kapcsolatos jogszabályokkal való összhangot.

2019. június 1- je óta az 1978. január 6-i „Informatique et Libertés”³⁵⁹ törvény új változatban van hatályban.³⁶⁰ Tartalmazza a korábbi módosító törvény említett hiányosságait. Az Informatique et Libertés törvény nem hivatott teljes mértékben lefedni a GDPR rendelkezéseit, sok esetben azonban kifejezetten hivatkozik rájuk. A csak a GDPR hatálya alá tartozó szabályozások esetében a jogi keret megfelelő értelmezése azt jelenti, hogy a GDPR-t és a 2019.

³⁵⁷LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique , https://www.legifrance.gouv.fr/loda/article_lc/JORFARTI000033202902/ (2022.07.12)

³⁵⁸ France – „Data Protection Overview”

³⁵⁹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, <https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624/#LEGIARTI000006528059>,(hozzáférés: 2022.07.12)

³⁶⁰ A 2018. december 12-i 2018-1125 számú rendelet és a 2019. május 29-i 2019-536 számú rendelet írta át a 2018. június 20-i 2018-493 számú törvényt, és lépett hatályba az 1978. január 6-i 78-17. sz., az adatkezelésre, a fájlokra és szabadságjogokra vonatkozó tv. második módosítása. A 2018. december 12-i rendelethez hasonlóan a 2019. május 29-i rendelet is a nemzeti jogi keret olvashatóságának javítását, valamint a szabályozási rendelkezések európai joggal és az annak alkalmazása érdekében hozott nemzeti jogszabályi intézkedésekkel való összhangba hozását célozta.

június 1-én módosított törvényt együtt kell értelmezni. A 2019-s adatvédelmi törvény teljes körűen alkalmazható valamennyi Franciaországhoz tartozó tengerentúli területen is.

2.3.2. A francia adatvédelmi törvény első módosítása, az 1978. január 6-i 78-17. számú törvényhez

A francia adatvédelmi hatóság, a CNIL ³⁶¹ honlapja szerint, az első módosított törvény a GDPR-ral ellentétes rendelkezéseket megszüntette és kiegészítette a szükséges rendelkezésekkel, beleértve a következőket.^{362,363}

A francia adatvédelmi szabályozás módosításai jelentős hatáskör-bővülést hoztak CNIL számára. A CNIL új, nem kötelező erejű jogi eszközöket, mint például iránymutatásokat, ajánlásokat, magatartási kódexeket, mintaszabályzatokat, referenciamódszereket dolgozhat ki vagy ösztönözheti azok kidolgozását (1. cikk). Az adatvédelmi tisztviselők hatásköreinek kibővítése mellett (5. cikk), a CNIL tisztviselői jogosultak lettek ellenőrzési és vizsgálati jogköröket gyakorolni más tagállamok adatvédelmi hatóságaival közösen végzett ellenőrzési műveletek során, ha ezek Franciaország területén zajlanak (6. cikk). Az intézkedések és szankciók megerősítését is tartalmazta a módosítás (7. cikk).

Ezenfelül a törvény kiterjesztette az érzékeny adatok definícióját, beleértve a biometrikus és genetikai adatokat is, megerősítve az érzékeny adatok feldolgozásának GDPR által előírt tilalmát (8. cikk). A korábbi előzetes alaki követelmények jelentős részét eltörölték, helyettük az adatkezelési műveletek adatvédelmi hatásvizsgálatának kötelezettségét vezették be, különös tekintettel azokra az esetekre, amikor az adatkezelés nagy kockázatot jelent az egyének jogaira és szabadságaira (11. cikk).

A nemzeti jog alkalmazásának pontosítása (10. cikk) értelmében a tagállamok eltérő jogszabályai esetén, ha az érintett Franciaországban rendelkezik lakóhellyel, a francia jog az irányadó, még akkor is, ha az adatkezelő nem rendelkezik telephellyel Franciaországban. Az

³⁶¹ A Számítástechnikai és Szabadságjogok Nemzeti Bizottsága (saját fordítás)

³⁶² CNIL, <https://www.cnil.fr/fr/entree-en-vigueur-de-la-nouvelle-loi-informatique-et-libertes> (2022.07.12)

³⁶³ A 2018. augusztus 3-án közzétett első végrehajtási rendelet, a 2018. augusztus 1-jei 2018-687. számú rendelet meghatározza a CNIL szervezetét és működését. Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037277401> / (2022.07.12.)

információszabadság és a véleménynyilvánítás szabadsága tekintetében azonban az adatkezelő letelepedési helyének jogszabálya az irányadó.

A bírósági határozatok újra felhasználói nyílt adatalapú megközelítést alkalmazhatnak (13. cikk), ahol a bűncselekményekre vonatkozó adatokat úgy teszik hozzáférhetővé a nyilvánosság számára, hogy közben az érintettek magánéletét tiszteletben tartják, és elemzik az újbóli azonosítás kockázatait. Az online beleegyezés korhatára 15 év lett a „digitális nagykorúság” tekintetében (20. cikk). A csoportos kereset hatályát kiterjesztették a kártérítésre (25. cikk). A Conseil d'Etat jogosult ideiglenesen felfüggeszteni a nemzetközi adattovábbítást, ha a CNIL ezt indokoltnak tartja (27. cikk).

2.3.3. A francia adatvédelmi törvény második módosítása, az 1978. január 6-i 78-17. számú törvényhez

A törvény jelenleg öt cím köré szerveződik, amelyek a következőkre vonatkoznak:

I. Közös rendelkezések: Itt a GDPR direkt hivatkozásaival együtt kerülnek meghatározásra a személyes adatvédelem alapfogalmai. Ez magában foglalja a törvény hatályát, az adatvédelmi elveket, az érzékeny adatok speciális szabályait, a CNIL szervezeti és működési szabályait, valamint a vonatkozó büntetőjogi előírásokat (1–41. cikkek).

II. A GDPR szerinti adatkezelési előírások: Ez a csoport a GDPR által előírt adatkezelési szabályokat tartalmazza (42-86. cikkek).

III. Adatkezelés a bűnüldözés területén: A személyes adatok kezelésének szabályai a bűnüldözés során, amelyek az (EU) 2016/680 irányelven alapulnak (87–114. cikkek).

IV. Állambiztonsági adatkezelés: Specifikus szabályok az állambiztonsági és védelmi tevékenységek adatkezelésére (115-124. cikkek).

V. Tengerentúli szabályozás: Személyes adatok kezelésére vonatkozó előírások, amelyek Franciaország tengerentúli területeire terjednek ki (125–128. cikkek).³⁶⁴

Az alábbiakban kiemelem a közös rendelkezések néhány aspektusát, amelyek a III. cím, azaz a bűnüldözési célú adatkezelés szempontjából is irányadók.

³⁶⁴ A személyes adatok védelméről szóló törvény 2018. június 20-i frissítése előtt a GDPR-t és a francia adatvédelmi törvényt különböző módon alkalmazták Franciaországban és annak különböző tengerentúli területi egységeiben. A 2019. június 1-jei hatálybalépéssel ez az eltérés megszűnt: a francia tengerentúli területekre a francia adatvédelmi törvény V. címe értelmében mostantól ugyanaz a jogi keret vonatkozik, mint a francia anyaországra.

A törvény személyi hatályának tekintetében előírja, hogy a személyes adatok kezelése esetén mindig e törvény rendelkezéseit kell alkalmazni, függetlenül attól, hogy az adatkezelő vagy adatfeldolgozó jogi vagy természetes személy, illetve hogy köz- vagy magánszemély.³⁶⁵

Területi hatály szempontjából a módosított jogszabály a Franciaországban letelepedett adatkezelők vagy adatfeldolgozók tevékenységével összefüggésben végzett adatfeldolgozásokra vonatkozik, attól függetlenül, hogy maga az adatkezelés Franciaországon belül történik-e.³⁶⁶ Az európai uniós jogszabályok alapján bevezetett kiegészítő nemzeti előírások minden esetben alkalmazandók, ha az adatalany Franciaországban tartózkodik, még abban az esetben is, ha az adatkezelő nem Franciaországban van bejegyezve.³⁶⁷

A CNIL, a GDPR jelentése és alkalmazása szerinti nemzeti felügyeleti hatóság.³⁶⁸ A fogalmak nagy részét nem határozza meg, hivatkozik a GDPR adott cikkeire.³⁶⁹ Az alapelvek a GDPR-nak megfelelőek.³⁷⁰

A törvény a GDPR 33. cikkére hivatkozik a CNIL-nek történő adatvédelmi incidens bejelentésére vonatkozóan.³⁷¹

A személyes adatok különleges kategóriáinak kezelése meghatározott kivételekkel tilos.³⁷²

A büntetőítéletekkel a törvény 46. cikke foglalkozik. Az ilyen adatkezelést végezhetik:

- joghatóságok, hatóságok és közszolgáltatást irányító jogi személyek,
- az igazságszolgáltatás segédtisztviselői (például közvetítők vagy szakértők) feladataik szigorú gyakorlására, valamint az igazságügyi szervezetekkel együttműködő szervezetek,
- természetes vagy jogi személyek, hogy lehetővé tegyék számukra, hogy sértettként, vádlottként vagy nevükben bírósági eljárást készítsenek elő, és adott esetben kezdeményezzenek és nyomon kövessék azt, és végrehajtsák a meghozott határozatot
- az áldozatoknak segítséget nyújtó egyesületek az Igazságügyi Minisztériummal kötött megállapodás alapján,
- az általuk kezelt szellemi tulajdonjogok vagy a szellemi tulajdonjogok megsértésének áldozatai nevében eljáró közös jogkezelő szervezetek, és

³⁶⁵ Informatique et Libertés, Article 8. I.

³⁶⁶ Informatique et Libertés, Article,3. I.- II.

³⁶⁷ Informatique Liberté n°78-17, 3. cikk II. szakasz

³⁶⁸ Informatique et Libertés, Article 2. I.

³⁶⁹ Informatique et Libertés, Article 1- 7.

³⁷⁰ Informatique et Libertés, Article 4.

³⁷¹ Informatique et Libertés, Article 58.

³⁷² Informatique et Libertés, Article 6. kivételek: Article 44.

- a bírósági határozatokban foglalt nyilvános információk újrafelhasználói, feltéve, hogy a feldolgozásnak nem célja, és nem is jár azzal, hogy lehetővé tegye az érintett személyek újbóli azonosítását.³⁷³

Az érintetti jogoknál³⁷⁴ az általános adatvédelmi rendeletre hivatkozik. A GDPR 23. cikkével összhangban, amely mérlegelési jogkört biztosít a tagállamoknak a GDPR 12–22. és 34. cikkében biztosított jogok korlátozására, a GDPR 14. cikke szerinti tájékoztatáshoz való jog nem alkalmazandó, ha a gyűjtött adatokat az állam nevében és a közbiztonság érdekében végzett feldolgozásra használják fel.³⁷⁵

A tájékoztatáshoz való jog ilyen korlátozása azonban csak annyiban alkalmazható, amennyiben az, az adatkezelés mögött meghúzódó céloknak való megfeleléshez szükséges. Ez a korlátozás akkor is alkalmazandó, ha az adatkezelést hivatalos feladatokért felelős hatóságok végzik, mint például az adó- és vámigazgatás vagy természetes vagy jogi személyek tevékenységének ellenőrzése, ami jogsértés felderítéséhez és szankció kiszabásához vezethet. Az adatalany jogainak GDPR és LED szerinti korlátozása esetén az adatkezelő tájékoztatja az adatalanyt arról a lehetőségről, hogy jogait a CNIL-en keresztül érvényesítheti. A GDPR szerinti meghatározott esettől eltekintve, az adatkezelő szintén tájékoztatja az adatalanyt a bírósági jogorvoslat igénybevételének lehetőségéről.³⁷⁶

A törvény konkrét kivételeket is biztosít az érintettek jogainak teljes körű alkalmazása alól, ha az adatkezelés közérdekű archiválási célok, tudományos és történelmi kutatás vagy statisztikai célok,³⁷⁷ újságírói, irodalmi vagy művészi alkotási cél,³⁷⁸ vagy bűncselekmények megelőzése, kivizsgálása és büntetőeljárás alá vonása esetében történik.³⁷⁹

A hozzáférési jog, a bűncselekmények megelőzésével, kivizsgálásával, felderítésével vagy büntetőeljárás alá vonásával, illetve az állam nevében hozott büntetőjogi szankciók vagy szabadságelvonással járó végzések végrehajtásával kapcsolatos adatkezelés tekintetében nem

³⁷³ Informatique et Libertés, Article 46. Megjegyzés: A digitális köztársaságról szóló, 2016-1321. sz. törvény már előírta egy előzetes tanulmány végrehajtását annak ellenőrzése érdekében, hogy az adatok közzéteskor lehetséges-e a személyek újbóli azonosítása.

³⁷⁴ Informatique et Libertés, Article 48.

³⁷⁵ Informatique et Libertés, Article 48.

³⁷⁶ Informatique Liberté n°78-17, 107. cikk IV. szakasz

³⁷⁷ Informatique et Libertés, Article 79.

³⁷⁸ Informatique et Libertés, Article 80.

³⁷⁹ Informatique et Libertés, Article 107., 108.

korlátozott, kivéve, ha a személyes adatokat bírósági határozat vagy bírósági akta tartalmazza.³⁸⁰ A törvény ezt a kivételt a szükséges és arányos mértékben írja elő.

A nyomozások, vizsgálatok vagy közigazgatási vagy bírósági eljárások akadályozásának elkerülése, a bűncselekmények megelőzésének, felderítésének, kivizsgálásának vagy üldözésének, illetve a büntetőjogi szankciók végrehajtásának akadályozásának elkerülése, és a közbiztonság, nemzetbiztonság, mások jogainak és szabadságainak védelme érdekében az adatkezelő megtagadhatja vagy korlátozhatja az érintett hozzáférési jogát.

A helyesbítési és törlési érintetti jogoknál is érvényes a kivétel a teljes körű alkalmazás alól bűncselekmények megelőzése, kivizsgálása és büntetőeljárás alá vonása esetén, ugyanakkor a CNIL a helyesbítési útmutatásai szerint az érintett nem kérheti a rendőrségi, csendőrségi és hírszerzési iratok helyesbítését. Az ilyen akták tekintetében a CNIL bírója felelős azért, hogy az érintett nevében elvégezze a szükséges javításokat.³⁸¹

A törlési jogokkal kapcsolatban a törvény 106. cikke rendelkezik a bűnügyi nyomozással kapcsolatban az adatkezelés korlátozásáról.

Az érintetti jogokkal kapcsolatban a kivételek közé minden esetben beletartozik a bűnügyi célú adatkezelés.

Az automatikus adatkezeléssel kapcsolatban a GDPR rendelkezései az irányadók, a kivételeket illetően is. Az érintettnek joga van ahhoz, hogy ne terjedjen ki rá olyan bírósági határozat hatálya, amely magában foglalja egy személy viselkedésének értékelését a személyes adatok automatizált feldolgozása alapján, amelynek célja a személyiségével kapcsolatos szempontok értékelése.³⁸² Nincsenek azonban ilyen korlátozások az állambiztonsággal - és védelemmel kapcsolatos adatkezelésre,³⁸³ valamint a bűncselekmények megelőzése, kivizsgálása és üldözése céljából végzett adatkezelésre vonatkozóan.³⁸⁴

³⁸⁰ A törvény konkrét kivételeket is biztosít az érintettek jogainak teljes körű alkalmazása alól, ha az adatkezelés célja: bűncselekmények megelőzése, kivizsgálása és büntetőeljárás alá vonása.

³⁸¹ A helyesbítéshez való jog nem vonatkozik az irodalmi, újságírói vagy művészeti feldolgozásra sem.

³⁸² Informatique et Libertés, Article 47. Ezen kívül kivételek még, a francia jogszabályoknak megfelelően meghozott egyedi adminisztratív határozatok, feltéve, hogy az adatkezelés nem érint a törvény 6. cikkében említett érzékeny adatokat, és az adatkezelő gondoskodik az algoritmikus feldolgozás és annak fejlesztéseinek ellenőrzéséről, hogy magyarázatot tudjon adni az adatkezelésre. az érintettel kapcsolatban az adatkezelés módjára.

³⁸³ Informatique et Libertés, Article 120.

³⁸⁴ Informatique et Libertés, Article 95. A törvény 95. cikke hozzáteszi, hogy tilos minden olyan profilalkotás, amely a személyes adatok különleges kategóriái alapján megkülönbözteti a természetes személyeket.

Az adattovábbítási gyakorlatot illetően, a GDPR-nak való megfelelés érdekében több iránymutatás is készült még az EDPB³⁸⁵ és a CNIL³⁸⁶ részéről is. Franciaországban főszabály szerint tilos az EGT-régió kívülrre történő adattovábbítás, kivéve, ha a GDPR V. fejezete szerinti biztosítékot alkalmaznak. Ha a Bizottság nem ad ki határozatot arról, hogy egyes EGT-n kívüli országok megfelelő szintű védelmet biztosítanak, a személyes adatokat az EGT-n kívülrre továbbító adatfeldolgozóknak általában végrehajtható szerződéses megállapodásokra³⁸⁷ kell támaszkodniuk az adatok GDPR V. fejezetével összhangban történő védelme érdekében. A francia adatvédelmi törvény III. része az (EU) 2016/680 rendelettel kapcsolatos szabályozást tartalmazza.

Négy fejezetből áll, ezek, az I. fejezet: általános rendelkezések (87 – 96.cikk), a II. fejezet: az illetékes hatóságok, a személyes adatfeldolgozók és az alvállalkozók kötelezettségei (97 – 103 cikk), a III. fejezet: az érintett jogai (104 – 111 cikk), és a IV. fejezet: személyes adatok továbbítása az Európai Unióhoz nem tartozó államokba vagy az Európai Unióhoz nem tartozó államokban letelepedett címzettek részére (112 – 114 cikk).

Az adatkezelés célja a bűnüldözési célból történő adatkezelés, az illetékes hatóságok által.³⁸⁸

Az általános rendelkezések cikkei az irányelvi szabályozástól nem különböznek.

A szabályozás szigorúbb, ha az adatkezelést az állam nevében hajtják végre az előbbi célok legalább egyike céljából a következők szerint: a személyes adatok állam nevében történő kezelését a CNIL indokolással ellátott és közzétett véleményét követően az illetékes miniszter engedélyezi, állambiztonsági, védelmi vagy közbiztonsági érdekből, vagy a bűncselekmények megelőzése, kivizsgálása, megfigyelése vagy üldözése, illetve büntetőítéletek vagy biztonsági intézkedések végrehajtása céljából.³⁸⁹³⁹⁰

³⁸⁵ EDPB. "05/2021 Iránymutatás a 3. cikk alkalmazása és az általános adatvédelmi rendelet V. fejezete szerinti, nemzetközi adattovábbításra vonatkozó rendelkezések közötti kölcsönhatásról"

EDPB. "Tájékoztató az általános adatvédelmi rendelet alapján az Egyesült Királyságba az átmeneti időszakot követően történő adattovábbításról" (elfogadva 2020. december 15-én).

EDPB. " 04/2021. Iránymutatás a magatartási kódexekről, mint az adattovábbítás eszközeiről"

EDPB. "07/2022 Iránymutatás a tanúsításról, mint az adattovábbítás eszközéről"

³⁸⁶ Az Európai Gazdasági Térségen ("EGT") kívülrre történő adattovábbítás tekintetében a CNIL ajánlásokat tett közzé a személyes adatoknak az Egyesült Államok jogi eljárásai keretében történő továbbítására vonatkozóan, amelyekre "Discovery" néven hivatkoznak.

³⁸⁷ Például az Európai Bizottság által kiadott általános szerződési feltételekre

³⁸⁸ Informatique et Libertés, Article 87.

³⁸⁹ Informatique et Libertés, Article 89.

³⁹⁰ Informatique et Libertés, Article 31.-32 IV. fejezet: A feldolgozás végrehajtását megelőző alaki követelmények.

A bűncselekmények megelőzésével, nyomozásával, felderítésével vagy üldözésével, illetve büntetőjogi szankciók vagy szabadságelvonással járó határozatok állam nevében történő végrehajtásával kapcsolatos adatkezelés tekintetében a törvény előírja ³⁹¹, hogy az adatkezelő milyen esetben továbbíthat adatokat vagy engedélyezheti a már nem uniós államba továbbított adatok továbbítását. Az adattovábbítás akkor lehetséges a bűnüldözés, büntetőjogi eljárások és szankciók végrehajtása céljából, ha:

- a személyes adatokat nemzetközi szervezetnek vagy olyan nem uniós államban letelepedett adatkezelőnek továbbítják, amely Franciaországban a bűncselekmények kezeléséért felelős;
- az adatokat továbbító ország nemzeti jogával összhangban előzetesen engedélyezte a továbbítást;
- az adatvédelmi irányelv 36. cikkének megfelelően megfelelőségi határozat áll rendelkezésre, vagy ha ilyen határozat hiányzik, jogilag kötelező erejű eszköz garantálja az adatvédelmet;
- ha sem határozat, sem jogilag kötelező erejű eszköz nem áll rendelkezésre, az adatkezelő megvizsgálta a továbbítás körülményeit és megfelelő garanciákat talált;
- az adatvédelmi irányelv 38. cikke szerinti egyedi eltérések és a 39. cikkben foglalt feltételek teljesülnek.

A törvény előírja, hogy a bűnügyi célú adatkezelés során az adatkezelőnek és adatfeldolgozónak az adatkezelési nyilvántartást a GDPR 30. cikkében meghatározott módon kell vezetnie. Ezen nyilvántartás tartalmaznia kell a kockázatok kezelésére irányuló biztonsági intézkedések általános leírását, az adatfeldolgozási műveletek jogalapját, beleértve azokat az eseteket is, amikor a személyes adatok továbbítása történik, valamint szükség esetén a profilalkotásra vonatkozó információkat is.³⁹²

Az illetékes hatóságokkal kapcsolatos kötelezettségek is megegyeznek az irányelvben közzétettel. Az egyes szabályozások gyakorlati megvalósítását illetően a francia illetékes hatóságok és bizottságok szerepelnek felelősként.³⁹³

³⁹¹ Informatique et Libertés, Article 112.

³⁹² Informatique et Libertés, Article 100.

³⁹³ Például, Informatique et Libertés, Article 105. 6. pontjában a Nemzeti Számítástechnikai és Szabadságjogi Bizottsághoz panasz benyújtásának joga és a bizottság Elérhetőségei (la Commission nationale de l'informatique et des libertés)

Összefoglalva a (EU) 2016/680 rendelet átültetése francia nemzeti jogba, a korábbi 1978 -s adatvédelmi törvény módosításával, az (EU) 2016/679 rendelettel együtt történt meg, jelenleg egységes szerkezetben ez a törvény hatályos. A 2018. jún. 20-án hatályos törvény még, a külön módosító törvénnyel együtt volt alkalmazandó, majd két módosító rendelet után 2019. júniusában jött létre az egységes adatvédelmi törvény, amely már összhangban van az uniós szabályozással.

2.4 A bűnügyi irányelv átültetése a svéd nemzeti jogba

2.4.1. Előzmények

Svédország volt az első ország Európában, amely adatvédelmi jogszabályokat fogadott el - SFS 1973:289 - ³⁹⁴ az 1973-as adattörvény beiktatásával. Ez a törvény hozta létre a Svéd Adatvédelmi Hatóságot - Integritetsskyddsmyndigheten (IMY).³⁹⁵

A következő svéd személyes adatokról szóló törvény, az - SFS 1998:204³⁹⁶ számú törvény harmonizálta az Európai Parlament és Tanács 95/46/EK irányelvét.

A svéd adatvédelmi rendszer jelenleg egy, az (EU) 2016/679 rendeletet kiegészítő törvényből, valamint úgynevezett nyilvántartási jogszabályokból épül fel, amelyek elsősorban a személyes adatok hatóságok általi feldolgozását szabályozzák.

Míg a GDPR-t kiegészítő törvények a GDPR hatálybalépésével összefüggésben készültek, az úgynevezett nyilvántartási szabályozás már a GDPR előtt is létezett. Ezeket módosították, a GDPR-ra való hivatkozásokkal, a korábbi 1998-s törvényt visszavonták, és helyette a GDPR kiegészítő rendelkezéseit tartalmazó törvény - SFS 2018:218³⁹⁷ - lépett hatályba. A törvényen

³⁹⁴ Datalag (1973:289).

https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289 (2022.07.15.)

³⁹⁵ Integritetsskyddsmyndigheten, <https://www.imy.se> (hozzáférés: 2022.07.15.)

³⁹⁶ Personuppgiftslag (1998:204), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204 , (hozzáférés: 2022.07.15.)

³⁹⁷ Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218, (hozzáférés: 2022.07.15.)

kívül a GDPR kiegészítő rendelkezéseit tartalmazó rendeletet - SFS 2018:219³⁹⁸ – is elfogadták. Ez azt jelenti, hogy a svéd adatvédelmi rendszer a vonatkozó nyilvántartási rendelettel együtt értelmezendő.³⁹⁹

Ezeket kiegészítik azonban ágazati adatkezelési tevékenységekre irányuló törvények, úgymint a svéd betegadatokról szóló törvény - SFS 2008:355⁴⁰⁰, amely szabályozza a személyes adatok kezelésének módját az egészségügyi szektorban. A svéd hitelinformációs törvény - SFS 1973:1173⁴⁰¹ - védi az egyének magánéletét a hitelinformációs szolgáltatásokkal kapcsolatban. Az SFS 2018:1177 számú törvény⁴⁰² a 2018-s bűnügyi adatokról szóló törvény az (EU) 2016/680/EU irányelvét ülteti át a svéd jogrendszerbe, 2018. augusztus 1-jén lépett hatályba. Ez a törvény a GDPR-t harmonizáló 2018:218 számú törvénnyel együtt része az EU adatvédelmi reformcsomagjának.

2.4.2. Az SFS 2018:218 számú törvény, az EU adatvédelmi rendelete szerinti kiegészítő rendelkezésekkel

Az SFS 2018:218 számú törvény az, amelyik implementálta az általános adatvédelmi rendeletet. Átfedések vannak a bűnügyi irányelvet harmonizáló törvénnyel és az alábbiakban kiemelt szabályok a bűnügyi adatokról szóló törvényben is megtalálhatók.

A GDPR 2. cikkében foglaltakkal ellentétben a törvény⁴⁰³ kiterjeszti a GDPR hatályát a személyes adatok kezelésére is az alábbi esetekben:

- olyan tevékenység, amely kívül esik az uniós jog hatályán, és

³⁹⁸Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219, (2022.07.15.)

³⁹⁹ Sweden - Data Protection Owerweiv, Guidance Note, <https://www.dataguidance.com/notes/sweden-data-protection-overview>, (2022.07.01)

⁴⁰⁰ Patientdatalag (2008:355), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355, (hozzáférés: 2022.07.15.)

⁴⁰¹Kreditupplysningslag (1973:1173), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kreditupplysningslag-19731173_sfs-1973-1173, (hozzáférés: 2022.07.15.)

⁴⁰² Brottsdatalag, (2018:1177) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177, (hozzáférés: 2022.07.14)

⁴⁰³ SFS 2018:218, 1. ch. 2 .§.

- az Európai Unióról szóló szerződés V. címe 2. fejezetének hatálya alá tartozó tevékenységek végzése esetén is alkalmazható.⁴⁰⁴

A törvény hatálya azonban nem terjed ki, a Svéd Fegyveres Erők Külföldi Hírszerző Műveleti és Katonai Biztonsági Szolgálatára - SFS 2007:258⁴⁰⁵-, a Nemzetvédelmi Rádióállomás működésére - SFS 2007:259⁴⁰⁶ -, vagy a Svéd Biztonsági Szolgálat által a személyes adatok kezeléséről szóló törvényre - SFS 2019:1182⁴⁰⁷.

A törvény területi hatályát illetően változás, hogy a gyermekek személyes adatainak feldolgozásához szükséges beleegyezési korhatárra vonatkozó rendelkezéseknek megfelelően a törvény 2. fejezetének 4. szakasza minden Svédországban élő gyermekekre vonatkozik, függetlenül attól, hogy az adatkezelő vagy adatfeldolgozó hol található.⁴⁰⁸

Az érintetti jogok esetében,⁴⁰⁹ a tájékoztatási joggal és a hozzáférési joggal kapcsolatosan általános kivételt állapít meg a tájékoztatás és a személyes adatokhoz való hozzáférés alól⁴¹⁰ azokban az esetekben, amikor más jogszabályok tiltják az információk közlését az érintettekkel.⁴¹¹

⁴⁰⁴ A törvény az EU/EGT-n kívüli országban letelepedett adatkezelők vagy adatfeldolgozók általi személyes adatok feldolgozására is vonatkozik, ha a feldolgozás Svédországban tartózkodó érintetteket érint, és az ilyen érintettek számára történő termékníjútáshoz vagy szolgáltatásnyújtáshoz kapcsolódik, vagy Svédországban tanúsított magatartásuk nyomán követéséhez szükséges.

⁴⁰⁵ Lag (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007258-om-behandling-av-personuppgifter-i_sfs-2007-258, (hozzáférés: 2022.07.15.)

⁴⁰⁶ Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259, (hozzáférés: 2022.07.15.)

⁴⁰⁷ Lag om Säkerhetspolisens behandling av personuppgifter Utfärdad den 28 november 2019, <https://svenskfornfattningssamling.se/sites/default/files/sfs/2019-11/SFS2019-1182.pdf>, (hozzáférés: 2022.07.15.)

⁴⁰⁸ Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, <https://rkrattsbaser.gov.se/sfst?bet=2018:218>, (hozzáférés: 2022.07.15.)

⁴⁰⁹ SFS 2018:218, 5. ch. 1.§.

⁴¹⁰ GDPR 13. és 14. cikk

⁴¹¹ A GDPR tájékoztatáshoz való jogról szóló 13. és 14. cikke nem vonatkozik azokra az információkra, amelyeket az adatvédelmi törvény vagy más rendelet, illetve jogszabály alapján hozott határozat alapján nem közölhet az érintettel. Ha az adatkezelő nem hatóság, ez a kivétel azokra az információkra is vonatkozik, amelyeket egy hatóság az információkhoz való nyilvános hozzáférésről és a titoktartásról szóló törvény - 2009:400 - értelmében valamely hatóság minősített volna. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400

A helyesbítési-, a törlési-, az adatkezelés korlátozásához való-, tiltakozási-, adathordozhatósághoz való joggal kapcsolatosan nincsenek nemzeti eltérések. Általánosságban megfogalmazható, hogy a törvény felhatalmazza a kormányt⁴¹², hogy további rendeleteket bocsásson ki a GDPR korlátozásokra vonatkozó cikkei alapján.⁴¹³ Ugyanez vonatkozik az automatizált döntéshozatal alóli mentesülés jogára is.

Az alapfogalmak nem különböznek a GDPR – tól. A jogalapok tekintetében a jogalkotó előírja, hogy a jogi kötelezettség alapján történő adatkezelés csak akkor megengedett, ha az adatkezelés szükséges ahhoz, hogy az adatkezelő eleget tudjon tenni a törvényből vagy más jogszabályból, kollektív szerződésből, illetve törvény vagy más jogszabály alapján kiadott határozatból következők.⁴¹⁴

A közérdek és az egyéb jogalapok tekintetében van eltérés a GDPR- tól. A törvény második fejezetének 2. szakasza értelmében a GDPR 6. cikk (1) bekezdés e) pontja lehetővé teszi a hatóságok számára, hogy jogszerűen feldolgozzák a személyes adatokat, amikor közérdekű feladataikat látják el vagy közhatalmi funkciókat gyakorolnak. Ezek a feladatok lehetnek törvényen, jogszabályon, kollektív szerződésen alapulóak, vagy a hatóságok által jogszabály alapján hozott döntésekkel összefüggőek. A törvény második fejezetének 3. szakasza alapján a nemzeti felügyelő hatóság – IMY- jogszabályokat alkothat, és dönthet arról, hogy az adatkezelők milyen feltételek mellett kezelhetik az adatokat archiválási célokra közérdek alapján.

Az adattovábbítás esetén a korlátozások a különleges adatok kategóriáira vonatkoznak.⁴¹⁵ A GDPR V. fejezetében meghatározott, határokon átnyúló adattovábbításra vonatkozó korlátozások a személyes adatoknak az EU/EGT régió kívülre történő továbbítására vonatkoznak.

A gyermekek beleegyezési korhatára a 2018:218 számú törvény szerint 13 év, amikor az információs társadalommal összefüggő szolgáltatásokat közvetlenül gyermekek számára kínálják, a személyes adatok feldolgozása a gyermek beleegyezése alapján történhet, ha a

⁴¹² SFS 2018:218, 5. ch. 3.§.

⁴¹³ GDPR 23. cikke, 89. cikkének (2) bekezdése és 89. cikkének (3) bekezdése alapján

⁴¹⁴ SFS 2018:218, 2. ch. 1.§. A jogszabály a a GDPR 6. cikke (1) bekezdésének c) pontjára hivatkozik: „az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges.)

⁴¹⁵ A törvény 3. fejezetének 2. szakasza korlátozza a személyes adatok különleges kategóriáinak továbbítását, ha azok kezelése abból a célból történik, hogy az adatkezelő vagy az érintett eleget tudjon tenni a munkajogban és a szociális területen fennálló kötelezettségeinek.

gyermek 13 éves vagy idősebb⁴¹⁶. Azonban az IMY által kiadott jogszabály⁴¹⁷ ennél szigorúbb feltételeket szab, 13- 16 éves kor között eseti megítélést kell alkalmazni, és 16 éves kor felett tekinthetők a gyermekek ebből a szempontból jogképesnek.

Megemlítendő még a svéd adatvédelmi hatóság utasításokról szóló rendelete, amely kiegészíti az adatvédelmi törvényeket - SFS 2007:975⁴¹⁸. Ennek 1. szakasza rögzíti, „*az IMY célja (...) az emberek alapvető jogainak és szabadságainak védelme, a személyes adatok feldolgozása, az ilyen adatok EU-n belüli szabad mozgásának elősegítése, valamint annak biztosítása, hogy a hitelminősítési és adósságbehajtási tevékenységek során betartsák a helyes gyakorlatot*”.⁴¹⁹

A megfelelés ellenőrzése és az ellenőrzések lefolytatása mellett az IMY jogosult adatvédelmi jogszabályokat kiadni. Az IMY többek között törvénysértésekkel kapcsolatos személyes adatok feldolgozására vonatkozó jogszabályt - DIFS 2018:2⁴²⁰ - alkotott, amely kifejezetten a magánszemélyek bűncselekményekkel és jogsértésekkel összefüggő személyes adatainak kezelésére vonatkozik.

Az IMY emellett állásfoglalást is kibocsátott a bűncselekményekkel összefüggő személyes adatok kezeléséről, amely összhangban áll a svéd adatvédelmi törvény előírásaival.^{421,422}

Az IMY a "büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatokat" úgy definiálja, mint olyan információkat, amelyek bűncselekményt elkövetett, büntetőügyben bíróság elé állított, kényszerintézkedések, mint őrizetbe vétel vagy utazási tilalom alatt álló, vagy bűncselekmény elkövetésével gyanúsított személyekre vonatkoznak, függetlenül attól, hogy jogi eljárás indult-e ellenük. Főszabályként a büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatok feldolgozása kizárólag a hatóságok számára van fenntartva. A büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatokat azonban más adatkezelők is

⁴¹⁶ SFS 2018:218, 2. ch. 4 .§

⁴¹⁷ DIFS 2018:2, Az IMY az EDPB álláspont szerint állapította meg a szigorúbb feltételt. Ez jó példa arra is, hogy az adatvédelmi törvényt, és kiegészítő jogszabályokat együttesen kell értelmezni.

⁴¹⁸Förordning (2007:975) med instruktion för Integritetskyddsmyndigheten. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2007975-med-instruktion-for_sfs-2007-975 (hozzáférés:2022.07.15.)

⁴¹⁹ saját fordítás

⁴²⁰Föreskrifter om behandling av personuppgifter som rör lagöverträdelser. Datainspektionens författningssamling. Datainspektionen, DIFS 2018:2,(hozzáférés: 2022.07.16.)

⁴²¹ SFS 2018:218, 2. ch. 8 .§.

⁴²²Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen, IMYRS 2021:1

feldolgozhatják, ha az adatkezelés az archiválási rendelkezéseknek való megfelelés érdekében szükséges⁴²³

Az adatkezelés "szükségességének" követelménye nem jelenti azt, hogy az adatkezelésnek elkerülhetetlennek kell lennie. A hatékonyság növelése például elegendő érv lehet arra, hogy miért tartanak szükségesnek egy bizonyos adatkezelési tevékenységet⁴²⁴. Ezenkívül a büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatokat a hatóságokon kívül más is feldolgozhatja, ha az adatkezelés jogi követelés megállapításához, érvényesítéséhez vagy védelméhez szükséges, vagy ha az adatkezelés törvény vagy rendelet szerinti jogi kötelezettség teljesítéséhez szükséges⁴²⁵. Az IMY azonban kijelentette, hogy nem engedélyezett a büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatok feldolgozása az érintetti hozzájárulása alapján.⁴²⁶

2.4.3. A svéd bűnügyi adatokról szóló törvény SFS 2018:1177⁴²⁷

A 2018-s bűnügyi adatokról szóló törvény hatályon kívül helyezte a korábbi, az Európai Unión belüli rendőrségi és igazságügyi együttműködés során a személyes adatok védelméről szóló egyes rendelkezésekről szóló - 2013:329⁴²⁸ számú törvényt. A hatályba lépés előtt történt jogsértésekre, valamint a hatálybalépés előtt bejelentett határozatok elleni fellebbezésekre továbbra is a régebbi szabályozás vonatkozik.⁴²⁹

A törvény a személyes adatoknak a bűnmegelőzési és bűnüldözési feladatokat ellátó hatóságok, úgy, mint a svéd rendőrség, a svéd adóhatóság és a svéd vámhatóság által végzett adatok kezelésére és feldolgozására vonatkozik, és ugyan azokon az elveken alapul, mint a GDPR.

⁴²³ SFS 2018:218, 3. ch. 8.§

⁴²⁴ A levéltárakra vonatkozó különös rendelkezések többek között a svéd levéltári törvényben SFS 1990:782, és a svéd levéltári rendeletben (SFS 1991:446 található. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivforordning-1991446_sfs-1991-446

⁴²⁵ SFS 2018:218, 5. ch.

⁴²⁶ Az IMY egyedi esetekben és kérelemre úgy is határozhat, hogy engedélyezi a büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatok meghatározott feldolgozását. Ilyen engedélyt kell beszerezni különösen az egyének harmadik országok szankciós listái (pl. az Egyesült Államok által kiszabott szankciók) alapján történő átvilágításával kapcsolatos, büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatok feldolgozásához.

⁴²⁷ Brottsdatalog, (2018:1177) .

⁴²⁸ Förordning (2013:343) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.,

⁴²⁹ SFS 2018:1177 , Övergångsbestämmelser, 2. , 5-6.

A hatóságoknak azonban egyértelmű különbséget kell tenniük a bűncselekmény elkövetésével gyanúsított vagy elítélt érintettekre vonatkozó személyes adatok kezelése és az olyan személyekre vonatkozó személyes adatok kezelése között, akiknek a személyes adatait más célból dolgozzák fel, például tanúk vagy hozzátartozók esetében.

A törvény nyolc fejezetből áll, az 1. fejezet az általános rendelkezések, a 2. fejezet a személyes adatok feldolgozása, a 3. fejezet a személyes adatkezelő kötelezettségei, a 4. fejezet az érintetti jogok, az 5. fejezet a felügyelet, a 6. fejezet az adminisztratív bírság díjai, a 7. fejezet a kártérítések és fellebbezések, a 8. fejezet a személyes adatok továbbítása harmadik országok - és nemzetközi szervezetek részére, valamint az átmeneti rendelkezések fejezet címetek viseli. A törvény első fejezete az általános rendelkezések keretében⁴³⁰ a célokat illetően megfogalmazza az uniós ajánlásokat. A törvény hatályát illetően kiemelném, hogy a törvény nem vonatkozik a nemzetbiztonsági vonatkozású személyes adatok biztonsági rendőrség (Säkerhetspolisens) általi kezelésére, illetve arra az esetre, ha a rendőrség nemzetbiztonsági feladatot vett át a biztonsági rendőrségtől. Továbbá a törvény nem vonatkozik a személyes adatok fegyveres erők általi kezeléséről szóló törvényre (2021:1171), illetve fegyveres műveletekkel kapcsolatos törvény által meghatározott adatkezelésekre (2021:1175).⁴³¹ Amennyiben az Alkotmányban szereplő más törvény vagy rendelet e törvénytől eltérő rendelkezést tartalmaz, azt a rendelkezést kell alkalmazni⁴³²

Az SFS 2018:1177 számú törvény a személyes adatoknak egy Svédországi telephellyel rendelkező adatkezelő vagy adatfeldolgozó általi kezelésére vonatkozik. A törvény továbbá alkalmazandó azon személyes adatok kezelésére is, amelyet egy Svédországban nem bejegyzett adatkezelő végez, azonban olyan helyszínen végzi azt, ahol a svéd jog a nemzetközi jog alapján alkalmazandó.

A törvény szintén vonatkozik a csak harmadik országban bejegyzett adatkezelők vagy adatfeldolgozók által végzett személyes adatok kezelésére, ha a kezelés olyan adatalanyokra érint, akik Svédországban tartózkodnak és kapcsolatban állnak az ilyen adatalanyoknak történő áruk vagy szolgáltatások kínálásával, vagy „viselkedésük” Svédországban történő megfigyelésével. A Svédországban élő gyerekek személyes adatainak kezelésére is vonatkozik, függetlenül attól, hogy az adatkezelők vagy adatfeldolgozók hol vannak bejegyezve.⁴³³

⁴³⁰ SFS 2018:1177,1 ch.

⁴³¹ SFS 2018:1177, 1 ch., 4. § A.

⁴³² SFS 2018:1177, 1 ch., 4. §.

⁴³³ SFS 2018:1177, 2.ch. 4. §.

A fogalom meghatározások terén a regisztrált, a harmadik ország és harmadik fél fogalmait is meghatározza.⁴³⁴

Az uniós irányelv megfogalmazza, hogy a tagállamok megfelelő határidőket állapítanak meg a személyes adatok törlésére vagy tárolásuk szükségességének rendszeres felülvizsgálatára. Ezen határidők betartását eljárásjogi intézkedésekkel kell biztosítani. A 2018-s bűnügyi adatokról szóló törvény 2. fejezete⁴³⁵ foglalkozik a személyes adatok kezelésével, részletezi, hogy mely személyes adatok, milyen célból, milyen feltételekkel, milyen időtartamra használhatók, továbbá, hogy mely mértékben és módon szükséges az érintett személyeket és nyilvánosságot tájékoztatni. Ha a személyes adatok kezelésének célja nem egyértelmű a szöveggörnyezetből vagy más módon, azt külön közzététellel kell egyértelművé tenni.⁴³⁶ Ezt a személyes adatok egyes kategóriának kezelésénél is láthatjuk, ha a szöveggörnyezetből vagy más módon nem derül ki, hogy a személy melyik kategóriába tartozik, azt külön közzététellel szükséges egyértelművé tenni.⁴³⁷ A törvény 3. 4. 6. és 7. fejezetei a bűnügyi irányelvvvel azonos szabályozást írnak elő.

A törvény bűnügyi célú adattovábbításokkal kapcsolatosan konkrét követelményeket tartalmaz a személyes adatok továbbítását illetően.

A személyes adatok továbbításával kapcsolatban kiemelném még, hogy amennyiben egy svéd illetékes hatóság személyes adatot kapott egy másik tagállamtól vagy uniós szervtől, és vannak olyan feltételek, amelyek korlátozzák az adatok felhasználásának lehetőségét, a svéd hatóságok kötelesek azokat a feltételeket betartani.⁴³⁸

A személyes adatok harmadik országokba és nemzetközi szervezeteknek történő továbbítása kérdéseivel az 8. fejezet foglalkozik. A 8. fejezetének 1. szakasza szerint néhány kivételtől eltekintve, az illetékes hatóságok csak akkor továbbíthatnak személyes adatokat harmadik országnak vagy nemzetközi szervezetnek, ha az adattovábbítás:

- ha a bűncselekmények megelőzéséhez, megelőzéséhez vagy felfedezéséhez, a bűncselekmények kivizsgálásához vagy a bűnözők üldözéséhez, a büntetőjogi szankciók végrehajtásához vagy a közrend és közbiztonság fenntartásához szükséges,

⁴³⁴ SFS 2018:1177,1 ch., 6. §

⁴³⁵ SFS 2018:1177, 2 ch. 1-23.§.

⁴³⁶ SFS 2018:1177, 2 ch.

⁴³⁷ SFS 2018:1177, 2 ch. 9. § .

⁴³⁸ Brottsdatalog (2018:1177), 2. ch. 20a §.

- ha a harmadik ország felhatalmazott hatóságához vagy olyan nemzetközi szervezethez irányítják, amely felhatalmazott hatóság,
- valamint megfelelőségi határozattól, megfelelő biztosítékoktól vagy egy adott helyzetre vonatkozó eltéréstől függően.^{439,440}

Ezen túlmenően a törvény 8. fejezetének 2. szakasza rögzíti, hogy főszabályként a svéd hatóság csak akkor továbbíthat egy másik EU-tagállamból kapott személyes adatokat harmadik országnak vagy nemzetközi szervezetnek, ha az adott uniós tagállam ehhez előzetesen hozzájárul.⁴⁴¹ Nincs szükség előzetes jóváhagyásra, ha az átadás a közbiztonságot érintő azonnali és súlyos fenyegetés, vagy Svédország vagy egy másik EU-tagállam kulcsintézménye elleni fenyegetés elkerülése érdekében szükséges⁴⁴². Ezenkívül törvény hatálya alá tartozó személyes adatok másik EU-tagállamba történő továbbításakor nem írhatók elő más feltételek, mint amelyek a svéd címzettre vonatkoznak, kivéve, ha jogszabály vagy rendelet kifejezetten másként rendelkezik.⁴⁴³

Összefoglalva a (EU) 2016/680 rendelet átültetése a svéd nemzeti jogba, a svéd bűnügyi adatokról szóló törvény, az SFS 2018:1177 számú törvény megalkotásával jött létre. A törvény hatályon kívül helyezte a korábbi, az Európai Unió belüli rendőrségi és igazságügyi együttműködés során a személyes adatok védelméről szóló egyes rendelkezésekről szóló - 2013:329⁴⁴⁴ - törvényt, így a személyes adatok bűnügyi célból történő kezelésére az 2018:1177 számú törvény szolgál. Az általános adatvédelmi rendeletet az SFS 2018:218 törvény és a GDPR kiegészítő rendelkezéseit tartalmazó rendeletet - SFS 2018:219– együttesen alkotja. Ez azt jelenti, hogy a svéd adatvédelmi rendszer ezen a hármas pilléren alapul, a külön ágazati adatvédelmi jogszabályok, és a svéd adatvédelmi hatóság IMY által alkotott törvényekkel együttesen.

3. Az egyes nemzeti szabályozások összehasonlító vizsgálata

⁴³⁹ Brottsdatalog (2018:1177), 2. ch. 1. §. 1.-3 .

⁴⁴⁰ A megfelelő védelmi szinteket a törvény 2. fejezetének 3. és 4. szakasza szabályozza.

⁴⁴¹ Brottsdatalog (2018:1177).

⁴⁴² Brottsdatalog (2018:1177), 8. ch.1. – 2. §.

⁴⁴³ Brottsdatalog (2018:1177), 2 ch. 20. §

⁴⁴⁴ Förordning (2013:343) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

3.1. Jogharmonizáció a nemzeti jogrendszer sajátosságai alapján

Általánosságban elmondható, hogy a jogharmonizáció kereteit tagállami részről, az adott tagállam jogrendszerének szabályai adják, azok történeti kialakulásának és hierarchiájának megfelelően.⁴⁴⁵

A magyar szabályozás ezen elvek mentén, az információs szabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról szóló 2018. évi XXXVIII. törvény által fogalmazta meg jogszabályok módosítását. A korábbi adatvédelmi szabályozás után 2011-ben az Alaptörvény a 95/46/EK irányelv alapján rendelkezett a felügyeleti hatóságról, amely többek között alapul szolgált a második magyar adatvédelmi- és információs szabadság törvény megalkotásához. A Nemzeti Adatvédelmi és Információs szabadság Hatóságot a korábbi törvény hozta létre. Az Infotv. a harmonizált szabályok mellett megtartotta a korábbi rendelkezéseket, és a változások kiemelésével implementálta a 2018-s adatvédelmi reformcsomagot.⁴⁴⁶ A törvény bünyügyi személyes adatok kezelésére vonatkozóan továbbra is a különleges adatok kezelésének feltételeire vonatkozó szabályokat alkalmazza. A bünyügyi irányelv adatkezelése az Infotv.-ben a bünyüdözési célú adatkezelések alatt szerepel a korábbi alkalmazásnak megfelelően, elkülönítve azt a személyes adatok bünyütőjogi védelmétől. A nemzetbiztonsági célú adatkezelések és a honvédelmi célú adatkezelések – mint a nemzeti jog által szabályozható adatkezelési jogviszonyok – szintén az Infotv. hatálya alá tartoznak. Az Infotv. teljes egységben az általános adatvédelmi rendelettel ültette át a bünyügyi irányelv rendelkezéseit, háttérszabályokat is biztosítva.

Németországban, hat évvel a hesseni (a világ első adatvédelmi törvénye) törvény után a szövetségi kormány követte a példáját. A német szövetségi adatvédelmi törvény első változata a „Die erste Fassung des deutschen Bundesdatenschutzgesetzes. A 95/46/EK adatvédelmi irányelv átültetése is tartományi szinten kezdődött meg. Hessen és Brandenburg tartomány reagált először, 1998-ban, illetve 1999-ben adatvédelmi törvényeiket az EU követelményeihez

⁴⁴⁵ Palánkai, Tibor.(2019.)⁴⁴⁵„Integráció és kohézió az EU-ban.” In *Tagállami integrációs modellek*, pp. 27–50.

„Az EU szabályozási szerkezete két lábon áll. Az egyik az uniós politikák, a másik pedig a nemzeti politikák rendszere. Mindkettő alapvető jelentőségű az Unió normális és hatékony fejlődése és működése szempontjából.”
31.o

⁴⁴⁶„Összhangban az Európa Tanács adatvédelmi egyezményéhez tett nyilatkozattal – Lásd, az egyezményt kihirdető 1998. évi VI. törvény 3. §. – kiterjeszti a személyes adatok védelmére vonatkozó szabályok alkalmazását azon adatkezelési tevékenységekre” Lásd: Sziklay Júlia és Bendik Tamás. "Az adatvédelem hazai és európai uniós szabályozása és alapintézményei." Budapest: NKE, 2018, p.17.

igazították. 2001 májusától hatályba léphetett a felülvizsgált szövetségi adatvédelmi törvény, majd 2006. január 1-én pedig hatályba lépett az információs szabadságról szóló törvény. Az új német szövetségi adatvédelmi törvény (*Bundesdatenschutzgesetz* – "BDSG") elfogadásával hozzáigazították a korábbi német jogi keretet a GDPR-hoz. A BDSG a GDPR-ral együtt lépett hatályba 2018. május 25-én. A második adatvédelmi kiigazítási törvény 2019. november 26-án lépett hatályba, amely tovább módosítja a BDSG-t, és módosít 154 másik szövetségi törvényt, hogy összeegyeztesse azokat a GDPR-ral, és a LED-el. A BDSG kihasználta a GDPR számos nyitózáradékát, melyek lehetővé teszik a tagállamok számára, hogy meghatározzák vagy akár korlátozzák a GDPR szerinti adatkezelési követelményeket. Az új német adatvédelmi törvény együttesen implementálta az EU 2016/680 rendeletét a GDPR-ral. A BDSG tehát az adatvédelmi reformot követő szabályozásig több módosításon esett át, melyek a tartományi módosításokkal kezdődtek, és ezek után jött létre az egységes törvény, amely tartalmazza a tartományi szabályozást is.

A francia szabályozás, az adatvédelmi reform kapcsán szintén követte a francia jogrendszer által korábban létrehozott törvényi szabályozási elveket.

A személyes adatok védelméről szóló, 2018. június 20 - i, 2018-493 számú törvény módosította a 78-17. számú törvényt, és ültette át a francia jogba a bünygyi adatvédelmi irányelvet és az általános adatvédelmi rendeletet együttesen. A törvény 2018. május 25-én, visszamenőlegesen lépett hatályba. Franciaország fenntartotta az 1978-as törvény architektúráját, megőrizve a 40 évvel korábban jogalkotó által meghatározott elveket, és csak az egymásnak ellentmondó rendelkezéseket helyezte hatályon kívül. A törvény olvasata így meglehetősen nehézkes volt, gyakorlati alkalmazás tekintetében nem volt egyértelmű. Ezt a 2018-as 2018-687. számú rendelet elfogadásával oldották meg. A 2018-687. számú rendelet meghatározza a CNIL szervezetét, összehangolja a Polgári perrendtartást⁴⁴⁷ és a Büntető Törvénykönyvet⁴⁴⁸. Végül ezen módosításokkal a 78-17. számú törvény felépítésében és szövegében is változott, külön fejezet cím alatt szabályozza a bünygyi adatvédelmi irányelv alapján létrejött rendelkezéseket. A 2019. június 1-én így hatályba lépett egységes adatvédelmi törvény, az „Informatique et Libertés” biztosítja az összhangot a többi hatályos szabályozással és az uniós joggal.

⁴⁴⁷ Code civil, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721/, (hozzáférés: 2022.07.15).

⁴⁴⁸ Code pénal, <https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070719/>, (hozzáférés: 2022.07.15).

A bűnügyi adatvédelmi irányelv átültetése a svéd nemzeti jogba szintén a nemzeti sajátosságokon alapul. Svédország az elsők között, 1973-ban alkotta meg a nemzeti adatvédelemmel kapcsolatos jogszabályait. A következő, az SFS 1998:204 számú törvény az Európai Parlament és Tanács 95/46/EK irányelvének átültetésével jött létre. A svéd adatvédelmi rendszer jelenleg egy, az (EU) 2016/679 rendeletet kiegészítő törvényből, valamint az úgynevezett nyilvántartási jogszabályokból épül fel, amelyek elsősorban a személyes adatok hatóságok általi feldolgozását szabályozzák. A korábbi 1998-s törvényt visszavonták, és helyette a GDPR kiegészítő rendelkezéseit tartalmazó törvény, az SFS 2018:218 számú törvény lépett hatályba. A törvényen kívül a GDPR kiegészítő rendelkezéseit tartalmazó SFS 2018:219 számú rendelet az, amellyel együtt értelmezendő a svéd adatvédelem jogi szabályozása.

Az SFS 2018:1177 számú törvény az (EU) 2016/680/EU irányelvet ülteti át a svéd jogrendszerbe, mely 2018. augusztus 1-én lépett hatályba. A törvény felépítése követi a bűnügyi adatvédelmi irányelv felépítését. A svéd adatvédelmi rendszer hármas pilléren alapul, melynek első két eleme – a létrehozás sorrendjét tekintve – az általános adatvédelmi rendelethez kapcsolódó SFS 2018:218 számú törvény és SFS 2018:219 számú rendelet együttese. A harmadik elem a személyes adatok bűnügyi célból történő kezelésére szolgáló 2018:1177 számú törvény.

A bűnügyi adatvédelmi irányelv tagállami átültetése a magyar, a német, a francia- és a svéd nemzeti jogrendszerekbe nem különíthető el teljesen az általános adatvédelmi rendelet nemzeti jogban történő alkalmazásától. A magyar, a német és a francia jogalkotó mindkét uniós jogszabályt egységesen, a nemzeti adatvédelmi szabályozás szerinti korábbi törvény keretében, módosító törvényjavaslattal ültette át, megtartva azok uniós szabályozással nem ellentétes rendelkezéseit. A svéd jogalkotás annyiban különbözik, hogy a korábbi adatvédelmi rendeleteket hatályon kívül helyezve új jogszabály megalkotásával alkalmazták az általános adatvédelmi rendeletet, és ugyanígy implementálták a bűnügyi irányelvet is, megfelelően a korábbi jogi szabályozásuknak, külön törvényi szabályozás keretei között. Az uniós jog által megengedett nemzeti mozgástér mindhárom tagállam szabályozásban fellelhető.

3.2. Az egyes nemzeti szabályozások összehasonlítása az Irányelv egyes szempontjai szerint

A Bizottság jelentései alapján,^{449,450} a tagállamok legtöbbje nem tartotta be, az átültetésre vonatkozó 2018. májusi határidőt, kötelezettségi eljárások után 2019-ig azonban ez legtöbb esetben megtörtént. 2022 áprilisában az Európai Bizottság kötelezettségszegési eljárásokat indított Görögország, Finnország és Svédország ellen, mivel ezek az államok nem ültették át megfelelően a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet. Görögország esetében a nemzeti jogszabályokat nem alkalmazták az igazságügyi hatóságok és a bűncselekményeket vizsgáló hatóságok általi adatkezelésre, továbbá hiányoztak a megfelelő adattárolási, adatkezelési jogalapra, és az automatizált döntéshozatali garanciákra vonatkozó rendelkezések. Finnország és Svédország esetében a probléma az érintettek bírósági vagy törvényszéki jogorvoslati lehetőségeinek hiánya volt. 2022-ben Németország ellen is hasonló indokokkal indítottak eljárást, ahol a bűnüldözési adatvédelmi irányelvet átültető jogszabályok nem biztosítottak hatékony korrekciós hatáskört a szövetségi és tartományi szinten.⁴⁵¹

A Bizottság tagállami szakértői csoportot hozott létre, hogy segítse a tagállamokat abban, hogy a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet beépítsék nemzeti jogukba.⁴⁵²

A megfeleléségi értékelés szerint a tagállamok az irányelv bevezetésekor vagy módosították meglévő adatvédelmi törvényeiket, vagy azokat hatályon kívül helyezve, új, horizontális adatvédelmi jogszabályokkal helyettesítették. A nemzeti jogszabályok gyakran hivatkoznak a GDPR megfelelő vagy hasonló rendelkezéseire a bűnüldözési adatvédelmi irányelv átültetésekor. A bűnüldözési adatvédelmi irányelv számos rendelkezését új jogszabályi elemek bevezetésével ültették át a tagállamok, például az általános közigazgatási jog, a közigazgatási eljárásjog és a büntetőeljárás területeken. Továbbá, egyes tagállamok ezen irányelv bizonyos rendelkezéseit beépítették ágazati jogszabályaikba is, amelyek az illetékes hatóságok működését és hatásköreit szabályozzák.

Az általam vizsgált átültetési gyakorlatok esetében is ez volt a jellemző gyakorlat mind a német, a francia, a svéd és a magyar harmonizáció során.

Az irányelv hatályát illetően alapvetően két szempont az irányadó, a személyi és a tárgyi hatály, melyek együttese határozza meg az egységes megközelítést. Ezek konjunktív feltételek,

⁴⁴⁹ COM (2020) 262 final, 2020

⁴⁵⁰ COM (2022) 364 final, 2022

⁴⁵¹ Ibid. L

⁴⁵² Az (EU) 2016/679 rendelettel és az (EU) 2016/680 irányelvvel foglalkozó bizottsági szakértői csoport (E03461); <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461>

az illetékes hatóságok kijelölése (megnevezése) és az adatkezelés célja – a bünygyi célból történő adatkezelés – amelyek alapvetően meghatározzák az irányelv hatályát.

A magyar joggyakorlat ezt jól tükrözi, és elméleti szempontból megfelel az irányelvnek. A LED a közbiztonság érdekében végzett feldolgozási tevékenységekre is vonatkozik, azonban a nemzetbiztonság célú tevékenységekre azonban nem vonatkozik.⁴⁵³ Az Infotv. kiterjesztette a törvény hatályát a nemzetbiztonsági- és honvédelmi célú adatkezelésekre is, „az *Infotv. előírásainak teljességét rendelte el alkalmazni*”⁴⁵⁴.

A német BDSG 45. szakasza (EU) 2016/680 irányelv hatályával kapcsolatban egyértelműen megjelöli az irányelv szerinti bünygyi adatkezelési célt. Arról is rendelkezik, hogy ez a hatály a szövetségi adatvédelmi biztosra és hivatalára is vonatkozik, tehát - „*a 11. § (1) bekezdésében említett szankciók, intézkedések végrehajtásáért felelős állami szervekre is vonatkozik*”⁴⁵⁵

Alkalmazható azokra a közigazgatási szabálysértésekre is, amely nem minősülnek büntetőjogi szabálysértésnek és csak pénzbírság formájában kiszabott közigazgatási szankciókkal sújthatók. A BDSG tárgyi hatálya ebben a tekintetben eltér a büncselekmény szűkebb értelmezését alkalmazó országokban megfigyelhető joggyakorlattól, amelyek a hasonló közigazgatási szankciókat nem tekintik a LED végrehajtása alá tartozónak.⁴⁵⁶

A francia 78-17- s számú adatvédelmi törvény a 87. cikkben határozza meg az irányelv szerinti hatályt. Eszerint ezt „*kell alkalmazni a személyes adatoknak a büncselekmények megelőzése, nyomozása, felderítése vagy büntetőeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása céljából - ideértve a közbiztonságot fenyegető veszélyek elleni védelmet és megelőzést is - bármely illetékes hatóság vagy a közhatalmi jogosítványok és közhatalmi*

⁴⁵³ A LED 2. cikke (3) bekezdésének a) pontja és a LED (14) preambulumbekzdése.

⁴⁵⁴ „A Módtv. egyrészt abból a megfontolásból, hogy az Infotv. kódexjellegét a megváltozott szabályozási környezetben is megőrizze, valamint a Magyarország külső és belső biztonságához kapcsolódó adatkezelési jogviszonyok azonos jellemzőire (például törvényi szinten részletesen szabályozott, közhatalmi szervek által folytatott, alapvető jogok korlátozásával járó tevékenységek) tekintettel a nemzetbiztonsági célú adatkezelések (Infotv. 3. § 10b. pont), valamint a honvédelmi célú adatkezelések (Infotv. 3. § 10b. pont) mint az uniós jog hatályán kívül eső tevékenységek [GDPR 2. cikk (2) bekezdés a) pont; bünygyi irányelv 2. cikk (3) bekezdés a) pont] körébe tartozó jogviszonyokra is - főszabály szerint - a bünygyi célú adatkezelésekre vonatkozó szabályösszességet, azaz az Infotv. előírásainak teljességét rendelte el alkalmazni [Infotv. 2. § (3) bekezdés]”

Bendik, Tamás: „A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása” p. 106.

⁴⁵⁵ Bürgerliches Gesetzbuch, BGB, 11. § (1) 8.

⁴⁵⁶ A német szövetségi törvény a GDPR hatálya alá sorolt számos köz- és magánjogi, közbiztonsággal megbízott szervezetet. Ennek megfelelően a személyes adatok állami szervek általi kezelése többek között közérdekből és közbiztonságból, a jelentős kár megelőzése és a honvédelem érdekében megengedett.

előjogok gyakorlásával megbízott bármely más szerv vagy szervezet (a továbbiakban: illetékes hatóság) általi kezelésére.” A 87. cikk külön kitér a hatóságok GDPR szerinti adatkezelési célokra. A 2018. júniusi törvényben még szerepelt a nemzetbiztonság védelme az adatkezelés céljai között, a jelenleg hatályos törvényben már nem szerepel.⁴⁵⁷

A svéd bűnügyi adatokról szóló törvény, az SFS 2018:1177 a 2. szakaszban határozza meg a törvény hatályát. *E törvényt kell alkalmazni az illetékes hatóságok által a bűncselekmények megelőzése, megelőzése vagy felderítése, bűncselekmények nyomozása vagy üldözése, illetve büntetőjogi szankciók végrehajtása céljából végzett személyes adatok kezelésére. Ugyancsak vonatkozik a személyes adatok illetékes hatóság általi, a közrend és közbiztonság fenntartása céljából történő kezelésére.”*⁴⁵⁸ A törvény nem vonatkozik a nemzetbiztonsági személyes adatok biztonsági rendőrség általi kezelésére, illetve arra az esetre sem, ha a rendőrség nemzetbiztonsági feladatot vett át a biztonsági rendőrségtől.⁴⁵⁹ Nem vonatkozik továbbá a személyes adatok fegyveres erők általi kezeléséről szóló törvényre, illetve fegyveres műveletekkel kapcsolatos törvény által meghatározott adatkezelésekre. Az illetékes hatóság fogalmát a törvény 6. szakasza határozza meg, nevesítve a bűnüldözési célt.

A hatályt illetően a közrend és a közbiztonság azok a fogalmak, melyekhez a tagállamok egy része a nemzetbiztonságot is köti, áttételesen, a közrend megzavarására alkalmas bűncselekmények által. Ez láthatóan a magyar, német és a korábbi francia joggyakorlatban is megjelent.

A hatály tekintetében a GDPR-tól való elhatárolás - a Bizottság jelentése szerint - nem minden tagállamban egyértelmű, elsősorban egyes közigazgatási egységek nem bűnüldözési célú, például pénzügyi információs adatkezelését is az irányelv hatálya alá sorolják. Az általam vizsgálat országok gyakorlatában ez nem lelhető fel.

Az adatvédelmi felügyeleti hatóságok irányítása és jogköreivel kapcsolatosan tagállamok GDPR végrehajtásáért is felelős felügyeleti hatóságot bízták meg a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásával. Jogkörükben a vizsgálati hatásköröket, a korrekciós hatásköröket biztosították, tényleges hatáskörrel rendelkeznek,

⁴⁵⁷ Hatályon kívül helyezte a 2018. december 12-i 2018-1125 sz. 1 Létrehozta: 2018. június 20-i 2018-493 törvény – cikk. 30

⁴⁵⁸ A törvény nem vonatkozik a személyes adatok feldolgozásáról szóló törvény (2021:1171) szerinti tevékenységekre a svéd fegyveres erőknél. (2021:1175) törvény a személyes adatoknak a Nemzeti Védelmi Rádióintézetben történő feldolgozásáról szóló törvényre (SFS 2007:259.) a személyes adatok svéd biztonsági szolgálat általi kezeléséről szóló törvény (SFS 2019:1182) törvényre, melyek a GDPR hatálya alá tartoznak.

⁴⁵⁹ SFS 2018: 1177, 1.ch.4.§

közigazgatási bíróságot kiszabhatnak. Magyarország és Svédország nemzeti felügyeleti hatóságai az irányelvben megszabott hatáskörökön túl is biztosított jogokat a hatóságokra, úgy, mint az adatkezelő és az adatfeldolgozó bármely helyiségébe való belépésének, valamint a bármely adatfeldolgozó berendezéshez és eszközhöz való hozzáférés jogát. A német gyakorlatban értelemszerűen a szövetségi adatvédelmi hatósági bonni székhellyel, a fő felügyeleti szerve a tartományok hatóságainak. Svédország esetében az egyes illetékes hatóságok – köztük a rendőrség – felügyeletét a GDPR tekintetében illetékes felügyeleti hatóság az IMY és a Svéd Biztonsági és Integritásvédelmi Bizottság⁴⁶⁰ felügyeleti hatóság közösen látja el. Az elektronikus hírközlési adatvédelmi irányelvet (2002/58/EK) (módosítva) végrehajtó elektronikus hírközlési törvény (2003:389) hatálya alá tartozó távközlési szolgáltatóknak csak a Svéd Posta és Távközlési Hatóság felé kell bejelenteniük a biztonsági eseményeket, azaz nem az IMY-nek, még akkor sem, ha az incidens személyes adatok megsértését is magában foglalja.⁴⁶¹ Ha azonban a távközlési szolgáltató nem köteles jelenteni az eseményt a Posta és Távközlési Hatóságnak, akkor értesítenie kell az eseményről az IMY-t, amennyiben az esemény személyes adatok megsértésének minősül.

A hatóságok az igazságszolgáltatás függetlensége miatt nem jogosultak az ezzel összefüggő adatkezeléseket felügyelni. Ugyanez a szabályozás jelenik meg a magyar, a német, a francia, és a svéd szabályozásban is. A NAIH személyes adatok tekintetében meghatározott feladatköre a bírósági döntés meghozatalára irányuló peres és nemperes eljárásokban végzett adatkezelési műveletekre nem terjed ki.⁴⁶² A német szövetségi biztos nem jogosult felügyelni a bírói minőségükben eljáró szövetségi bíróságokat.⁴⁶³ Franciaországban a CNIL nem rendelkezik hatáskörrel a bíróságok által végzett adatkezelési műveletek felügyeletére, ha azok igazságszolgáltatási minőségükben járnak el.⁴⁶⁴ A svéd adatvédelmi törvény 5. fejezet 2. szakasza szerint a felügyelet szintén nem terjed ki a személyes adatoknak a bíróságok igazságszolgáltatási tevékenysége keretében történő kezelésére.

Fontos szempont a hatáskör tekintetében, hogy az irányelvvel kapcsolatos nemzeti adatvédelmi jogszabályok megsértését a nemzeti adatvédelmi hatóságok, az igazságügyi hatóságok tudomására hozhatják-e, vagy indíthatnak-e bírósági eljárást, vagy abban részt vesznek-e. A

⁴⁶⁰ SINT, www.sakint.se

⁴⁶¹ SFS 2018: 1177, 3.ch. 9.§: kivételek a 2018:585, és 2018:1249 törvények szerinti kötelezettségek.

⁴⁶² Infotv. 38.§ (2b)

⁴⁶³ BDSG 9.§ (2)

⁴⁶⁴ Informatique Liberté n°78-17 19.cikk V.

NAIH az Infotv. 64. szakasza (1) bekezdése – alapján bírósági pert indíthat, a német BfDi rendelkezik a GDPR 58. cikk (5) bekezdésében említett hatáskörökkel BDSG 16. szakasza alapján. A magánszervezetek GDPR-megfelelőségének felügyelete a tartományok felügyeleti hatóságaira tartozik a BDSG 40. szakasza alapján, és jogosult a jogsértések bejelentésére olyan illetékes szerveknél, amelyek vádemelésre vagy büntetés végrehajtására irányulnak. A francia 78-17- s számú törvény 8. cikk f.) pontja alapján a CNIL haladéktalanul tájékoztatja az ügyészséget, a meghatározott feltételek mellett a büntetőeljárás törvénykönyv (Code de procédure pénale) 40. cikkében foglaltaknak megfelelően, minden olyan bűncselekményről vagy szabálysértésről, amelyről tudomást szerzett, és előterjeszheti észrevételeit a büntetőeljárásban, a büntetőeljárás törvény 41. cikkében meghatározott feltételek szerint⁴⁶⁵ valamint az 52.cikk alapján biztosított a CNIL részvétele bírósági eljárásokban. Az IMY az SFS 2018:1177 törvény szerint bár szankciós jogkörrel rendelkezik, nincs perindítási eljárási képessége.⁴⁶⁶

A jogorvoslati lehetőségekkel kapcsolatban valamennyi tagállam biztosította a jogot arra, hogy az érintett panaszt nyújtson be az illetékes felügyeleti hatóságához. Az irányelv VIII. fejezete rendelkezik az érintetteket megillető jogorvoslatokról, ezen belül az 52. cikk a felügyeleti hatóságnál történő panasztételhez való jogról, az 53. cikk a felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jogról, az 54. cikk az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jogról.

Az Infotv. 55. szakasza (3) bekezdése, a BDSG 20. szakasza, az Informatique Liberté 108. cikke, és az SFS 2018:1177 a 2. és 3. szakasza alapján biztosítja ezeket a jogokat az érintettek számára.

A bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel összhangban valamennyi tagállam bírósági jogorvoslatot is biztosít a felügyeleti hatóság határozatai ellen. Svédország kivételével bírósági jogorvoslat áll rendelkezésre abban az esetben is, ha a felügyeleti hatóság három hónapon belül nem foglalkozik a panasszal, vagy nem tájékoztatja az érintettet a panasz állásáról vagy eredményéről.

A LED 8. cikkének (2) bekezdése szerint a nemzeti adatvédelmi jogszabályoknak az adatkezelés jogalapját meg kell határozni, rendelkezniük kell legalább az adatkezelés célkitűzéseiről, a kezelendő személyes adatokról és az adatkezelés céljairól.

⁴⁶⁵ Informatique Liberté 8. cikk f)

⁴⁶⁶ Finnország és Svédország ellen azért indítottak jogsértési eljárást, mert jogszabályaik nem biztosítják az érintettek számára a bíróság előtti hatékony jogorvoslat lehetőségét. lásd.: COM (2022) 364 final

Az Infotv. 5. szakasza az (1)–(4) bekezdései részletesen megjelölik az adatkezelés céljait és az illetékes hatóságokat a jogalapokat illetően. Az 5. szakasz (2) bekezdése a különleges adatok kategóriáinak kezelését az irányelvnek megfelelően szabályozza.

Németország kifogásolta azt a gyakorlatot, amely szerint a LED 8. cikk (2) bekezdésének egyszerű megisméltése nem elegendő ahhoz, hogy meghatározza, mely hatóság rendelkezik hatáskörrel a személyes adatok kezelésére az adatkezelést indokoló közfeladatokat, valamint az adatkezelés célját illetően. A BDSG az irányelv szerint jogalapot külön nem sorolja fel, azonban ezen címszó alatt a 48. szakasza a személyes adatok különleges kategóriáinak kezelését tárgyalja. A törvény 22. szakasza a GDPR szerint részletezi szintén a személyes adatok különleges kategóriáinak kezelésével kapcsolatos adatkezelést, és ezzel kapcsolatosan rendelkezik az adatkezelés célkitűzéseiről, a kezelendő személyes adatokról és az adatkezelés céljairól.

A francia adatvédelmi törvény a 87. cikk által meghatározott bűnüldözési célú adatkezeléssel kapcsolatosan az első fejezetben az 5. és 6. cikk által meghatározott általános szempontokat sorolja fel, az utóbbi a különleges adatokkal kapcsolatos tiltó intézkedéseket.

A svéd 2018:1177 törvény, amely a 2. fejezet 1. szakaszában meghatározza a bűnügyi adatkezelés jogalapját, ugyanezen fejezet 2. és 3. szakaszaiban általánosan fogalmazza meg az adatkezelési célokat. Az illetékes hatóságok a fogalom meghatározások alatt szerepelnek. A különleges adatok kategóriáira szintén a 2. fejezet 11.- 14. szakaszai vonatkoznak „*ha az általános adatkezelés céljához szükséges.*”

A Bizottság jelentése szerint néhány nemzeti átültető jogszabály hivatkozik a személyes adatok kezelésével kapcsolatos hozzájárulásra mint jogalapra, ideértve a személyes adatok különleges kategóriáinak kezelését is. A bűnügyi célú adatkezeléshez ez csak garanciaként szolgálhat, nem képezheti alapját az adatkezelésnek, a német, francia, svéd és a magyar harmonizált joggyakorlat ezt nem is használta.

Minden tagállam tiltja az automatizált döntéshozatalt, amikor különleges kategóriájú személyes adatok kezeléséről van szó, kivéve ha a megfelelő garanciák biztosítottak. Tilos az olyan profilalkotás is, amely hátrányos megkülönböztetést eredményez.⁴⁶⁷ Nem minden tagállam biztosítja az adatkezelő általi emberi beavatkozás kéréséhez való jogot, vagy nem ír elő megfelelő intézkedéseket az érintett jogainak és/vagy szabadságainak és jogos érdekeinek védelme érdekében.⁴⁶⁸ Az Infotv. 6. szakaszának ba), és bb) bekezdése rögzíti az érintett emberi

⁴⁶⁷ (EU) 2016/680 11 cikk. (2), (3)

⁴⁶⁸ COM (2022) 364 final

közreműködés kéréséhez való jogát, a BDSG 37. szakasza szintén biztosítja ezt a jogot. A francia adatvédelmi törvény ezt a jogot a Loi.No.78-17 101. szakasz alapján biztosítja, a svéd 2018:1177 törvény 19. szakasza megjelöli ezt a feltételt.

Az érintettek jogaival kapcsolatban az irányelv szerinti korlátozás lehetőségével valamennyi tagállam élt. Az érintetti jogok gyakorlása a nemzeti adatvédelmi hatóságon keresztül történik a nemzeti joggal összhangban.

A német átültetés értelmében az adatkezelő elhalaszthatja, korlátozhatja vagy mellőzheti a 13. cikkben foglalt tájékoztatási kötelezettségeket a 13. cikk (3) bekezdésében felsorolt feltételek teljesülése esetén, azonban kiegészíti azt: ha úgy ítéli meg, hogy a veszély elhárítása meghaladja az érintett tájékoztatásához fűződő érdekeket.⁴⁶⁹ A német törvény továbbá előírja, hogy ha az adatok címzettjei nemzetbiztonsági hatóságok, például hírszerző szolgálatok, akkor az ilyen címzettekről csak akkor adható tájékoztatás az érintettnek, ha az érintett címzett hozzájárulását adja. Ebben az esetben a címzett széles mérlegelési mozgástérrel rendelkezik, amely az adatkezelő ellenőrzésén kívül esik.⁴⁷⁰ A német jogalkotó emellett a hozzáférés megtagadását kibővítette: az adatkezelő akkor is korlátozhatja a hozzáférési jogot, ha az adatokat csak jogszabályi követelmények miatt tárolják.^{471,472}

A hozzáféréssel kapcsolatban – LED 14. cikk - csak néhány nemzeti jogszabály fogadott el eltérő megfogalmazást vagy további követelményeket.⁴⁷³ Franciaország az érintett azonosítására vonatkozóan külön eljárást ír elő, amelynek során az érintettnek bármilyen, az adatkezelő által a hitelesítéshez elegendőnek ítélt eszközzel (beleértve a digitális személyazonosság használatát is) igazolnia kell személyazonosságát. Az említett azonosítási eljárás során a válaszadási időszak felfüggesztésre kerül.⁴⁷⁴ A hozzáférési jog akkor is megtagadható, ha az érintett nem ad elegendő információt ahhoz, hogy az adatkezelő aránytalan

⁴⁶⁹ BDSG Section 13. (3)

⁴⁷⁰ BDSG Section 34.

⁴⁷¹ BDSG Section 57.

⁴⁷² A legutóbb a 2019. november 20-i törvény 12. cikkével (Szövetségi Jogi Közlöny I., 1626. o.) módosított, 2017. június 30-i szövetségi adatvédelmi törvény (Szövetségi Jogi Közlöny I., 2097. o.) 353.§ 56.

⁴⁷³ (EU) 2016/680 14.cikk. A holland jogszabály meghatározott határidőt határoz meg az adatkezelő válaszára

⁴⁷⁴ Vogiatzoglou, P. et al. "Assessment of the implementation of the Law Enforcement Directive" p.104.

erőfeszítés nélkül megtalálja a személyes adatait. Kérdéses, hogy ezek az indokok összhangban vannak-e a LED-del.⁴⁷⁵

Az érintettek kategóriái közötti irányelv által meghatározott különbségtétel mindegyik általam vizsgálat tagállam esetén jelen van. Az Infotv. 7. szakasza 1.a) bekezdése jelöli meg, az irányelv szerint megnevezett gyanúsított fogalmát, bár nem nevesíti. „*akik tekintetében alapos okkal feltételezhető, hogy bűncselekményt vagy szabálysértést követtek el vagy bűncselekményt készülnék elkövetni.*” A BDSG szintén megnevezi a 72. szakaszban az érintettek különböző kategóriái közötti különbségtétel között, olyan személyek, akikről alapos okkal feltételezhető, hogy bűncselekményt követtek el, illetve olyan személyek, akikről alapos okkal feltételezhető, hogy bűncselekmény elkövetésére készülnék. A 78-17 francia adatvédelmi törvény 98. szakasza rendelkezik miszerint az adatkezelő lehetőség szerint és adott esetben egyértelmű különbséget tesz az érintettek különböző kategóriáinak személyes adatai között, mint például: „*olyan személyek, akikről alapos okkal feltételezhető, hogy bűncselekményt követtek el vagy készülnék elkövetni.*” A svéd Brodsdata lag úgy fogalmaz a törvény 9. szakaszában, hogy amennyire lehetséges, az érintettek különböző kategóriáira vonatkozó személyes adatokat úgy kell megkülönböztetni, hogy jelezzék, hogy az adott személy gyanúsított, elítélt elkövető, bűncselekmény áldozata vagy bűncselekmény által érintett más személy. Ha a szöveggörnyezetből vagy más módon nem derül ki, hogy a személy melyik kategóriába tartozik, azt külön közzététellel kell egyértelművé tenni.

A Ministerstvo na vatreshnite raboti kontra BC ügyben benyújtott előzetes döntéshozatal iránti kérelem C-205/21. ügyben az EUB ítélete kapcsolódik irányelv az érintettek kategóriái tekintetében történő különbségtételhez.⁴⁷⁶ Az ítélet 83. pontja kimondja, hogy a tagállamoknak biztosítaniuk kell, hogy az adatkezelők egyértelműen különbséget tegyenek az érintettek

⁴⁷⁵ Dimitrova, Diana. and De Hert, Paul. "The right of access under the Police Directive: Small Steps Forward." In: Medina, M. et al. (szerk.), *Privacy Technologies and Policy*, Lecture Notes in Computer Science, Springer International Publishing, 2018, 111–130.

⁴⁷⁶ C-205/21. sz. ügy: Ítélet 1.pont: „Az előzetes döntéshozatal iránti kérelem a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében (...) az (EU) 2016/680 (...) 4. cikke (1) bekezdése a) és c) pontjának, 6. cikke a) pontjának, továbbá 8. és 10. cikkének, valamint az Európai Unió Alapjogi Chartája (a továbbiakban: Charta) 3., 8., 48. és 52. cikkének értelmezésére vonatkozik.”

különböző kategóriáinak adatai között, a 84. pont szerint azonban ez nem abszolút jellegű, tehát minden esetben külön kell meghatározni azt.⁴⁷⁷

A bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 25. cikke a meghatározza azokat a minimális információ típusokat, amelyeket az automatizált adatkezelési rendszerben a naplónak tartalmazniuk kell. Az Infotv.25/E. szakasza tartalmazza ezeket, az automatizált adatkezelési rendszerekkel kapcsolatban a 25/F. szakasz rendelkezik. A német BDSG 76. szakasza szabályozza a naplózást, és tárgyalja többek között, hogy az automatizált feldolgozási rendszerekben milyen feldolgozási műveletet kell naplózniuk. A francia 78-17 törvény 101. cikke szerint a bűncselekmények megelőzése, kivizsgálása, felderítése vagy üldözése céljából történő feldolgozással kapcsolatban az adatkezelő és az adatfeldolgozó naplót vezet minden egyes automatizált feldolgozási műveletről, amely többek között magában foglalja az adatok gyűjtését, megváltoztatását, betekintését, nyilvánosságra hozatalát és törlését. A svéd 2018:1177 3. fejezetének 5. szakasza úgy fogalmaz, hogy a személyes adatkezelő gondoskodik arról, hogy az automatizált adatfeldolgozó rendszerekben a személyes adatok kezeléséről a külön előírt mértékben naplót vezessenek.

A német adatvédelmi törvénnyel kapcsolatban, a LED 21. cikk - a közös adatkezelőkről szóló rendelkezés - általános követelményeinek beépítése és a kapcsolattartó pont létrehozása tekintetében mutatkoznak eltérések. A német adatvédelmi törvény nem tesz kifejezett említést a közös adatkezelésre vonatkozó kapcsolattartási pont kijelölésének kötelezettségéről, így a LED e követelménye látszólag teljesen hiányzik a nemzeti jogi keretből.⁴⁷⁸

Összefoglalva a tagállamok között tapasztalható eltérések a bűnügyi irányelv átültetésében, a problémák elsősorban az irányelv értelmezésében és ezáltal az alkalmazásában is megjelennek, ami az irányelv által biztosított tág mérlegelési jogkörből adódik. Különösen a "bűncselekmény", "közbiztonság" és "illetékes hatóság" fogalmak nemzeti értelmezési különbségei jelentek meg, ami befolyásolja a hatály fogalmának értelmezését. Az eltérések abból is adódnak, hogy nincs egységes meghatározás ezekre a fogalmakra.

⁴⁷⁷ Valamely személy bűnösségére vonatkozó elegendő számú bizonyíték fennállása főszabály szerint alapos okot jelent annak feltételezésére, hogy e személy elkövette a szóban forgó bűncselekményt. A fentiek alapján úgy tűnik, hogy az a nemzeti szabályozás, amely előírja a természetes személyek biometrikus és genetikai adatainak kényszer alkalmazásával, nyilvántartásba vétel céljából történő gyűjtését abban az esetben, ha elegendő bizonyíték áll rendelkezésre arra vonatkozóan, hogy az érintett személy bűncselekményt követett el, megfelel a 2016/680 irányelv 6. cikke a) pontja célkitűzésének.

⁴⁷⁸ COM (2022) 364 final

A Bizottság jelentése alapján ugyanez látható a különleges adatok kezelésével kapcsolatban, valamint a 21. cikk szerinti közös irányítással kapcsolatos átláthatóság és a hozzáférhető információk elégtelensége miatt, amit tovább súlyosbít az egyablakos ügyintézési pont létrehozásának következtelen nemzeti végrehajtása.

A LED végrehajtásával kapcsolatban felmerült aggályok a felügyeleti hatóságok függetlenségével is kapcsolatosak. A felügyeleti hatóságoknak teljes mértékben függetlennek kell lenniük az adatvédelmi normák érvényesítéséhez. Bár a nemzeti jogszabályok kiterjeszthetik az irányelv minimumszabályait, a hatóságok hatáskörei gyakran korlátozottabbak, mint amit az uniós ajánlások javasolnak. Ez az általam vizsgált összehasonlításban Svédország gyakorlatában merült fel, ahol egy másik felügyeleti hatóság látja el a rendőrség adatvédelmi szempontú felügyeletét.

Véleményem szerint az irányelv végrehajtásának további pontosítása érdekében fontos a tagállamok közötti együttműködés erősítése, a legjobb gyakorlatok cseréje, és az Európai Bizottság, az Adatvédelmi Testület iránymutatásai, és a folyamatban lévő EUB döntések által nyújtott iránymutatások és támogatások hatékony alkalmazása. A 2026-ban esedékes bizottsági felülvizsgálat a tagállami joggyakorlatokat illetően kiemelt fontosságú lesz ezeken a területeken. Álláspontom szerint jelenleg az Irányelv megfelelő keretrendszert biztosít a tagállamok számára. A fogalmak értelmezése tekintetében az EUB gyakorlata megfelelő útmutatást ad, az EDPB által kialakított gyakorlat és a kötelező érvényű döntések képesek a technikai fejlődés által megkívánt kiegészítéseket a szabályozási folyamatba „kívülről” beépíteni.

Fontos figyelembe venni, hogy a bűnüldözési célú adatkezelések uniós szabályozása nem rendeleti formában, hanem irányelvi megfogalmazás keretei között jött létre. Ez lehetőséget ad a tagállamoknak saját nemzeti jogszabályaik kialakítására. A bűnüldözéssel és intézményeivel kapcsolatos további uniós szabályozások adatvédelmi szempontból az EDPB és EDPBS által felügyeltek, ezen szabályozások nemzetközi kontextusban segíthetik a tagállamokat abban, hogy az adatvédelmi elveket hatékonyan integrálják nemzetközi együttműködéseikbe.

IV. A bűncselekményekhez kapcsolódó személyes adatok védelme

1. Elméleti megfontolások a bűnügyi célú adatkezelések kapcsán

A személyes adatok védelme gyakorlati szempontból álláspontom alapján, a természetes személyek jogainak és szabadságainak védelme a természetes személyek személyes adataihoz

fűződő önrendelkezési jog gyakorlási körülményeinek meghatározása- , valamint a természetes személyek személyes adatait kezelő adatkezelőkre vonatkozó adatkezelési felételek szabályozásának meghatározása által.

Ennek értelmében mind az adatkezelő, mind az adatkezeléssel érintett természetes személy (továbbiakban: érintett) rendelkezési joggal bírnak az érintett személyes adatai felett. Míg az adatkezelő által történő rendelkezési jog jogszerűségét, másnéven jogalapját a vonatkozó szabályozásban, úgy, mint a GDPR-ban, valamint a LED-ben foglalt jogalapok valamelyike biztosítja, addig az érintett személyes adataival információs önrendelkezési joga keretében saját maga rendelkezik. Azaz az adatkezelés feltételeit, a személyes adatok feletti rendelkezési jog gyakorlásának feltételeit az érintetten kívüli személyek, vagyis az adatkezelők vonatkozásában valamely „adatvédelmi” jogszabály vonatkozó rendelkezése határozza meg.

A rendelkezési jognak vannak korlátai mindkét irányból. Az adatkezelés mint fogalom⁴⁷⁹ maga is jogszabály által szabályozott rendelkezési jogosultság az érintett személyes adatai felett. Az adatkezelő által végzett adatkezeléseknek, vagyis a személyes adatokon végrehajtott valamely műveleteknek vannak bizonyos korlátai. Ha elméleti síkon egy mérleg két serpenyőjébe helyeznénk az érintett személyes adatait érintő rendelkezési jogosultságokat adatkezelői, valamint érintett oldalról egyaránt, akkor általános következtetésként elmondható lenne, hogy a személyes adatokkal kapcsolatos rendelkezési jogosultságoknak több jogszabályi korlátja van adatkezelői oldalon, mint érintetti oldalon.

Ugyanakkor ettől függetlenül az érintett saját személyes adatai feletti önrendelkezési jogának is vannak egyéb korlátai, amelyek klasszikus értelemben nem az úgynevezett „adatvédelmi szabályozás” részét képezik, hanem egyéb jogi normák által és etikai elvek által meghatározottak. (pl. nem küldhetünk intim képet kiskorú személy részére saját magunkról).

Az adatkezelés mindig egy bizonyos mértékű korlátozás. A jogszabályi követelmény, hogy az adatkezelés annak céljától függően nem korlátozhatja aránytalan mértékben az érintettek jogait és szabadságait.

A hatósági típusú adatkezelések - ideértve a bünygyi típusú adatkezeléseket is - során jellemzően az előbbi mérleges példával ellentétben az adatkezelők rendelkezési jogosultsága

⁴⁷⁹ GDPR 4.cikk. 2.” adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;”

van túlsúlyban. Ezen belül a bűnügyi célú adatkezelések a büntetőjog ultima ratio elvet megtestesítő jellege okán jellemzően magukon hordozzák a hatósági jogosultságok többletét a hatósági eljáráson belül megvalósuló adatkezelések tekintetében.

2 .A büntetőeljárás adatvédelmi vonatkozásai

A büntetőeljárás során a magánéleti jogok védelme kiemelt figyelmet igényel, hiszen a büntetőjogi intézkedések, mint például a nyomozati eljárások, a lehallgatás, a házkutatás vagy az adatgyűjtés, mélyen beavatkozhatnak az egyének magánéletébe. A büntetőeljárások alapvető célja a bűncselekmények felderítése, az elkövetők felelősségre vonása és a jogellenes cselekményekből eredő károk orvoslása, miközben az alapvető jogokat, így a magánélet védelmét is tiszteletben kell tartani.⁴⁸⁰ Köhalmi László szavaival élve, *„rendkívül fontos kérdés az emberi jogok garantálása a büntetőeljárás során, és bár a törvénytisztelő állampolgárok többsége csak ritkán kerül kapcsolatba a joghatósággal "ügyfélként", véleményem szerint jobb, ha sok bűnöst szabadon engednek, mintsem hogy egyetlen ártatlan embert elítéljenek.”*

Az Infotv. rendelkezik a bűnüldözési célú adatkezelésekről.⁴⁸¹ Bűnüldözési célú adatkezelés alatt azt a tevékenységet értjük, amikor egy adott szerv vagy személy a jogszabályokban meghatározott feladat- és hatáskörében eljárva a közrendet vagy a közbiztonságot fenyegető veszélyeket igyekszik megelőzni vagy elhárítani, tevékenysége kiterjed a bűnmegelőzésre, bűnfelderítésre, a büntető- és szabálysértési eljárások lefolytatására vagy ezekben való közreműködésre, továbbá a büntetőeljárások vagy szabálysértési eljárások során megállapított jogkövetkezmények végrehajtására.

A büntetőeljárást folytató illetékes hatóságok számára az Infotv. a bűnüldözési célú adatkezelésekkel kapcsolatban szabályozza az érintettek személyes adatainak az elkülönítését az alábbiak szerint:⁴⁸²

„(1) Bűnüldözési célú adatkezelés esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó (...) az általa kezelt személyes adatokat annak alapján rendszerezi, hogy azok azon érintettek személyes adatai

⁴⁸⁰ Köhalmi, László. (2013) "The Human Rights in the Criminal Procedure." In: Magdalena Sitek, Gaetano Dammacco, Aleksandra Ukleja és Marta Wojcicka (szerk.), *Europe of Founding Fathers: Investment in the Common Future*. Olsztyn, Lengyelország: University of Warmia and Mazury, Faculty of Law and Administration, pp.397–407.

⁴⁸¹ Infotv. 3.§ (10) a.)

⁴⁸² Infotv. 5.§ (7)

- a) akik tekintetében alapos okkal feltételezhető, hogy bűncselekményt vagy szabálysértést követtek el vagy bűncselekményt készülnek elkövetni,
- b) akik büntetőjogi vagy szabálysértési felelősségét jogerősen megállapították,
- c) akik bűncselekmény vagy szabálysértés sértettjei voltak, vagy akikről megalapozottan feltételezhető, hogy bűncselekmény vagy szabálysértés sértettjei lehetnek, vagy
- d) akik az a)–c) pontban meghatározottakon túl bűncselekménnyel vagy szabálysértéssel, vagy azok elkövetőivel kapcsolatba hozhatóak, így különösen, akik a büntetőeljárás során tanúként meghallgathatóak, (...)"

Az Infotv. rendelkezései alapján – az érintett hozzájárulása nélkül – személyes adat, illetve különleges adat csak törvény rendelkezése alapján kezelhető.⁴⁸³ Ezzel összhangban a 2017. évi XC. törvény (továbbiakban: Büntetőeljárás törvény, Be.) felhatalmazást biztosít a büntetőeljárásban eljáró hatóságok számára – beleértve a nyomozó hatóságot, az ügyészséget és a bíróságot –, hogy a büntetőeljárás során szükséges és az adott jogszabályban meghatározott feladatok ellátása érdekében hozzáférjenek és kezeljenek minden releváns személyes adatot.⁴⁸⁴ A bírósági eljáráshoz való fordulás nem az érintett szabad választása, mivel a büntetőeljárásban az érintett részvételét általában olyan külső körülmények indokolják, mint hogy terhelt, sértett vagy tanú szerepébe kerül. Továbbá gyakran a bíróság jelenti az egyetlen legitim lehetőséget jogainak és érdekeinek védelmére. Ebből kifolyólag a büntetőeljárásban való részvételt nem szabad úgy tekinteni, mint a személyes adatok védelméhez való jogról való „önkéntes lemondást”.⁴⁸⁵

A büntetőeljárás kezdeti szakasza a nyomozás, melynek fő célja az elkövető azonosítása és a bűncselekmény körülményeinek tisztázása. Ebben az időszakban az eljáró hatóságok arra törekcsenek, hogy megtalálják és megőrizsék azokat a bizonyítékokat, amelyek a további jogi lépések alapját képezik.⁴⁸⁶ Ezt követően az azonosított és rendelkezésre álló bizonyítékokat a

⁴⁸³ Infotv. 7. §.

⁴⁸⁴ Be. 97. § (1)

⁴⁸⁵ 873/B/2008. AB határozat. Idézi: Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," *Büntetőjogi Szemle* 2023/1. szám, p. 54

⁴⁸⁶ Nyiri Sándor, (2018) "A nyomozóhatóságok és az ügyészség kapcsolata a büntetőeljárásról szóló törvényben," *Belügyi Szemle* 66. évf. (6) pp. 5–16.

„A nyomozásnak a büntetőeljárásban kiemelkedő jelentősége van. Ahogy Király Tibor írja: Ha ugyanis a nyomozás során a bűncselekményt, a gyanúsítottat, a bizonyítási eszközöket nem derítik fel, további eljárásra nincs lehetőség, és büntetlenül maradnak bűncselekmények elkövetői, nem történik meg felelősségre vonás.” Lásd. Király Tibor, *Büntetőeljárás jog* (Budapest: Osiris Kiadó, 2000),” p.305.

hatóságok részletesen elemezve készítik elő a büntetőjogi felelősségre vonás folyamatát.⁴⁸⁷ Tremmel Flórián hangsúlyozza,⁴⁸⁸ hogy ebben az eljárási szakaszban nem a nyilvánosság, hanem annak ellenkezője, a titkosság az alapvető irányelv.

A nyomozási szakaszban alapvetően az eljárási cselekmények nem nyilvánosak, kizárólag az érintett személyek jelenlétében történnek. Antal Dániel ezt "*mikroszintű nyilvánosságnak*" nevezi, amely gyakorlatilag nem tekinthető igazi nyilvánosságnak, mert a nyomozás folyamán a titkosság az alapvető elv. Az egyes eljárási cselekmények, mint például a helyszíni szemle vagy a kihallgatás, csak azok számára nyitottak, akiket a Be. részvételre kötelez vagy lehetővé teszi számukra.⁴⁸⁹

A rendőrség, mint elsődleges nyomozó hatóság személyes adatok kezelésére vonatkozó alapvető szabályai között kiemelt helyet foglal el a bűnügyi személyes adatok nagy mennyiségű kezelésének szükségessége, amely a rendőrség alapvető feladatainak végrehajtásához elengedhetetlen. Csak állami vagy önkormányzati hatóságok jogosultak kezelni azokat a bűnügyi személyes adatokat, amelyek a bűncselekmények megelőzésére, felderítésére és üldözésére, valamint az állam közigazgatási és igazságszolgáltatási feladatainak ellátására vonatkoznak. Ez magában foglalja a szabálysértési, polgári peres és nemperes ügyekkel, valamint a közigazgatási peres és nemperes ügyekkel kapcsolatos adatokat tartalmazó nyilvántartások kezelését is.⁴⁹⁰

A rendőrség bűnüldözési tevékenységéhez kapcsolódóan gyűjtött és tárolt személyes adatok felhasználása kizárólag bűnüldözési célokat szolgálhat. Különleges adatok⁴⁹¹, ezen kívül mint

⁴⁸⁷ Herke Csongor, *Büntető eljárás* (Pécs: PTE Állam- és Jogtudományi Kar, 2018), p.25.

A büntetőeljárás (ha nincs előkészítő eljárás) nyomozással kezdődik, és felderítésből, valamint vizsgálatból áll: a felderítés célja a tárgyi és személyi megalapozott gyanú megállapítása, valamint a bizonyítási eszközök felkutatása és biztosítása, a vizsgálat során (szükség esetén bizonyítási eszköz beszerzése és megvizsgálása útján) az ügyészség dönt a nyomozás befejezésének kérdésében (eljárás megszüntetése vagy vádemelés).

⁴⁸⁸ Fenyvesi Csaba, Herke Csongor és Tremmel Flórián, *Új magyar büntetőeljárás* (Budapest-Pécs: Dialóg Campus Kiadó, 2004),p. 95.

⁴⁸⁹Antal Dániel. (2010) "A nyilvánosság és a büntetőeljárás," *Studia Iuvenum Iurisperitorium* (5), p.219. https://epa.oszk.hu/02500/02567/00005/pdf/EPA02567_Studia_Iuvenum_Iurisperitorium_5_2010_217-271.pdf (hozzáférés ideje :2022. augusztus 31.).

⁴⁹⁰ Infotv., 5. § (4)

⁴⁹¹ Infotv., 5. § (1) b.) „, akkor kezelhető, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli.”

amilyenek a faji hovatartozásra, vallási nézetre, szexuális magatartásra és politikai véleményre utaló információk, csak abban az esetben kezelhetők, ha azok közvetlenül kapcsolódnak a bűnüldözés során vizsgált bűncselekményhez, vagy az érintett személy ezen adatok kezeléséhez írásos hozzájárulását adta.⁴⁹² A különleges adatok kezelésének szabályai során az adatkezelő vagy a megbízásából vagy utasítására eljáró adatfeldolgozó megfelelő technikai és szervezési intézkedésekkel biztosítja, hogy az adatkezelés során csak azok férjenek hozzá a különleges adatokhoz, akiknek ez az adatkezelési tevékenység ellátásához szükséges.⁴⁹³

A bűnügyi személyes adatok⁴⁹⁴ is a különleges adatok kategóriáinak elve szerint kezelendők.⁴⁹⁵ A bűnüldözési adatkezelés folyamatában alapvető fontosságú a tényeken alapuló adatok elkülönítése azoktól az adatoktól, amelyek következtetéseken, véleményeken, elemzéseken vagy becsléseken alapulnak.⁴⁹⁶

A nyomozási szakaszt a bírósági eljárási szakasz követi.⁴⁹⁷ A büntető eljárás alanyai a büntetőügyben eljáró hatóságokhoz és magánszemélyekhez, köthetők, akiknek büntetőeljárási jogaik és kötelezettségeik lehetnek, és akik e jogok gyakorlása, illetve kötelezettségek teljesítése érdekében büntetőeljárási cselekményeket végeznek.⁴⁹⁸ A büntetőügyekben eljáró

⁴⁹² Be. 97. § (1)

⁴⁹³ Infotv., 5. § (6)

⁴⁹⁴ Infotv.3.§ (4) *bűnügyi személyes adat*: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

⁴⁹⁵ Infotv.5.§.(7) Bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni.

⁴⁹⁶ Infotv. 7.§ (2)'' Bűnüldözési célú adatkezelés esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó (...)egyértelműen megkülönbözteti az érintettel kapcsolatba hozható tényeket és az érintettel kapcsolatba hozható szubjektív értékeléseket.''

⁴⁹⁷ A büntetőeljárás két alapvető részre bontható: az előzetes nyomozás és a bírósági tárgyalás szakaszára. Ezek a fázisok elvileg egymást követik, de bizonyos esetekben az eljárás csak az egyik szakaszt foglalhatja magában. Az eljárás akkor áll csak a nyomozási szakaszból, ha a nyomozást vezető hatóság vagy az ügyész valamilyen indokból lezárja a nyomozást anélkül, hogy bírósági tárgyalásra kerülne sor, (Be.) 398–399. cikkei. A kizárólag bírósági eljárással rendelkező esetek közé tartoznak a magánvádas ügyek, amelyeket a Be. CIV. fejezete szabályoz.

⁴⁹⁸ Fantoly Zsanett és Budaházi Árpád, *Büntető eljárásjogi ismeretek I.* (Budapest: Dialóg Campus Kiadó, 2019), p. 39.

illetékes hatóságok a nyomozó hatóság, az ügyészség, és a bíróság. A magánszemélyeket illetően a Be. megkülönböztet büntetőeljárásban részt vevő személyeket és segítőkét.⁴⁹⁹

A büntetőeljárásban részt vevő személyek, az eljárás alanyai: a terhelt, a védő, a sértett, a magánvádló, pótmagánvádló, a magánfél, a vagyoni érdekelt, az egyéb érdekelt, az eljárás alá vont jogi személy. A segítőkét és egyéb más szereplőket itt nem részletezem, kivéve a tanút, és a szakértőt. Mindezen szereplők adatvédelmi szempontból a büntetőeljárás során adatkezeléssel érintett személynek tekinthetők. A továbbiakban érintetti oldalról közelítem meg a személyes adataik védelmét, azaz az érintettek egyes kategóriáinak megkülönböztetése alapján, ahogy ez a bűnügyi irányelv alapján az Infotv. egyik alapeleme.⁵⁰⁰

2.1. A gyanúsított személyes adatainak kezelése

A gyanúsított fogalmának különös jelentősége van a személyes adatok védelme szempontjából, hiszen a bűnügyi irányelv különös hangsúlyt helyez ennek meghatározásra. A büntetőeljárás folyamán azonban az elnevezés az eljárás szakaszaihoz igazodik, a nyomozás során gyanúsítottnak nevezzük a terheltet, a vádemelés utáni bírósági eljárásban vádlottnak, a büntetés, a megrovás, a próbára bocsátás, a jóvátételi munka vagy a javítóintézeti nevelés jogerős ügydöntő határozattal történő kiszabása, illetve alkalmazása után pedig elítéltnak.⁵⁰¹ Amennyiben a nyomozó hatóság valakit gyanúsítottként⁵⁰² tervez kihallgatni, az idézés tartalmazza a gyanúsított nevét és azonosításához szükséges személyes adatokat, úgymint a születési hely és idő, anyja neve, lakcím, személyi igazolvány száma, és az állampolgársága. A gyanúsított személyes adatainak védelmével kapcsolatban kulcsfontosságú, hogy megfelelő intézkedések biztosítsák az adatok illetéktelenek általi hozzáféréseinek megakadályozását és

„A hatóságok és magánszemélyek közötti különbség a büntetőeljárási feladatok (büntető anyagi jog érvényre juttatása, törvényesség biztosítása, igazság megállapítása) megvalósításához való viszonyukban nyilvánul meg. A büntetőeljárás feladatainak megvalósítása ugyanis hatósági kötelezettség, ezért a hatóságok az állam nevében közhatalommal felruházva, a legszélesebb körű jogokkal és kötelezettségekkel rendelkező alanyai a büntetőeljárásnak.”

⁴⁹⁹ Fantoly Zsanett és Budaházi Árpád, *Büntető eljárásjogi ismeretek I.* p.40.

⁵⁰⁰ Infotv. 7.§

⁵⁰¹ Fantoly Zsanett és Budaházi Árpád, *Büntető eljárásjogi ismeretek I.* ,p. 50

⁵⁰² Infotv.7.§.a) „akik tekintetében alapos okkal feltételezhető, hogy bűncselekményt vagy szabálysértést követtek el vagy bűncselekményt készülnék elkövetni,” megfelelően a LED.6.cikk.a.) pontjának.

azt, hogy illetéktelen személy ne értesülhessen arról, hogy az érintettet gyanúsítottként hallgatja meg a nyomozó hatóság.⁵⁰³

A Be. előírja a papíralapú idézések és értesítések zárt borítékban történő kézbesítését.⁵⁰⁴ Amikor a gyanúsított kihallgatására kerül sor, a nyomozásért felelős személy felhívja a gyanúsított figyelmét, hogy azonosságának egyértelmű megállapítása érdekében köteles nyilatkozni nevééről, születési nevééről, születési helyéről és idejéről, anyja nevééről, állampolgárságáról, személyazonosító okmányainak adatairól, lak- és értesítési címéről, tartózkodási helyéről, valamint telefonos és egyéb elérhetőségeiről.⁵⁰⁵

Továbbá büntetőjogi kódexünk alapvetően előírja, a terhelt igazmondási kötelezettsége alapján, hogy azokra a kérdésekre is válaszolnia kell, amelyek azonosságának megállapítását célozzák, még abban az esetben is, ha egyéb kérdésekre adandó válaszadását megtagadja.⁵⁰⁶

A kihallgatás során kulcsfontosságú az érintett személyazonosságának pontos meghatározása, ami alapvetően szükséges annak érdekében, hogy a bíróság, az ügyészség, valamint a nyomozó hatóság minden kétséget kizáróan tudja azonosítani a vizsgált személyt. Ennek jelentősége az eljárásban az, ha az ügydöntő határozat a terheltet nem a valós személyazonosságával tünteti fel, és ez a tévedés nem korrigálható, akkor az adott ügyben a perújítás válik lehetővé.⁵⁰⁷

A gyanúsított személyazonosságának rögzítésekor nem szükséges az összes, a Büntetőeljárás törvényben felsorolt személyes adatot dokumentálni. Mándi véleménye szerint elég lehet csak azon személyes adatok rögzítése, amelyek az azonosításhoz szükségesek és elégségesek az adattakarékosság elve alapján.⁵⁰⁸ Ez valóban megfelelne az adatminimalizálás elvének⁵⁰⁹, de kérdés, hogy milyen adat elég az azonosításhoz, másrészt, ha az adat a természetes személyes adattal kapcsolatba hozható, (vagy az helyreállítható)⁵¹⁰ márpedig az azonosítás ezt a célt szolgálja, ez az érintett szempontjából mekkora jelentőséggel bír. Az azonosíthatóság

⁵⁰³ Be. 113. § (2) bekezdés.

⁵⁰⁴ A Be. szerint az idézés módjai: Az idézés, illetve az értesítés módjai: írásban, kézbesítés útján: ez a leggyakoribb idézési/értesítési mód, ilyenkor a papíralapú idézést vagy értesítést zárt iratban kell kézbesíteni, vagy kizárólag hangkapcsolatot biztosító elektronikus úton.

⁵⁰⁵ Be. 184. § (2)

⁵⁰⁶ Btk. 342. § (1) c) pont.

⁵⁰⁷ Be. 637. § (1), c), „Perújításnak van helye (...)a terhelt az ügydöntő határozatban nem a valódi személyazonosságával szerepel és ez a határozat kijavításával nem orvosolható”

⁵⁰⁸ Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.56

⁵⁰⁹ GDPR 5.cikk.c)

⁵¹⁰ Infotv. 4. § (3). „A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható”

kérdésével a Kúria is foglalkozott, melyről még a későbbiekben lesz szó. Miután a személyes adatok rögzítése megtörtént, a gyanúsítottat tájékoztatják az eljárás során fennálló jogairól és kötelezettségeiről. Ezen a ponton lehetősége van további, nem kötelező jellegű személyes adatok megadására, mint például iskolai végzettség, jövedelmi helyzet, vagyoni helyzet, családi állapot, egészségi állapot. Az egészségügyi állapotáról szóló adatok a személyes adatok különleges kategóriáiba sorolhatók.⁵¹¹

Az eljárási cselekményekkel kapcsolatos tájékoztatásnak ki kell terjednie a személyes adatok zártan kezelésének lehetőségére, magára a tájékoztatási jogra, valamint arra, hogy az eljárási cselekmény során megismert adatok és az eljárási cselekményen tapasztaltak személyes adatnak, illetve védett adatnak minősülnek, és annak kezelése csak jogszabályban meghatározottak szerint lehetséges, valamint az ügyiratok megismerésére való jogosultságra is.⁵¹²

A nyomozás során történő eljárási cselekményekkel kapcsolatosan más hatóságok közreműködése is szükségessé válhat.⁵¹³

A nyomozás során készült jegyzőkönyv tartalmazza a Be. előírásait, és ezenkívül a 100/2018. (VI. 8.) Korm. rendelet alapján⁵¹⁴ a személyes adatokkal kapcsolatban elrendeli, hogy az eljárási cselekményen jelen lévő büntetőeljárásban részt vevő személy személyes adatait a személyazonosságának megállapításához és a későbbi elérhetőségének biztosításához szükséges mértékben kell a jegyzőkönyvben rögzíteni, és kérésére zártan kell kezelni.⁵¹⁵

⁵¹¹ Infotv. 3. § (3).. „(...) különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok”

⁵¹² 100/2018. (VI. 8.) Korm. rendelet, 42.§.(3).h), (i)

⁵¹³ 100/2018. (VI. 8.) Korm. rendelet, 29.§ (1). Amennyiben a büntetőeljárás kontextusában a nyomozó hatóság megállapítja, hogy a rendőrségről szóló törvény vagy a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény által előírt intézkedésre van szükség, mivel a törvényben meghatározott feltételek fennállnak, az illetékes hatóságnál kezdeményezi a rendészeti intézkedés megtételét, vagy adott esetben, amennyiben rendelkezik az ehhez szükséges jogosultsággal, a nyomozó hatóság egyik tagja maga hajthatja végre az intézkedést.

⁵¹⁴ 100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól - A Kormány a büntetőeljárásról szóló 2017. évi XC. törvény 866. § (1) bekezdés *b*) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva hozta létre a rendeletet.

⁵¹⁵ 100/2018. (VI. 8.) Korm. rendelet, 5.§ (2)

2.2. A tanú személyes adatainak kezelése

Amennyiben a nyomozó hatóság valakit tanúi minőségben kíván meghallgatni, tanúként történő idézésre kerül sor.⁵¹⁶ Az idézés tartalmazza a tanú nevét, születési idejét és lakcímét. Az idézés és az értesítés kézbesítés útján, kizárólag hangkapcsolatot biztosító elektronikus úton, vagy a bíróság, az ügyészség, illetve a nyomozó hatóság előtti megjelenés alkalmával szóban történik.⁵¹⁷ Annak érdekében, hogy illetéktelen személyek ne szerezzenek tudomást arról, hogy valakit büntetőeljárásban tanúként kívánnak meghallgatni, a Be. előírásai szerint a papíralapú idézéseket vagy értesítéseket zárt borítékban kell kézbesíteni.⁵¹⁸

A tanúk meghallgatása sorrendben, egymás után történik. A meghallgatás elején a tanú személyazonosságának ellenőrzésére kerül sor, amely személyi igazolvány, útlevél, jogosítvány vagy bármely más, a személyazonosság igazolására alkalmas okirat alapján történhet.⁵¹⁹ A tanú részére kizárólag a vallomását tartalmazó jegyzőkönyvről, jegyzőkönyvrészletről adható ki iratmásolat, így értelemszerűen ők a teljes iratanyag megismerésére és másolatára nem jogosultak.⁵²⁰

A büntetőeljárás során illetékes hatóság vagy bíróság bármikor, saját kezdeményezésre vagy a tanú, illetve képviselőjében eljáró ügyvéd kérésére, elrendelheti a tanú személyes adatainak bizalmas, azaz zártan kezelését. E kezelési mód alatt a tanú nevén kívüli egyéb személyes adatait külön kezelik és bizalmasan tartják, amelyekhez kizárólag az adott ügyben eljáró bíró, ügyész vagy nyomozó szerv férhet hozzá. Ezen adatok nem kerülhetnek nyilvánosságra az eljárás dokumentumaiból, illetve a kiadott másolatokból. Az eljáró hatóságok és bíróság köteles ezen rendelkezés betartását garantálni. A tanú adatainak nyilvánosságra hozatalát csak a tanú hozzájárulásával lehet feloldani. Ennek ellenére, ha a tanú személyes adatai bizalmas kezelésre kerülnek is, az eljárási cselekményre történő megidézés esetén kötelező személyesen megjelenni és tanúvallomást tenni. Pálvölgyi felveti, ha egy eljárás terheltje tanúvá válik, gyakran felesleges lehet a zárt adatkezelés kérése, még akkor is, ha személyes adatainak védelme fontos szempont. Ennek oka, hogy amíg valaki terheltként szerepel egy ügyben, addig

⁵¹⁶ 112. § (1) A bíróság, az ügyészség és a nyomozó hatóság azt idézi, akinek a jelenléte az eljárási cselekménynél kötelező, és azt értesíti, akinek a jelenléte nem kötelező, de azt a törvény lehetővé teszi.

⁵¹⁷ Be.113. § (1)

⁵¹⁸ Be. 113. § (2)

⁵¹⁹ Be. 85-88. §

⁵²⁰ Az iratokról történő másolatadásra vonatkozó rendelkezéseket kell alkalmazni a kép- vagy hangfelvételtől, a képet és hangot egyidejűleg tartalmazó felvételtől készített másolat kiadására is.

adatai szerepelnek az ügy irataiban, például a jegyzőkönyvekben, és azok, akik jogosultak az iratok megtekintésére, hozzáférhetnek ezekhez az adatokhoz.⁵²¹ Speciális körülmények között előfordulhat, hogy a tanú nevének bizalmas kezelése is elrendelhető, ebben az esetben a tanú egy egyedi sorszám alapján azonosítható az eljárás során.⁵²² A különösen védett tanú esetében a védő sem ismeri a tanú semmilyen adatát vagy személyét.⁵²³

A tanú személyes adatainak zártan kezelése az információs önrendelkezéshez való joggal összhangban áll.⁵²⁴

A Be. ezen rendelkezései biztosítják, hogy a büntetőeljárás során a tanúk személyes adatai megfelelő védelemben részesüljenek.

2.3. A vádlott személyes adatainak kezelése

A vádlottak személyes adatainak kezelése a vádemelési szakaszban történik. Ebben a szakaszban az ügyészség átvizsgálja a nyomozás során összegyűlt dokumentációkat. Ezután hoz döntést arról, hogy szükséges-e ügyészi intézkedést vagy határozatot hozni, megfontolni az egyezség kezdeményezését, alkalmazni az eljárás felfüggesztését közvetítői eljárás céljából, bevezetni a feltételes ügyészi felfüggesztést, lezárni az eljárást valamilyen okból, vádat emelni, a vizsgálat során eljárási lépéseket megtenni, külön eljárást indítani, ügyeket egyesíteni, vagy az ügyet áthelyezni.⁵²⁵

Amennyiben az ügyészség vádat emel, azt vádirat formájában teszi meg, amelynek egy jogszabályban meghatározott alapvető eleme a vádlott pontos azonosítására szolgáló adatok megadása. Ez azért szükséges, mivel az ismeretlen személy elleni vádemelés nem felel meg a törvényi előírásoknak.⁵²⁶ A vádirat tartalmazza a vádlott nevét, születési helyét és idejét, lak-

⁵²¹ Pálvölgyi, Ákos.(2014)"A hírérték margóján: személyhez fűződő jogok védelméhez való jog a büntetőeljárásban különös tekintettel a személyes adatok védelmére." *Büntetőjog Szemle* (3) pp. 41-45.

⁵²² Be. 25.§

⁵²³ Hesz, Tibor és Kőhalmi, László.(2009) "A tanúvédelem a terhelt védőjének aspektusából." In *A tanú védelmének elméleti és gyakorlati kérdései*, szerkesztette Mészáros Bence, 101-102. Pécs: Pécsi Tudományegyetem, Gazdasági Büntetőjogi Kutatóintézet. p.98.

⁵²⁴ ABH. 2010, 562. „Nincs alkotmányos alap vagy cél, ami lehetővé tenné a nyomozó hatóság, az ügyész vagy a bíróság számára, hogy a tanú fenyegettségének objektív alapjait vizsgálva és a kérelem teljesíthetőségét mérlegelve megtagadják ezt a kérelmet."

⁵²⁵ Be. 391. § (1) bekezdés.

⁵²⁶ Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.58.

és tartózkodási helyét, értesítési címét, személyazonosító okmányának számát, valamint állampolgárságát. A büntetőeljárás során a bíróság a nyomozati iratok és a vádirat beérkezését követően a vádiratot a vádlottnak és annak védőjének kézbesíti.⁵²⁷ Ebben a szakaszban adatvédelmi szempontból jelentősége van annak, hogy milyen intézkedések biztosítják a vádirat biztonságát és azt, hogy illetéktelen személyek ne férjenek hozzá a dokumentumhoz, amely részletesen tartalmazza a vádlott személyes adatait, a rá vonatkozó bűnügyi vádak, a vádak tényállását és a cselekmények jogi megítélését.⁵²⁸ Ez megfelel az Infotv. rendelkezésnek, miszerint az adatokat olyan módon kell kezelni, hogy „*biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével,(...) szembeni védelmet is ideértve.*”⁵²⁹

A jogszabályok értelmében a jogalkotó előírja,⁵³⁰ hogy azokat a papíralapú ügyiratokat, melyek átvételéhez jogi következmények kapcsolódnak, vagy amelyek átvételének igazolása szükséges, hivatalos iratként kell postázni⁵³¹ büntetőeljárás keretében, amikor a vádirat kézbesítésre kerül, az A/4. jelzésű értesítést kell alkalmazni, ami azt jelenti, hogy az iratot személyesen, a címzett saját kezébe kell kézbesíteni.⁵³²

Miután a vádiratot a vádlottnak és annak védőjének kézbesítették, a bíróság előkészítő ülést hirdet meg a büntetőügyben. Ezen az ülésen a vádlottat és a védőt írásban idézik, míg az ügyészt tárgyalási jegyzékkel értesítik.⁵³³ Az előkészítő ülés előtt a tárgyalóterem bejáratánál a jegyzőkönyvvezető kihelyezi a napi tárgyalási jegyzéket. Ennek tartalmaznia kell aznap tárgyalásra kerülő ügyek adatait, beleértve az ügyek sorrendi sorszámát, az ügyszámot, az ügy tárgyát, a tárgyalás kezdési időpontját, valamint a vádlottak neveit. Ez a gyakorlat elősegíti az érintett felek pontos és időben történő informálását.^{534, 535}

A tárgyalási jegyzék adatvédelmi szempontból releváns a bírósági eljárásokban.

⁵²⁷ Be. 497. §.

⁵²⁸ Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.58.

⁵²⁹ (EU) 2016/680 4.cikk.f) és Infotv. 4.§.(4a)

⁵³⁰ 12/2018. (VI. 12.) IM rendelet

⁵³¹ 12/2018. (VI. 12.) IM rendelet 30. §

⁵³² 12/2018. (VI. 12.) IM rendelet 30. § (4) bekezdés e) pont.” A büntetőeljárásban A/4. jelzésű értesítést kell használni (...) a vádirat Be. 497. §-a alapján történő kézbesítésekor.”

⁵³³ Be. 499. § (2) bekezdés

⁵³⁴ A bírósági ügyvitel szabályairól szóló 14/2002. (VIII. 1.) IM rendelet 19. § (2), (3) bekezdés.

⁵³⁵ Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.59.

A bíróság épületében kifüggesztett tárgyalási jegyzék bárki számára hozzáférhető, amely tartalmazza a büntetőeljárásban érintett személyek személyes adatait, mint például a vádlott nevét és az ügy részleteit. Ez a gyakorlat ellentmondásban állhat a személyes adatok védelmére vonatkozó előírásokkal, tekintettel arra, hogy ezek az adatok bűnügyi személyes adatoknak minősülhetnek, amelyek a személyes adatok különleges kategóriáiba tartozó információk. Németh megfogalmazása szerint „*A tartalomból kifolyólag bűnügyi személyes adat(ok)ról van szó, a contrario ezek nem nyilvános adatok, de mégis a bíróság épületében, bárki által szabadon látogatható helyen kerülnek kifüggesztésre. Az igazságszolgáltatás nyilvánossága és a személyes adatok védelme áll összeütközésben egymással.*”⁵³⁶ Digitalizált világunkban a jegyzék adatai könnyen lefényképezhetők és terjeszthetők. Ezek az adatok a büntetőtárgyalás nyilvánosságának elve alapján megjelenhetnek az írott vagy elektronikus sajtóban, ám jelentős különbség, hogy ezek az információk tipikusan csak anonimizált formában kerülnek közzétételre, általában a büntetőeljárás ügydöntő határozatának meghozatala után.⁵³⁷

A vádirat ismertetését követően a bíróság rögzíti a vádlott személyes adatait, majd tájékoztatja őt az eljárásbeli jogairól és kötelezettségeiről. A vádlott ezután nyilatkozik a vádirat és a tájékoztatás megértéséről, és a tárgyalás előtt a vádlott és a védő kifejtheti álláspontját a váddal kapcsolatban, valamint közreműködhet a büntetőeljárás további menetének alakításában.⁵³⁸

Véleményem szerint a beépített adatvédelem elvét figyelembe véve, az adatkezelőnek aktív lépéseket kell tennie az adatok védelme érdekében vádeljárásnak ebben a fázisában is, mint például a fotózás tiltása vagy a jelenlévők figyelmének felhívása az adatvédelmi szabályok betartására. Amennyiben ezek az intézkedések hiányoznak, a bírósági tárgyalási jegyzék nyilvánosságra hozatala adatvédelmi kockázatot jelenthet a modern technológia által könnyített adatmegosztás miatt, ahol egy fotó gyorsan és egyszerűen továbbítható. Egyetértek Németh azon javaslatával, hogy a tárgyalási jegyzéken csak az ügyszám szerepeljen.⁵³⁹

⁵³⁶ Németh, Kata. (2019) "A büntetőeljárás nyilvánosságának jogszabályi háttérében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." *Debreceni Jogi Műhely* 16, no. 1-2 pp.55- 76. (DOI 10.24169/DJM/2019/1-2/5.

⁵³⁷ Ibid., Németh Kata." Itt nyilvánul meg az alapjogsérelem a büntetőeljárás alanya oldalán. Az ellentmondást abban látom, hogy amíg az Info.tv foggal körömmel védi büntetőeljárás bírósági szakaszában a bűnügyi személyes adatokat, addig a bíróság folyosóján, mint ügyfélforgalom előtt nyitva álló helyiségben kifüggesztésre kerül, sőt, arról akár képfelvétel is készíthető, amely nyilvánosságra is hozható."

⁵³⁸ Be. 499. § (1) bekezdés.

⁵³⁹ Németh Kata A büntetőeljárás nyilvánosságának jogszabályi háttérében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." p.62.

2.4. A sértett személyes adatainak védelme

A sértett az a természetes vagy nem természetes személy, akinek vagy amelynek a jogát vagy a jogos érdekét a bűncselekmény közvetlenül sértette vagy veszélyeztette.⁵⁴⁰ A sértett jogait az eljárás során a Be. az 51. szakasz a) – f) pontokban sorolja fel. Adatvédelmi tárgykörbe is tartozik, „*hogy jogosult arra, hogy az őt érintő bűncselekménnyel összefüggésben keletkezett ügyiratokat – az e törvényben meghatározott kivételekkel – megismerje,⁵⁴¹ a büntetőeljárás jogairól és kötelességeiről a bíróságtól, az ügyészségtől és a nyomozó hatóságtól felvilágosítást kapjon.*⁵⁴² A sértett jogosult arra is, hogy kérelmére tájékoztassák az őt érintő bűncselekménnyel összefüggésben.⁵⁴³ Az érintettek jogait megillető jogosultságok körén belül a hozzáférési jog alapján a Be. ezen rendelkezés az Infotv. 14. szakasza b) pontjának megfeleltethető.

A sértetti személyes adatok, úgymint lakcíme, értesítési címe, tényleges tartózkodási helye, kézbesítési címe, telefonos elérhetősége, elektronikus levelezési címe, vagy más elektronikus elérhetősége, és ennek megváltozásai esetén annak bejelentése az eljárás részei (bíróság, ügyészség, vagy nyomozó hatóság)⁵⁴⁴

A sértettnek a nyomozás és a bírósági eljárás során járó jelenléti és iratmegtekintési jogaik nagyjából megegyeznek a terheltek számára biztosított jogokkal, azzal a különbséggel, hogy a sértett nem lehet jelen a terhelt kihallgatásánál. A nyomozás időszakában a sértett iratbetekintési joga korlátozott, de a bírósági szakaszban ez a jog kiterjedtebbé válik, és a sértett hozzáférhet az őt érintő bűncselekmény irataihoz, amennyiben ez nem sérti az adatvédelmi szabályokat vagy az eljárás zavartalanságát. Ez a nyomozási szakban a sértettre vonatkozóan az előzetes tájékoztatói jog⁵⁴⁵ adatkezelési célból szükséges korlátozása.⁵⁴⁶

⁵⁴⁰ Be.50. §

⁵⁴¹ Be.51. §, (1) d)

⁵⁴² Be.51. § (2) e)

⁵⁴³ Be. 51. § (5) a) – f)

⁵⁴⁴ Be. 51. § (6) (b)

⁵⁴⁵ Infotv.14§.a) előzetes tájékoztatóhoz való jog

⁵⁴⁶ Infotv.16.§ (3), a „ (...)tájékoztatás teljesítését az elérni kívánt céllal arányosan az adatkezelő késleltetheti, a tájékoztatás tartalmát korlátozhatja vagy a tájékoztatást mellőzheti,(...) az általa vagy részvételével végzett vizsgálatok vagy eljárások – így különösen a büntetőeljárás – hatékony és eredményes lefolytatásának, (...) a bűncselekmények hatékony és eredményes megelőzésének és felderítésének,(...)biztosításához.”

A sértett jogosult az eljárás során beadványok benyújtására, észrevételek megfogalmazására, kérdések feltevésére a vádlottnak, szakértőknek, tanúknak, továbbá kérdésfeltevés kezdeményezésére, és a bizonyítási eljárás lezárulta után, az ügyész perbeszédét követően, szólalhat fel.

A sértettet a büntetőeljárás jogairól és kötelezettségeiről tájékoztatni kell, nem csak kérésre.

A vádemelés tényéről az ügyésznek, az ítélethirdetésről pedig a bíróságnak kell értesítenie a sértettet, amely többnyire postai úton történik. A sértett, valamint a magánvádló, a pótmagánvádló, a magánfél és ezek képviselője jogosult a bírósági eljárás során az őket érintő bűncselekményre vonatkozó iratok hiteles vagy nem hiteles másolatának megkérésére, kivéve, ha a jogszabály kifejezetten kizárja az iratmásolat kiadását. Ez a jog nem sértheti az emberi méltóságot, személyiségi és kegyeleti jogokat, és nem vezethet a magánéletre vonatkozó információk indokolatlan közzétételéhez.⁵⁴⁷ A sértett továbbá köteles a lakcímét, értesítési címét, tényleges tartózkodási helyét, kézbesítési címét, telefonos elérhetőségét, elektronikus levelezési címét vagy más elektronikus elérhetőségét és – a változást követő három munkanapon belül – ennek megváltozását az eljáró bírósággal, ügyészszéggel vagy nyomozó hatósággal közölni.⁵⁴⁸

Sértetti jogutódlás esetén ugyanezen kötelezettségei és jogai vannak a jogutódnak.⁵⁴⁹

Értelemszerűen a magánvádló, a pótmagánvádló, és a magánfél jogi és kötelezettségeit is a Be. szabályozza, személyes adatait illetően is azonos kötelezettségek és jogok illetik meg. Ugyanez vonatkozik a vagyoni érdekelt és az egyéb érdekelt vagy ezek segítőjének személyes adataira is.⁵⁵⁰

3. A szakértő a büntetőeljárásban és a személyes adatok védelme

A szakértő a büntetőeljárásban az egyéb érdekelték körébe sorolható. A Be. 188. szakasza (1) bekezdése szerint *„ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni.”* A szakértői vizsgálat során köteles és

⁵⁴⁷ Be. 51. §, (1) d), e), (5), 93. §, (b)

⁵⁴⁸ Be.51§. (6). b)

⁵⁴⁹ Be. 52. §

⁵⁵⁰ Be., 65. §, 69. §, 70/B. §,

jogosult a szakértő azokat az adatokat megismerni, melyek a feladatának teljesítéséhez szükségesek, az eljárás ügyiratait is – kivéve amit a törvény kizár megismerheti.⁵⁵¹

A szakértőt illetően a szóbeli előterjesztés előtt az eljáró bíróságnak meg kell állapítani a szakértő személyazonosságát. A bírósági eljárásokban a szakértői meghallgatás során a tanúkihallgatás szabályait kell megfelelően alkalmazni.⁵⁵² Az írásban benyújtott szakvélemény lényegi elemeit az egyes bíró, vagy a tanács elnöke, esetlegesen az ügyész, a vádlott, vagy annak védője kezdeményezésére kell nyilvánosan felolvasni, vagy a tárgyalási jegyzőkönyv vezetőjével felolvasatni.⁵⁵³

Az igazságügyi szakértő véleményét a fentiek alapján a nyilvános tárgyaláson bárki megismerheti. A szakértői vélemény gyakran tartalmaz különleges adatokat, többek között a sértett egészségügyi állapotára is vonatkozó adatokat. Ezek megismerése a nyilvános tárgyalás esetében bárki számára lehetséges. Nyilvánvaló, hogy nem lehet minden esetben zárt tárgyalást elrendelni, a Be. taxatívén felsorolja az erre vonatkozó lehetséges feltételeket⁵⁵⁴, köztük az erkölcsi okból történő elrendelést is. Mándi véleményével egyetértve, azonban egyedi esetekben az „erkölcsi okból” történő elrendelése megoldás kínálhat.⁵⁵⁵ „A törvényben megjelölt „erkölcsi ok” a gyakorlatban átfoghatja azokat az eseteket is, amikor a nyilvánosság kizárását a felnőttkorú terhelt jogainak, jogos érdekeinek, emberi méltóságának, jóhírének, személyes adatainak védelme indokolja”⁵⁵⁶

Az egészségügyi adatok mint különleges (és a védett) adatok kezelése okán Németh egy sajátos fogalom az „ igazságügyi adat” bevezetését javasolja. „Az igazságügyi adat specifikumát a bírósági közegben való lét, megjelenés adja.”⁵⁵⁷ Hivatkozik Harangozó véleményére miszerint „ki kell választani bizonyos adatokat, amelyekkel összefüggésben, azt kell mondani, hogy ezek másképpen védendők bírósági eljárásokban, azaz csak abban és ott másfajta védelembe részesülnek.”⁵⁵⁸ Amint az adat kikerül a bírósági kontextusból, ismét

⁵⁵¹ Be.192.§. a)

⁵⁵² Be. 529. § (1)

⁵⁵³ Be. 530. § (1)

⁵⁵⁴ Be. 436.§ (4)

⁵⁵⁵ Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p. 59

⁵⁵⁶ 58/1995. (IX. 15.) AB határozat.

⁵⁵⁷ Németh, Kata. „A büntetőeljárás nyilvánosságának jogszabályi háttérében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." p.70.

⁵⁵⁸ Harangozó, Attila. "Az igazságügyi adatkezelésről és tájékoztatásról szóló törvény koncepciója." Kézirat előadás a konferencián. Debrecen, 2014. március 14. 3. o., Idézi: Németh Kata Ibid. p.64.

személyes vagy különleges adatnak minősül, ami azt jelenti, hogy eredeti keletkezése szerinti módon kell megóvni és védeni azt. Álláspontom szerint –bár a bírósági eljárás valóban különbözik az adatok kezelése, feldolgozása tekintetében más közigazgatási területektől, elég csak a tárgyalás nyilvánosságának elvére gondolni – az igazságügyi adat fogalmának bevezetése nem lenne szerencsés abban a tekintetben, hogy többszörös „feladatot” jelentene az eljáró szervek számára, hiszen még büntetés-végrehajtási fázisban is kerülhet sor bírósági adatkezelésre, ebben az esetben az érintett személyes adatai többféle minőségben részesülnének.

Az adatok zártan kezelése megoldást jelenthetne, azonban a Be. szerint a személyes adatok zártan történő kezelése⁵⁵⁹ esetén sem az egészségügyi adatok, sem más különleges adatok nem kerülnek felsorolásra.

4. Az adatkezelés jogalapja és az adatvédelem a büntetőeljárás törvényben

A Be. külön fejezetet szentel a büntetőeljárásban kezelt adatok védelmének. A XV. fejezet 97. szakasza szabályozza az adatkezelés jogalapját, és az általános adatvédelmi elveket. A büntetőeljárás során a bíróság, az ügyészség és a nyomozó hatóság jogosult minden olyan személyes adat megismerésére és kezelésére, amely ezen törvény keretében meghatározott feladatok végrehajtásához elengedhetetlen.⁵⁶⁰ A büntetőeljárás céljából – a jogszabályok által szabályozott módon és terjedelemben – a bíróság, az ügyészség és a nyomozó hatóság hozzáférhet és felhasználhat olyan adatokat, amelyek törvény által védett vagy bizonyos szakmák gyakorlásával összefüggő titkokat tartalmaznak - ezeket a továbbiakban "védett adatoknak" nevezzük - amennyiben ezek az adatok az említett törvényben foglalt kötelezettségek teljesítéséhez szükségesek.⁵⁶¹

A büntetőeljárás során a bíróság, az ügyészség és a nyomozó hatóság kötelezettséget vállal arra, hogy a kezelésükben lévő védett adatokat óvják a szükségtelen nyilvánosságtól, megakadályozzák, hogy illetéktelenek tudomására jussanak, és garantálják a személyes adatok védelmét. Ezek az intézmények kizárólag a törvényi előírásoknak megfelelően teszik hozzáférhetővé a büntetőeljárás során kezelt személyes és védett adatokat.

⁵⁵⁹ Be. 99.§. (1)

⁵⁶⁰ Be. 97.(1). §

⁵⁶¹ Be. 97.(2). §

A fent említett követelmények biztosítása érdekében az alábbi intézkedéseket szükséges alkalmazni:

- A pénzmosás és a terrorizmus finanszírozásának megelőzésével és megakadályozásával kapcsolatos törvény alapján a pénzügyi információk védelme céljából a pénzügyi információs egység operatív elemzés eredményeit tartalmazó dokumentumokat zártan kell kezelni.
- Amennyiben egy érintett személy személyes adatainak zártan történő kezelését közigazgatási, polgári peres vagy egyéb eljárásokban elrendelték, az adatok védelme érdekében az érintett személyes adatait tartalmazó dokumentumokat, az érintett kihallgatásáig zártan kell kezelni.
- Valamint a panaszok, közérdekű bejelentések és a visszaélések bejelentésével kapcsolatos törvény szerinti védelem biztosítása érdekében a közérdekű bejelentők vagy a visszaélést jelentő személyek kihallgatásáig a bejelentéseket tartalmazó dokumentumokat szintén zártan kell kezelni.⁵⁶²

A zárt adatkezeléssel kapcsolatosan meg kell említenünk az iratkohoz való hozzáférések jogát az e- ügyintézés területén. Róth, a digitális ügyintézés kifejti, hogy a Be. elektronikus hozzáférési lehetőséget kínál az ügyiratokhoz, és lehetővé teszi a másolatok adathordozóra történő átmásolását is. A Digitális Bíróság Projekt keretében bevezetett újítások közé tartozik az ügyiratok elektronikus formába való átalakítása (E-akta) és az iratok elektronikus úton történő megtekintésének lehetősége, amelyhez az ügyészek, a terheltek, a védők és azok törvényes vagy jogi képviselői jogosultak, az előzetes azonosítás és az online betekintési kérelem benyújtása és elbírálása után. A zártan kezelt adatok védelme az E.akta rendszerben is biztosított.⁵⁶³

Amennyiben az érintett adatkörre vonatkozó jogszabály másként nem rendelkezik, a büntetőeljárásban érintett szereplők e törvény által meghatározott kereteken belül ismert személyes adatokat és védett adatokat csak saját jogosultságaik érvényesítése vagy kötelezettségeik teljesítése érdekében, szükséges mértékben és időtartamig kezelhetik.⁵⁶⁴

⁵⁶² Be. 98. § (1). – (2)

⁵⁶³ Róth, Erika. (2021) "A digitalizáció és a terhelti jogok érvényesülése a büntetőeljárásban." *Miskolci Jogi Szemle* 16, no. 1, különszám pp.270-278.

⁵⁶⁴ Be. 98.§ (3), Infotv. 4.§,(2.)

A büntetőeljárás során kezelt személyes adatok és védett adatok törlése kizárólag e törvény előírásainak megfelelően történhet az eljárás befejezéséig.

A büntetőeljárásban megismert személyes adatokat – amennyiben azok egyedi azonosításra alkalmatlanná válnak – statisztikai célokra felhasználhatóak.⁵⁶⁵

5. A személyes adatok zártan történő kezelése

A Be. a XV. fejezetben a 99. szakasza alapján szabályozza a személyes adatok zártan történő kezelését. Eszerint a bíróság, az ügyészség és a nyomozó hatóság kezdeményezésre határozatot hoz arról, hogy a sértett, a vagyoni jogok érdekében eljáró személy és az egyéb érintettek, valamint az őket támogató személyek nevét, születési nevét, születési helyét és idejét, anyjuk nevét, állampolgárságukat, személyazonosító okmányaik számát, lakcímüket, értesítési címüket, valós tartózkodási helyüket, postázási címüket és elektronikus elérhetőségeiket különleges védelem alá helyezi, azaz zártan kezeli ezeket az információkat.⁵⁶⁶

A kérelmet a sértett, a vagyoni jogokban érintett személy, valamint az egyéb érintett vagy az őket segítő személyek nyújthatják be⁵⁶⁷ valamint a sértettek védelmében a bíróság, az ügyészség és a nyomozó hatóság kezdeményezés nélkül is dönthet a személyes adatok zárt kezeléséről.⁵⁶⁸

A bíróság, az ügyészség és a nyomozó hatóság az érintettek hozzájárulásával feloldhatja bizonyos személyes adatok ilyen módon történő kezelését.⁵⁶⁹

A zártan kezelt személyes adatok kezelése kizárólag az ügyben eljáró bíróság, ügyészség és nyomozó hatóság hatáskörébe tartozik. Ezek az adatok az érintett hozzájárulása nélkül csak az ügyben közreműködő bíróság, ügyészség és nyomozó hatóság számára, az áldozatsegítő szolgálat számára az áldozatsegítési feladatok végrehajtása céljából, valamint a mediációs tevékenységet végző pártfogó felügyelet részére a közvetítési eljárás lebonyolításához szükséges mértékben adhatók át.⁵⁷⁰

Az zártan kezelt iratokból a zárt adatkezeléstől érintetlen részeket az általános szabályoknak megfelelően hozzáférhetővé kell tenni, például olyan kivonat készítésével, amely a zártan

⁵⁶⁵ Be. 98. § (3). – (4) - (5)

⁵⁶⁶ Be. 99.§ (1)

⁵⁶⁷ Be. 99.§ (2)

⁵⁶⁸ Be. 99.§ (3)

⁵⁶⁹ Be. 99.§ (4)

⁵⁷⁰ Be. 99.§ (5)

kezelt adatokat nem tartalmazza. A zárt adatkezelés nem jelenti azt, hogy a bíróság, az ügyészség vagy a nyomozó hatóság ne vehetné fel és ne továbbíthatná a zártan kezelt adatokat azon ügyiratokban, amelyek a büntetőeljárás feladatainak elvégzéséhez nélkülözhetetlenek, még az érintett fél beleegyezése nélkül is. A zártan kezelt adatok felhasználását követően, kivéve a vádiratot, az eljárást lezáró vagy megszüntető határozatokat, valamint az ügydöntő határozatot és a külön törvényi rendelkezés alapján kezelt iratokat, az említett iratokat újból zártan kell kezelni, így biztosítva az adatok védelmét.⁵⁷¹

A Be. az adatvédelmi szabályozástól függetlenül is szabályozza az eljárás ügyiratainak megismerését és zártan kezelését.⁵⁷² A büntetőeljárásban az ügyiratokhoz való hozzáférés alapvető jogok és eljárási garanciák közé tartozik, amelyet a terhelt és védője, a sértett, valamint az egyéb és vagyoni érdekeltek is gyakorolhatnak, indítvány alapján. Ez a jog kiterjed minden releváns ügyírátra, beleértve a bíróság, az ügyészség és a nyomozó hatóság által beszerzett vagy a büntetőeljárás során benyújtott dokumentumokat és bizonyítékokat. A zárt ügyiratkezelés elsősorban a személyes adatok zárt kezelésére vonatkozó ügyiratokat érinti, de más helyzetekben is szükségessé válhat. Ilyen körülményeket szabályoz a jogszabály például speciális kezelést igénylő esetekben, különösen védett tanúk esetében, vagy bizonyos kizárt bizonyítékok kapcsán. Az ügyiratok zárt kezelése a büntetőeljárás során kiterjedt védelmet nyújt a zártan kezelt dokumentumok és azokban szereplő adatok számára, mivel ilyenkor a büntetőeljárás résztvevői nem rendelkeznek megismerési vagy iratbetekintési jogosultsággal. Az ügyészség és nyomozó hatóság közötti belső kommunikáció azonban nem része az ügyiratoknak.

Az eljárás során az ügyiratokhoz való hozzáférés különböző módon biztosítható, mint például a dokumentumok megtekintésével, az ügyiratok tartalmáról szóló tájékoztatással, másolatok vagy felvételek készítésével, vagy az ügyiratok kivonatainak kézbesítésével. Ezen jog gyakorlását nem befolyásolják a zártan kezelt ügyíratokra vonatkozó külön rendelkezések.⁵⁷³

⁵⁷¹ Be. 99.§ (8)- (10)

⁵⁷² A Büntetőeljárás törvény 102. § (3) bekezdése értelmében, ha egy ügyirat zárt kezelés alá esik, akkor a bíróság, az ügyészség és a nyomozó hatóság gondoskodik arról, hogy az ilyen ügyirat vagy annak tartalma ne váljon ismertté az eljárás többi dokumentumából vagy adataiból, valamint, hogy az ügyiratok megismerése ne vezessen a zártan kezelt dokumentumok felfedéséhez.

⁵⁷³ Be. 99. § (8) – (10) Az ügyiratok zárt kezelése nem zárja ki azok részleges megismerését, amennyiben ez az általános eljárási szabályokkal összhangban áll. Ebben az esetben a hatóság gyakran készít kivonatot, hogy az ügyiratok nem zártan kezelt részeit hozzáférhetővé tegye. A zárt adatkezelés nem jelent akadályt arra, hogy az

A bíróság, az ügyészség és a nyomozó hatóság korlátozhatja az ügyiratokhoz való hozzáférés jogát bizonyos esetekben, például amikor az eljárás érdekeit szem előtt tartva, a nyomozás befejezéséig szükségesnek ítéli, vagy amikor a dokumentumok átvizsgálása még folyamatban van. A hozzáférési jog korlátozásait határozat formájában kell meghozni, és azok ellen nincs helye jogorvoslatnak.⁵⁷⁴

Ez a szabályozás biztosítja azt a célt, hogy megfelelő egyensúlyt teremtsen az eljárásban érintettek jogainak védelme és az eljárás hatékonysága között, megőrizve az igazságszolgáltatás integritását.

Kiemelném, hogy a törvény meghatározza a hozzáférési jogokat illetően az illetékes hatóságokat. A büntetőeljárás során a bíróság, az ügyészség, közjegyzők, bírósági végrehajtók, az állami adó- és vámhatóság, pártfogó felügyelők, nyomozó hatóságok, közigazgatási és kormányzati ellenőrzési szervek, valamint a Nemzeti Adatvédelmi és Információszabadság Hatóság, a rendőrség belső bűnmegelőzésért és bűnfelderítésért felelős egységei, a terrorizmus elleni szervei és a katonai parancsnokok jogosultak az őket érintő feladatok végrehajtásához szükséges információkhoz hozzáférni az eljárás dokumentumai közül. E hozzáférési jog a nyomozás lezárásáig, az eljárás érdekeit szem előtt tartva korlátozható, és az ilyen korlátozások ellen nem illeti meg az érintetteket jogorvoslati lehetőség.⁵⁷⁵

Nemzetközi szerződések vagy az Európai Unió jogi aktusai által létrehozott szervek szintén hozzáférhetnek az eljárás dokumentumaihoz, amennyiben ez az ő feladataik ellátásához szükséges, azonos mértékben és időtartamban, mint a fent említett belföldi szervek.⁵⁷⁶

Ez a megismerési jog nem befolyásolja azokat a különleges szabályokat, amelyek az eljárás során zártan kezelt adatokra, a minősített információk kezelésére vagy az adatok bizalmas kezelésére vonatkoznak.⁵⁷⁷

Az ügyirat zárt kezelésével kapcsolatosan a törvény alapján ezen ügyiratokat a törvény vagy az eljárást vezető bíróság, ügyészség külön rendelkezése nélkül kizárólag csak a bíróság, az

eljáró hatóság, amennyiben a büntetőeljárás során felmerülő feladatainak ellátása szempontjából ez nélkülözhetetlen, bizonyos zártan kezelt személyes adatokat közvetlenül érintett ügyiratokon feltüntessen és a zártan kezelt adatokkal érintett személy hozzájárulása nélkül is továbbíthassa azokat. A büntetőeljárás egyes feladatainak teljesítése után – a vádirat, az eljárást felfüggesztő vagy megszüntető határozat, valamint az ügydöntő határozat kivételével – az ügyiratokat ismét zártan kell kezelni.

⁵⁷⁴ Be. 100 §. (1) – (9)

⁵⁷⁵ Be. 101 §. (1)

⁵⁷⁶ Be. 101 §. (2)

⁵⁷⁷ Be. 101 §. (3)

ügyészség vagy a nyomozó hatóság tekintheti meg. Azt is biztosítaniuk kell, hogy a zártan kezelt ügyirat, illetve annak tartalma az eljárás egyéb ügyirataiból és adataiból ne váljon megismerhetővé.⁵⁷⁸

A minősített adatok felhasználásáról a Be. külön rendelkezik, úgymint a minősített adat felhasználása a bíróság és az ügyészség által, a minősített adat felhasználása a büntetőeljárásban részt vevő személyek által, valamint a minősített adathoz történő hozzáférés biztosításáról szóló szakaszaiban.⁵⁷⁹

A zártan történő kezeléssel kapcsolatban azonban nem csak a sértett, a vagyoni érdekelt, és az egyéb érdekelt adatról van szó, hanem ezek segítőt is megilleti ez a jog, a Be. 99.szakasza (1) bekezdése alapján. A jogi képviselő azonban a felsoroltak között nem szerepel, és nem is indítványozhatja azt saját személyes adatait illetően.

Ezzel kapcsolatban a NAIH beadvánnyal fordult az Igazságügyi Minisztériumhoz, tekintettel arra, hogy a jogi képviselő számára kötelező az elektronikus ügyintézés.⁵⁸⁰

2018 január 1-től a büntetőeljárásokban részt vevő állami szervek, mint a nyomozó hatóságok, az ügyészség, a bíróságok és a büntetésvégrehajtási szervek számára kötelezővé vált az elektronikus kapcsolattartás az ekkor vagy azt követően kezdődő eljárásokban.⁵⁸¹ Róth megjegyzi, hogy a digitalizáció hatása nem korlátozódik csupán az elektronikus kapcsolattartásra és a szélesebb körű E-ügyintézésre, hanem már korábban is jelentős mértékben átszötte a büntetőeljárás több területét, így a bizonyítási folyamatot, a kényszerintézkedések alkalmazását, valamint a különleges, telekommunikációs eszközökkel történő kapcsolattartás formáit. Ez utóbbi a zártcélú távközlő hálózaton keresztül folyó kihallgatásokra is kiterjedt.⁵⁸²

⁵⁷⁸ Be. 102. § (1)-(3)

⁵⁷⁹ Be. 104. § - 106 § Amikor egy ügyirat minősített adatot tartalmaz, annak kézbesítésekor vagy az ügyirat 105. § szerinti megismerésének lehetővé tételénél a bíróság, az ügyészség vagy a nyomozó hatóság ellenőrzi, hogy az érintett megfelel-e a minősített adatok védelmére vonatkozó jogszabályban előírt személyi, fizikai, adminisztratív és elektronikus biztonsági követelményeknek. Amennyiben a minősített adatokat tartalmazó ügyirat kézbesítésekor a hozzáférés csak a minősített adatok kezelésére jogosult bíróságnál, ügyészségnél vagy nyomozó hatóságnál biztosítható a fent említett okok miatt, akkor a címzett számára az ügyiratnak csak a minősített adatot nem tartalmazó részleteit kell kézbesíteni.

⁵⁸⁰ 2015.évi CCXXII. törvény 9.§.(1)

⁵⁸¹ 2015. évi CCXXII. törvény

⁵⁸² Róth, Erika. "A digitalizáció hatása a büntetőeljárásra." p.166

Az e-Papír szolgáltatással kitöltött űrlap és csatolmányai részei a büntetőeljárás valamennyi folyamatának, és az űrlap az okiratok sorsát osztja, attól függetlenül nem kezelhető.⁵⁸³ A Hatóság rámutatott arra, hogy ezen űrlap személyes adatokat tartalmaz – a jogi képviselőre vonatkozóan, melyek az eljárás folyamán a korábban már tárgyalt esetekben, pl. betekintéskor megismerhetők. A Hatóság ezért indítványozza az Infotv.38.szakasza (4) bekezdése alapján, hogy a Be. a zárt adatkezelésre vonatkozó rendelkezéseket illetően módosítsa a szabályozást, hogy a védő ügyvéd az ügygel nem összefüggő személyes adatai az iratbetekintési jog során ne legyen megismerhetőek.⁵⁸⁴ Ezzel kapcsolatban osztom a NAIH álláspontját.

A Be. XVI. fejezete az eljárás ügyiratainak megismerése és zárt kezelésével foglalkozik. Az eljárás ügyirataihoz a terhelt és annak jogi képviselője, a terhelt gyanúsított kihallgatását követően, a bűncselekmény áldozata, az esetet érintő kontextusban, és minden érintett személy, beleértve a vagyoni jogokban érdekelt feleket is, az őket érintő esetekben hozzáférhet. Ez a jog kiterjed az eljárás során keletkezett összes dokumentumra és bizonyítékra, beleértve a bírósági, ügyészi, és nyomozati dokumentumokat, az eljárásban részt vevő személyek által benyújtott vagy csatolt dokumentumokat és egyéb bizonyítékokat.⁵⁸⁵ A megismerés joga nem érvényes a zártan kezelt eljárás dokumentumaira, valamint nem befolyásolja az információk zártan történő kezelésének kötelezettségét.⁵⁸⁶

6. A tárgyalás nyilvánosságának elve és a természetes személyek adatainak védelme

„A nyilvánosság elve – mint a Be.-ben egyedülként nevesített processzuális alapelv – szerint „[a] bíróság tárgyalása nyilvános”. [Be. 436. § (1) bekezdés] A nyilvánosság elve tehát csupán a bírósági eljárásban érvényesülő alapelv, és nem az egész eljárásban (például a nyomozás során sem) érvényesül.”⁵⁸⁷

Nemzetközi jogi keretek között, a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (PPJE) garantálja az egyén jogát arra, hogy bármely ellene felhozott vád vagy jogi vitában érintett jogok és kötelezettségek igazságos és nyilvános tárgyalás keretében kerüljenek elbírálásra egy független és pártatlan bíróság által. Hasonlóan, az Európai Emberi Jogi

⁵⁸³100/2018. (VI. 8.) Korm. rendelet (Nyer) 104.§.(1), II. fejezet 12§, és a 451/2016 8XII.19) Korm. Rendelet I.fejezet 2. pontja alapján a benyújtott és digitálisan aláírt űrlap, okirat. Tartalmazza ki, mikor, milyen módon nyújtotta be azt.

⁵⁸⁴ NAIH/2020/4229/2 ügyirat szám

⁵⁸⁵ Be.610.§ (1)-(4)

⁵⁸⁶ Be. 610.§ (5)

⁵⁸⁷ Fantoly ,Zsanett és Budaházi ,Árpád. „Büntető eljárásjogi ismeretek” p.37.

Egyezmény (EEJE) is alapjogként ismeri el a tárgyalások nyilvánosságát és az ítéletek nyilvános kihirdetését. A PPJE 14. cikkének első bekezdése és az EEJE 6. cikkének első bekezdése részletesen rögzíti, hogy a tárgyalás nyilvánosságát bizonyos esetekben - például erkölcsi okokból, a demokratikus társadalom közrendjének, az állam biztonságának védelme érdekében, vagy amikor a felek magánéletének védelme ezt indokolja - korlátozni lehet, a bíróság által szükségesnek ítélt mértékben. Az egyezmények alapelveként kezelik, hogy a büntetőügyekben hozott ítéleteket nyilvánosan kell kihirdetni, ám a PPJE lehetővé teszi kivételek alkalmazását is, különösen, amikor a fiatakorúak érdekei más igényelnek.⁵⁸⁸

Az Európai Emberi Jogi Bíróság (EJEB) ítélkezési gyakorlatában kiemelkedő jelentőségű a tárgyalások nyilvánosságának elve. A Bíróság a nyilvánosság kérdését a büntetőeljárásokban fontosnak tartja, és ezt számos ítéletében is megerősíti. Az elsőfokú eljárásban az EJEB szerint szinte minden esetben - csak nagyon korlátozott kivételekkel, mint például, ha a jogosult lemond erről a jogáról, vagy ha az adott ügytípusban általánosságban nem tartanak nyilvános tárgyalást - biztosítani kell a nyilvános tárgyalás lehetőségét. Fellebbviteli szinten a Bíróság már rugalmasabban kezeli ezt a követelményt, de itt is csak megfelelően alátámasztott indokokkal lehet korlátozni a nyilvános tárgyaláshoz való jogot. Az ítéletek nyilvános kihirdetése ugyanakkor olyan alapvető fontosságú, mint az elsőfokú nyilvános tárgyalások megtartásának kötelezettsége.⁵⁸⁹

Az igazságos, független és pártatlan eljáráshoz való jog mindenkit megillető, alkotmányos szinten biztosított alapvető jog. Az Alaptörvény a XXVIII. cikkében rögzíti ezt az igazságszolgáltatás működésének alapvető, garanciális jelentőségű elvét. A nyilvánosság kulcsszerepet tölt be az igazságszolgáltatási folyamat átláthatóságának biztosításában, lehetővé téve annak ellenőrizhetőségét és elősegítve egy pártatlan eljárás megvalósulását. Alaptörvény, és a már többször idézett Be. mellett a bíróságok szervezetről és igazgatásáról szóló törvény,⁵⁹⁰

⁵⁸⁸ Márki, Dávid. "Az igazságszolgáltatás nyilvánosságának alkotmányjogi vizsgálata: Alapjogi kollíziók a büntetőeljárás, a sajtó és a politika kereszttüzében." Szeged, Magyarország: Iurisperitus Kiadó, 2023. [Online]. Elérhető: https://publicatio.bibl.u-szeged.hu/27808/1/Marki_2023_07_05.pdf, p. 47.

⁵⁸⁹ Varga Petra, (2018) A nyilvánosság elvének érvényesülése a büntetőeljárásban*Debreceni Jogi Műhely, 2018. évi (XV. évfolyam) 1-2. szám DOI 10.24169/DJM/2018/1-2/9

⁵⁹⁰ 2011. évi CLXI. törvény a bíróságok szervezetről és igazgatásáról

illetőleg a bírósági ügyvitel szabályairól szóló rendelet⁵⁹¹, valamint a sajtóról szóló törvény^{592,593}, is rendelkezik róla.

Cséka a nyilvánosságot általános elvként azonosítja a büntetőeljáráásban, kiemelve annak előnyeit, mint például a társadalmi ellenőrzés jelenlétét, ugyanakkor figyelmeztet a lehetséges hátrányokra is. Ezek közé tartozik többek között az ártatlanul megvádolt személyek vagy a sértettek magánéleti adatainak nyilvánosságra kerülése.⁵⁹⁴

Erdei a nyilvánosságot a közvetlenség és szóbeliség mellett egy alapvető tárgyalási elvként azonosítja, amely a bírói önkény ellen szolgál biztosítékként. Felhívja a figyelmet arra, hogy a modern kor tárgyalásnyilvánossága különösen sebezhetővé válik az elektronikus média jelenléte és a tudósítások kihívásai által.⁵⁹⁵

Navratil az informatikai fejlődés figyelembevételével több dimenzióra bontja a nyilvánosság fogalmát: az intézményi-szervezeti nyilvánosság, az eljárási nyilvánosság, a pillanatnyi és az elektronikus nyilvánosság. Az intézményi-szervezeti nyilvánosság az olyan információkat foglalja magában, mint a bíróságok költségvetése vagy a szervezeti struktúra, míg az eljárási nyilvánosság a tárgyalások nyilvánosságát, a pillanatnyi nyilvánosság pedig az ítéletek kihirdetését jelöli.⁵⁹⁶

Petrik Ferenc szerint a tisztességes eljáráshoz való jog (fair trial) elengedhetetlen részeleme a nyilvánosság, a nyilvános tárgyaláshoz, nyilvános eljáráshoz való jog (public hearing). A public hearing minden ügyben, minden fokon és mindenféle eljárási rendben megvédi a feleket a titkos eljárásoktól.⁵⁹⁷

⁵⁹¹ 14/2002. (VIII.1.) IM rendelet – a bírósági ügyvitel szabályairól

⁵⁹² 2010. évi CIV. tv – a sajtószabadságról és a médiatartalmak alapvető szabályairól: a médiarendszer feladatául határozza meg a helyi, az országos és az európai közélet ügyeiről, valamint Magyarország polgárai és a magyar nemzet tagjai számára jelentőséggel bíró eseményekről a „hiteles, gyors, pontos tájékoztatást.”

⁵⁹³ 2010. évi CLXXXV. törvény a médiaszolgáltatókról és a tömegkommunikációról

⁵⁹⁴ Cséka Ervin, Fantoly Zsanett, Hegedűs István, Kovács Judit, és Maráz Vilmosné. (2007.) *A büntetőeljárási jog alapvonalai. II.* Szeged: Bába Kiadó, pp. 75-77.

⁵⁹⁵ Erdei Árpád. (2011.) *Tanok és tévtanok a büntető eljárásjog tudományában.* Budapest: ELTE Eötvös Kiadó.

⁵⁹⁶ Navratil Szonja. (2011.) "Az igazságszolgáltatás nyilvánossága. Összehasonlító elemzés." In *A bírói függetlenség, a tisztességes eljárás és a politika*, szerkesztette Badó Attila, 156. Budapest: Gondolat Kiadó.

⁵⁹⁷ Petrik Ferenc: Alkotmány a gyakorlatban, kommentár a gyakorlat számára, 2009, HVG-ORAC, Budapest, 444. Idézi: Márki Dávid, „Az igazságszolgáltatás nyilvánossága, különös tekintettel a büntetőeljárás sajtónyilvánosságára” p.151.

Kőhalmi szerint a nyilvánosság elve szorosan összefügg az ártatlanság vélelméhez és a tisztességes eljáráshoz való joggal, ahogy azt a jogot az Emberi Jogok Egyetemes Egyezménye (EJEE) 11.cikke is rögzíti. A nyilvánosság követelménye garanciális jelentőségű alapelv: biztosítja az igazságszolgáltatás működésének átláthatóságát, ellenőrizhetőségét.⁵⁹⁸

Márki véleménye szerint a büntetőeljárás alapvető szabályait, a büntetőeljárás törvény általános és különös rendelkezéseit az eljáró bíróságnak a tárgyalás egészére nézve maradéktalanul be kell tartania. Ilyen alapvető szabály a tárgyalás nyilvánossága, valamint az ítéletek nyilvános kihirdetése is. Az igazságszolgáltatás és sajtó viszonyrendszerében is érvényesülnie kell a fékek és ellensúlyok rendszerének.⁵⁹⁹

Ezeket a nézőpontokat összegezve megállapítható, hogy a nyilvánosság a büntetőeljárás során egy alkotmányos és működési jellegű alapelv, amely nem csak a terhelt és az állam közötti viszonyt határozza meg, hanem a bírói önkény elleni biztosítékot is jelent, elősegítve az igazságszolgáltatás átláthatóságát. A tárgyalás a nyilvánosság kulcsfontosságú eleme, ahol a pillanatnyi és az elektronikus nyilvánosság egyaránt megvalósul.⁶⁰⁰

Németh szerint a társadalmi nyilvánosság és a nyilvánosság tájékoztatáshoz való joga bár összefügg, nem tekinthető azonos fogalomnak.⁶⁰¹ A bírósági tárgyalások nyilvánosságát a Be. rendeli el⁶⁰², hangsúlyozva, hogy ezek a tárgyalások nyitottak mindenki számára, nem csak az ügyben közvetlenül érintett személyek, mint a felek, képviselőik, tanúk, szakértők, hanem bárki részt vehet rajtuk.

A tárgyalás nyilvánosságának kizárása és a nyilvánosság tájékoztatására vonatkozó engedély megtagadásának feltételei nem teljesen azonosak, a Be. 107-109.szakaszai sem fedik le teljesen

⁵⁹⁸ Kőhalmi László.(2022.) "Nyilvánosság és büntetőeljárás." In Az internet és a közösségi média jogi kihívásai, szerkesztette Tóth Dávid. Konferenciakötet. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetésvégrehajtási Jogi Tanszék, Pécs,pp.36- 46

⁵⁹⁹ Márki, Dávid. "Az igazságszolgáltatás nyilvánosságának alkotmányjogi vizsgálata: Alapjogi kollíziók a büntetőeljárás, a sajtó és a politika kereszttüzében." p.146

⁶⁰⁰ Havasiné Kulcsár, Petra.(2017) "A tárgyalás nyilvánossága, a tárgyalás nyilvánosságának korlátozása. A sajtó jelenléte a büntetőeljárásban: avagy a nyilvánosság fogságában." In: *Büntetőjogi tanulmányok*, 18. köt. Budapest, Magyarország: Matarka Kiadó

⁶⁰¹ Németh, Kata, A büntetőeljárás nyilvánosságának jogszabályi háttérében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." p.58

⁶⁰² 436. § (1) A bíróság tárgyalása nyilvános.

egymást. Ez a megkülönböztetés két fontos dimenzió – a társadalmi nyilvánosság és a tárgyalótermi nyilvánosság – közötti határvonalat jelöli ki.⁶⁰³

A Büntetőeljárás törvény (Be.) részletesen meghatározza, hogy a büntetőeljárás különböző szakaszaiban mely hatóságok felelősek a nyilvánosság tájékoztatásáért. A nyomozás lezárásáig a nyomozó hatóság erre kijelölt tagja⁶⁰⁴ és az ügyészség, míg a bírósági eljárás alatt – beleértve a vádemelés előtti szakaszt is – a bírák jogállásáról és javadalmazásáról szóló törvény által erre felhatalmazott személyek és az ügyészség adhatnak tájékoztatást.⁶⁰⁵ Az egyes hatóságok belső szabályzatai döntenek el, hogy ki jogosult az adott információ szolgáltatási feladatok ellátására.⁶⁰⁶ Az eljáró hatóságtól nyilvánosság tájékoztatása céljából információt kérő személyeknek, beleértve a kép-, hang- vagy kép- és hangfelvételek készítésére vonatkozó engedély kérelmezőit is, meg kell adniuk nevüket (vagy megnevezésüket, ha nem természetes személyről van szó), elérhetőségeiket, valamint azt, hogy milyen módon – különösen mely médiatartalom-szolgáltató vagy más információs szolgáltatás segítségével⁶⁰⁷ – kívánják a nyilvánosságot tájékoztatni. A törvény mindenki számára lehetővé teszi, hogy bírósági tárgyalásokról a médiarendszeren keresztül tájékoztatást kapjon. Kép-, hang-, vagy kép- és hangfelvételek készítése a bíró vagy a tanács elnökének engedélyével lehetséges, és a tárgyaláson jelen lévő személyekről (a bíróság tagjai, jegyzőkönyvvezető, ügyész és védő kivételével) csak az

⁶⁰³ Németh, Kata, A büntetőeljárás nyilvánosságának jogszabályi háttérében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre.”p.59

⁶⁰⁴ A Rendőrségre irányadó tájékoztatási kötelezettséget a büntetőeljárás nyomozási szakaszában a sajtó felé történő tájékoztatás keretében a 30/2011. (IX. 22.) BM rendelet rögzíti. Ezen dokumentumok meghatározzák, hogy a rendőrség milyen módon köteles információkat nyújtani a médiának a nyomozási folyamatokkal kapcsolatban.

⁶⁰⁵ 2011. évi CLXII. törvény a bírák jogállásáról és javadalmazásáról 22. 43.§-44.§

⁶⁰⁶ Be. 107. § (2)

⁶⁰⁷ A 2010. évi CIV. törvény, mely a sajtószabadságról és a médiatartalmak alapvető szabályairól rendelkezik, a médiarendszer egyik lényeges feladatává teszi a helyi, nemzeti és európai közélet, valamint a magyar állampolgárok és a nemzeti közösség tagjai számára fontos események megbízható, időszerű és precíz tájékoztatását. A sajtószabadságról és a médiatartalmak alapvető szabályairól, valamint a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény. törvény hatálya alá alapvetően két szolgáltatási kör tartozik. Az országban letelepedett médiatartalom-szolgáltató által nyújtott médiaszolgáltatás, valamint a médiatartalom-szolgáltató, által kiadott sajtótermék, melyeket gyűjtőnéven médiatartalom-szolgáltatásnak nevezünk. A média működését, jogkörét és felelősségeit nem csak az Alaptörvény és a sajtótörvény, de az eljárási jogszabályok és számos egyéb rendelet is szabályozza.

érintettek hozzájárulásával készülhetnek. A hallgatóság létszámának korlátozása semmilyen formában nem korlátozhatja a nyilvánosság tájékoztatáshoz való jogát.⁶⁰⁸

Az eljáró hatóság az információ szolgáltatást, illetve a kép-, hang-, vagy kép- és hangfelvételek készítéséhez szükséges engedélyt megtagadhatja, ha ezek következményeként a büntetőeljárásban részt vevő személyek, - vagy különös bánásmódra szorulók esetén - élete, testi épsége, egészsége vagy magánélethez való joga közvetlen veszélynek lenne kitéve.⁶⁰⁹ Ha a személyes adatok védelme elengedhetetlenül szükséges a minősített adatok, valamint zárt tárgyalás esetében a nyilvánosság kizárását indokló érdekek védelmében, és ha a tájékoztatás megadása veszélyeztetné a büntetőeljárás vagy az egyes eljárási cselekmények eredményességét, illetve azok folyamatosságát vagy zavartalanságát megtagadható az engedély.⁶¹⁰

Az ügyiratok megismerésére és a nyilvánosság tájékoztatására vonatkozó rendelkezésekben meghatározott személyeken kívül az eljárásról tájékoztatás annak adható, akinek jogi érdeke fűződik az eljáráshoz. A vádemelés előtt az ügyészség vezetője, a vádemelést követően pedig az eljáró bíróság elnöke – a jogi érdek fennállásának igazolása esetén – engedélyezheti az ügyiratok megismerését vagy a kért információk megadását.⁶¹¹

Háger szerint a tárgyalás nyilvánosságának korlátozására vonatkozó okok két fő kategóriába sorolhatók: az egyik a rendfenntartás és a bizonyítási folyamat zavartalan lefolytatásának szükségessége, a a hallgatóság életkorával kapcsolatos szabályozás, a másik erkölcsi okból, titokvédelmi-vagy tanúvédelmi érdek miatt kerül a nyilvánosság korlátozásra.⁶¹² Az 14 év alattiak nem lehetnek jelen a hallgatóságban, míg a 14 és 18 év közöttiek esetében a bíró dönthet jelenlétükről, figyelembe véve az ügy sajátosságait és az érintettek közötti viszonyokat.

⁶⁰⁸ Be. 108. § (1) – (3)

⁶⁰⁹ „A különös bánásmód körébe tartozik különösen (85. §) a jogok gyakorlásának és a kötelezettségek teljesítésének az elősegítése (akár segítővel); fokozott körültekintés az adott személynél (kapcsolattartás, magánélet kímélete, más résztvevőkkel való találkozás elkerülése, akár külön helyiségben, telekommunikációs eszköz igénybevétele, nyilvánosság kizárása stb.); fokozott adatvédelem; haladéktalan, megismétlést nem igénylő eljárás (ennek érdekében akár kép- és hangfelvétel készítése); védelemben részesítés.” Herke Csongor, Büntető eljárásjog Egyetemi jegyzet Pécsi Tudományegyetem Állam- és Jogtudományi Kar Pécs, 2018, 23.o

⁶¹⁰ Be. 109. § (1)

⁶¹¹ Be. 110. § (1) – (2)

⁶¹² Háger Tamás. "A nyilvánosság mint a tisztességes eljárás egyik garanciája a büntetőperben." In: Pro Futuro 2014/1, p. 52

A nyilvánosság kizárása vagy a zárt tárgyalás elrendelése csak törvényben meghatározott esetekben lehetséges, például a különleges védelemre szoruló személyek védelme vagy a védett adatok érdekében.⁶¹³ A védett adatok körébe tartozik a törvény által védett és a hivatás gyakorlásához kötött titkok. Különös jelentőséggel bírnak ezek az esetek a gazdasági bűncselekmények kapcsán, ahol az üzleti vagy banktitok nyilvánosságra kerülése súlyos sérelmeket okozhat.

„A nyilvánosság alapelvét két módon lehet megsérteni, törvényes ok fennforgása ellenére nem zárják ki a nyilvánosságot a tárgyalásról (ennek fegyelmi, esetleg titoksértés esetén akár büntetőjogi következményei lehetnek); vagy törvényes ok hiányában zárja ki a nyilvánosságot a bíróság a tárgyalásról (ez relatív hatályon kívül helyezési okot képező eljárási szabálysértés, ld. 609. §).”⁶¹⁴

Németh a tárgyalótermi nyilvánosság kapcsán a médiarendszer nyilvánosságát illetően felveti a tárgyalással egy időben, az élő-közvetítés (online-streaming) problematikáját, amelyet a Be. szerint csupán mint a „mediarendszer” részét értelmezhetjük, mert külön szabályozás nem vonatkozik rá.⁶¹⁵ Felveti a kérdést, hogyan valósítható meg az érintett Be. szerinti hozzájárulása egy a tárgyalással azonos időben megjelenő, élő tudósítás kapcsán, miként biztosítható azon személyek arcképének torzítása, akik nem járultak hozzá a róluk készült felvétel készítéséhez. A nyilvános tárgyalás során tehát a hallgatók és a média képviselői hozzájuthatnak az eljárás résztvevőinek, így a terhelt, sértett vagy tanúk személyes és különleges adataihoz is.

Ez az érintettek szempontjából adatvédelmi aggályokat vet fel. Azonban a bíróságnak mérlegelési lehetősége van abban a tekintetben, hogy az érintettek jogos magánérdekét milyen mértékben befolyásolja a tárgyalás nyilvánossága. Ezt is figyelembe véve szükséges megfontolnia a hallgatóság létszámának korlátozását, a zárt tárgyalás elrendelését, amelyet erkölcsi okokból, a különleges bánásmódot igénylő személyek védelmében, valamint minősített

⁶¹³ A bíróság tárgyalása nyilvános (436. §), kivéve, ha a tanácselnök meghatározza a tárgyalás létszámát vagy a bíróság a nyilvánosságot kizárja: A nyilvánosság részleges kizárása a tárgyalásról (a tanács elnöke rendelheti el), vagy Zárt tárgyalás (a bíróság rendelheti el) Ez utóbbi esetekben erkölcsi okból, különleges bánásmódot igénylő személy védelme érdekében, minősített adat és egyéb adat védelme érdekében, a fiatakorú érdekében (még a terhelt is kizárható). Lásd: Herke, Csongor „*Büntető eljárás*”, p.100.

⁶¹⁴ Ibid., 101.o

⁶¹⁵ Németh, Kata, A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre.” pp. 60-62

és egyéb védett adatok védelmében lehet alkalmazni.⁶¹⁶ Ahogy már szó volt róla zárt tárgyalást csak indokolt és nyilvánosan kihirdetett végzéssel lehet elrendelni. A „erkölcsi okok” kategóriája gyakorlatilag magában foglalhatja azokat az eseteket is, amikor a nyilvánosság kizárását a terhelt jogainak, jogos érdekeinek, emberi méltóságának, jóhírének és személyes adatoknak a védelme teszi szükségessé. Ez utóbbi véleményt képviseli Németh és Mándi is.

A Be. 436. szakasza (4) bekezdése kimondja, hogy *„A bíróság hivatalból vagy az ügyészség, a vádlott, a védő, a sértett, illetve a vagyoni érdekelt és az egyéb érdekelt indítványára a nyilvánosságot az egész tárgyalásról vagy annak egy részéről indokolt határozattal kizárhatja és a) erkölcsi okból, (...) zárt tárgyalást rendelhet el.”*

A bíróság – ahogy a büntetőeljárás más hatóságai is - az igazságszolgáltatási tevékenységük kapcsán is adatkezelőknek minősülnek.⁶¹⁷ ⁶¹⁸ Ennek megfelelően az Infotv. alapelvei alapján a legmagasabb szintű védelmet kell biztosítaniuk a személyes adatok védelmének az igazságszolgáltatási eljárás során, azzal összhangban, hogy egyúttal megfeleljenek az uniós jognak, az Alaptörvényben, Büntetőeljárás törvényben, a bíróságok szervezetéről és igazgatásáról szóló törvényben, és a korábban már felsorolt egyéb vonatkozó ágazati jogszabályoknak.

Adatvédelmi aggályok a tárgyalási jegyzék kifüggesztése, a tárgyalás nyilvánossága vagy zárt tárgyalás elrendelése, valamint az ítélethirdetés nyilvánossága, és a bírósági tárgyalásokról szóló tudósítás kapcsán merültek fel.

⁶¹⁶ Ibid., Az ügyfélnyilvánosságról akkor beszélünk, amikor a bíróság zárt tárgyalást rendel el, ekkor a tárgyaló tanács tagjai és a jegyzőkönyvvezető mellett csak a vádló, a védő és a vádlott jogosult részt venni a tárgyaláson. A bíróság ezen felül lehetőséget biztosíthat az igazságszolgáltatási feladatokat végző hivatalos személyek, például a bíróság elnöke vagy, amennyiben a vádlott fogvatartásban van, a büntetésvégrehajtási intézet őre számára, hogy részt vehessenek a tárgyaláson. Ez a jog kiterjedhet azon esetekre is, ha a vádlott külföldi állampolgár, vagy amennyiben a bűncselekmény külföldi állampolgár ellen történt, annak konzuli képviselője is jelen lehet a tárgyaláson. A zárt tárgyalásról való tudósítás, akár elektronikus, akár egyéb módon, valamint a média képviselőinek a tárgyaláson való jelenléte nem lehetséges.

Az ítélet rendelkező részének kihirdetése ebben az esetben is kötelező.

A Be. 436. (4) alapján „Ha a bíróság zárt tárgyalást rendel el, figyelmezteti a jelenlévőket arra, hogy a tárgyaláson elhangzottról tájékoztatást nem adhatnak.(...)”

⁶¹⁷ Infotv. 25.L.§. a) Annak ellenére, hogy állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot látnak el ebben a minőségükben, nem kötelezettek adatvédelmi tisztviselő kijelölésére.

⁶¹⁸ Infotv. 38.§ (1) A Hatóságnak a személyes adatok tekintetében meghatározott feladatköre a bírósági döntés meghozatalára irányuló peres és nemperes eljárásokban, az azokra vonatkozó előírások alapján a bíróság által végzett adatkezelési műveletek vonatkozásában nem terjed ki meghatározott hatáskörök gyakorlására.

Az aggályokra adott válaszokat a bünygyi adatkezelést szabályozó keretrendszer, azaz a bünygyi irányelv nyomán, az Infotv. által előírt rendelkezések tartalmazzák.

Egyrészt az adatkezelésnek meg kell felelnie a jogszerűség, a törvényesség⁶¹⁹ és a célhoz kötöttség alapelveinek.⁶²⁰ Ez utóbbi, melyet a Be. is megfogalmaz, kimondja, hogy személyes adatok kezelése kizárólag abban az esetben történhet, ha az adott cél megvalósításához szükséges, és a cél elérését lehetővé teszi. Az adatkezelés mértéke és időtartama korlátozódik arra az időszakra, amely a megfogalmazott cél eléréséhez elengedhetetlen. A Be. megfogalmazása szerint, ha jogszabály másképp nem rendelkezik, a büntetőeljárásban érintett személyek személyes és védett adatokat kizárólag a törvényben meghatározott jogok gyakorlása, illetve kötelezettségek teljesítése céljából, és csak a szükséges mértékben és ideig kezelhetik.⁶²¹

Másrészt a bünygyi adatkezelés folyamatában az érintettek kategóriájának elkülönítése kiemelt jelentőséggel bír. Az adatkezelés során figyelembe kell venni az érintettek kategóriáit, mivel ez meghatározza az alkalmazandó adatvédelmi szabályozásból adódó jogokat és korlátokat. Az Infotv. rendelkezései alapján a bíróság az adatkezelő szerepét tölti be a vádeljárás során, az érintetti jogok és korlátozások tekintetében rendelkezhet.^{622,623}

Álláspontom szerint a bíróság mérlegelési jogkörét figyelembe véve, amennyiben az eljáró bíró úgy ítéli meg, hogy valamely - az eljárásban felsorolt egyéni kategóriák szerinti megkülönböztetés alapján - személyes adat védelméhez az elengedhetetlenül szükséges a Be. szerinti „erkölcsi okból”, elrendelheti a zárt tárgyalást, egyetértve Németh és Mándi felvetésével. De lege ferenda javaslatom azonban a Be. taxatív felsorolásainak ilyen irányú módosítása. [Be. 436.§. (4) c)] A 436. szakasz (4) bekezdése c) pontjának „*minősített adat és egyéb védett adat védelme érdekében*” kiegészítését javasolnám az alábbiak szerint: - „

⁶¹⁹ Infotv. 4.§. (1) Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

⁶²⁰ Infotv.5.§. (2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

⁶²¹ Be. 98.§ (3) Ha az érintett adatkörre vonatkozó jogszabály másképp nem rendelkezik, a büntetőeljárásban részt vevő személyek az e törvény rendelkezései alapján megismert személyes adatot és védett adatot e törvény szerinti jogaik gyakorlásához vagy kötelezettségeik teljesítéséhez szükséges mértékben és ideig kezelhetik.

⁶²² Infotv. 7.§ (1) a) – d)

⁶²³ Infotv. 7.§ (4)

minősített adat és egyéb védett adat védelme érdekében, valamint olyan személyes adat esetében melynek védelméhez az elengedhetetlenül szükséges, különös tekintettel az érintettek kategóriái közötti különbségtételre.”

Felmerül a kérdés az „*az elengedhetetlenül szükséges*” kategória értelmezését illetően. Azonban Be. használja ezt a kifejezést, a személyes adatok zárt kezelése esetében a személyes adatot a Be. 99. szakasza (5) b) pontjában, az áldozat segítés és pártfogói felügyelet ellátásához elengedhetetlenül szükséges mértékben lehet továbbítani. Használja továbbá a minősített adat felhasználása esetén, a Be.104.§.(2) bekezdés alapján, a bíró és az ügyész által elengedhetetlenül szükséges mértékben kezelhet minősített adatot. A különleges bánásmódot igénylő személy személyes adatainak védelméhez, ha az elengedhetetlenül szükséges a Be. 109.szakasza (1) bekezdése b), c), d) pontjai szerint , valamint a leplezett eszközök megszerzése esetén a 214.szakasz (5) bekezdés a) pontja szerint ha az a személyes adat vagy az információ megszerzéshez elengedhetetlenül szükséges. Az adatkérési szolgáltatással kapcsolatban a 264.szakasz (4) bekezdése szerint „*csak annyi és olyan személyes adat szolgáltatása kérhető, amely az adatkérés céljának megvalósításához elengedhetetlenül szükséges.*”

A tárgyalási jegyzék nyilvánosságával kapcsolatban egyetértek a korábban már említett álláspontokkal, amennyiben az eljárás ügyszámának önmagában történő kifüggesztése biztosíthatja az érintettek személyes adatainak védelmét. Az ügyszám csak akkor válik személyes adattá, ha az a természetes személlyel kapcsolatba hozható, és megismerhető, egyébként közérdekű adatnak minősül, ahogy ezt a NAIH is rögzíti állásfoglalásában.⁶²⁴ Az állásfoglalás hivatkozik BDT2019. 4060. számon közzétett bírósági határozatra⁶²⁵, amely szerint a bírósági eljárás során nyilvánosságra hozott személyes adatok nem nyilvános adatokként kezelendők, és a tárgyalás nyilvánossága nem terjed ki a periratokra. Azaz a periratok, így a tárgyalási jegyzőkönyvek is, a benne szereplő személyes adatok védelme

⁶²⁴ NAIH/2020/294/4 ügyszámú állásfoglalása.

⁶²⁵ Megjelent: Bírósági Döntések Tára 2019/9/100, Szegedi Ítéletábla Pf. 20.307/2018/4. Polgári ügyben hozott határozata alapján, Idézi NAIH/2020/294/4

Tehát a” bíróság határozata értelmében, I. A bírósági eljárás során nyilvánosságra került személyes és különleges adatok nem osztják a közérdekből nyilvános vagy közérdekű adatok jogi sorsát. II. A peres eljárás tárgyalásának nyilvánossága nem azonos a periratok nyilvánosságával. A tárgyaláson az érdeklődők megjelenhetnek és a szóbeli eljárást figyelemmel kísérhetik, e jog azonban nem foglalja magában az iratok nyilvánosságát. A peres eljárás iratai - ide értve a tárgyalási jegyzőkönyveket is - nem hozhatók nyilvánosságra a bennük foglalt személyes adatok miatt általában akkor sem, ha egyébként az az eljárási cselekmény, amelyről készültek, nyilvánosan zajlott.”

érdekében nem tekinthetők nyilvánosan hozzáférhetőnek, még nyilvános tárgyalás esetében sem.

A tárgyalás nyilvánossága mellett a zártan történő eljárás esetében az ítélet nyilvános kihirdetésének problémája merült fel még adatvédelmi szempontból. Ezzel és az ehhez kapcsolódó sajtónyilvánosságával kapcsolatban a NAIH állásfoglalása⁶²⁶ irányadó. A bírósági eljárások során kialakított ítéletek nyilvános kihirdetése egyrészt a társadalmi normák érvényesítését szolgálja az elkövetőkkel szemben, másrészt pedig preventív célt is hordoz, mivel célja a hasonló jogsértések megelőzése. A büntetőeljárás nem csupán a megtorlást célozza, hanem arra is törekszik, hogy elrettentse a terhelteket a további bűncselekmények elkövetésétől. Ezáltal alapvető fontosságú, hogy a büntetőjogi rendszer lehetőséget biztosítson az elítéltek számára, hogy a büntetésük letöltése után sikeresen reintegrálódjanak a társadalomba, a büntetett előéletből adódó hátrányok nélkül. Ennek érdekében lényeges, hogy a bírósági tárgyalások nyilvánossága és különösen az ítéletek kihirdetése során csak a cél eléréséhez szigorúan szükséges személyes adatok kerüljenek feldolgozásra. Ezzel összefüggésben az online térben közzétett bírósági tárgyalásokról szóló tudósítások esetében megjelenő személyes adatok, mint az elítéltek neve, a bűncselekmények és a kiszabott büntetések, hosszú távon is hozzáférhetővé válnak, ami figyelmen kívül hagyja az elítéltek jogát a büntetett előlethez fűződő hátrányok idővel történő eltörlésére. Ez a gyakorlat jelentős hatással van az érintettek magánéletére és társadalmi reintegrációjukra. Ezért felmerül a kérdés, hogy a nyilvános bírósági tárgyalásokról szóló tudósítások milyen mélységben és mely személyes adatokat tartalmazhatnak jogosan. Ennek érdekében az Infotv. alapján, a személyes adatok kezelése során - ahogy a tárgyalás nyilvánosságával kapcsolatosan is, az ítélethirdetés kapcsán is, csak a célnak megfelelő - jelen esetben a bírósági tárgyalásról történő tájékoztatás megvalósulásához elengedhetetlenül szükséges személyes adat kezelhető, a cél megvalósulásáig szükséges mértékben és ideig.

A bírósági tárgyalásokról szóló tudósítás során kiemelt figyelmet kell fordítani a büntetőeljárás célkitűzéseire, az érintettek személyes és különleges adatok iránti védelmére, valamint az információhoz való jog és az arra való kötelezettség egyensúlyára. Ezáltal egy kényes egyensúlyt kell megvalósítani a közvélemény tájékoztatásának jogos igénye és az egyének magánszférája, személyes adatokhoz való jogának védelme között. A 2010. évi CIV. törvény,

⁶²⁶ NAIH-4418-5/2012/V, Állásfoglalás a bírósági tárgyalásokról készített MTI tudósítások során nyilvánosságra hozott személyes adatokról. Bár az állásfoglalás még az Infotv. és a Be. korábbi változatit Idézi, az elvi szempontok helytállóak.

amely a sajtószabadságról és a médiatartalmak alapvető szabályairól szól, hangsúlyozza, hogy a sajtószabadság gyakorlása nem eredményezhet bűncselekmény elkövetését vagy annak felhívását, nem sérti a közízlést, továbbá nem sértheti harmadik fél személyhez fűződő jogait. A törvény 14. § (1) bekezdése előírja, hogy a médiatartalom-szolgáltatónak meg kell őriznie az emberi méltóságot a közvetített tartalmakban. E rendelkezések, hasonlóan a büntetőeljárás szabályozásához, általános keretet biztosítanak, melyek egyensúlyt teremtenek a sajtószabadság gyakorlásának korlátai és az egyéni jogok tiszteletben tartása között.

A jogszabályi előírások alapján adatvédelmi szempontokból csak kivételes esetekben indokolt, hogy a bírósági tárgyalásokról szóló sajtóbeszámolók személyes adatokat tartalmazzanak. Ilyen különleges helyzetek lehetnek például az erőszakos bűncselekmények, amelyek különösen nagy közérdeklődést váltanak ki, és amelyekben a büntetések, vagy a büntetőjogi következmények hosszabb időre vonatkoznak. Fontos figyelembe venni azokat az eseteket is, ahol az információközlés hozzájárulhat a jövőbeli bűncselekmények megelőzéséhez, különösen, ha az érintett nem közszereplő vagy nem lát el közfeladatot. A sajtótermék kiadójának vagy szerkesztőségének ezeket a tényezőket mérlegelnie kell, eldöntve, hogy a publikáció céljai szempontjából valóban szükséges-e a személyes adatok közzététele. Meg kell vizsgálni, hogy a célt anonimizált adatok, vagy csak a kezdőbetűk használatával is el lehet-e érni, miközben a személyiségvédelem maximálisan biztosított marad, összhangban a sajtószabadságról és médiatartalmak alapvető szabályairól szóló törvény általános elveivel.⁶²⁷ Képi-és hangszközök használata esetére is vonatkoztatható ez megállapítás.

A sajtónyilvánosság kapcsán a digitális kor veszélyeire figyelmeztet Kőhalmi. „A „Medienjustiz” jelentősége kiszámíthatatlan folyamatokat indíthat el és kétségeket ébreszthet, hogy tud-e, képes-e a büntető igazságszolgáltatás a tömegtájékoztatásban megjelenő hírekkel nem foglalkozva pártatlan és igazságos döntést hozni.” A közösségi platformok jogi szempontból szabályozatlan területek, ami rendkívül megnehezíti mind a normatív előírások, mind az erkölcsi elvárások hatékony betartását.⁶²⁸

⁶²⁷ A NAIH állásfoglalás rögzíti azt a tényt is, hogy a” A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (Smtv.) 4. § (3) bekezdése alapján a sajtószabadság gyakorlása nem valósíthat meg bűncselekményt vagy bűncselekmény elkövetésére való felhívást, nem sértheti a közérkölcset, valamint nem járhat mások személyhez fűződő jogainak sérelmével. Az Smtv. 14. § (1) bekezdése előírja, hogy a médiaszolgáltatónak az általa közzétett médiatartalomban tiszteletben kell tartania az emberi méltóságot.”

⁶²⁸ Kőhalmi László. "Nyilvánosság és büntetőeljárás." Pécs, 2022.p.41

7. A bírósági adatkezelési műveletek ellenőrzése

Az Infotv. a VI/A fejezetben szabályozza a bírósági adatkezelések ellenőrzését. Jelen esetben a bűnügyi célú adatkezelésre vonatkozó rendelkezések kerülnek ismertetésre.

A bírósági döntést szolgáló peres és nemperes eljárások (továbbiakban: alapügy) keretében, az ezekre alkalmazandó szabályok szerint végrehajtott adatkezelési tevékenységek esetében a személyes adatok védelmére vonatkozó jogok gyakorlását és azok megsértése esetén a személyes adatok védelméhez való jog érvényesülésének ellenőrzésére adatvédelmi kifogást lehet benyújtani. A kifogások értékelése az alapügyben alkalmazandó eljárási normák figyelembe vételével történik. Amennyiben az alapügyet a büntetőeljárás vagy szabálysértési jogszabályok alapján kell lefolytatni, úgy a Be. 143. szakasza (3) bekezdése, valamint a 144. szakasz (3) és (8) bekezdésének a) pontja szerint kell eljárni.⁶²⁹ A kifogást az alapügyben eljáró bíróságnál írásban lehet előterjeszteni.⁶³⁰ A kifogást benyújthatja a peres fél, a vádlott, valamint az eljárás további szereplői – többek között a sértett, a magánvádló, a tanú és a szakértő –, illetve bárki, aki jogi érdekének védelmét a kifogás előterjesztésével párhuzamosan igazolni tudja.⁶³¹ A személyes adatok bírósági kezelésével kapcsolatos kifogásokat a bíróság az alapügy releváns eljárási szabályai szerint bírálja el, különös tekintettel arra, hogy az adatkezelés megfelelt-e a jogszabályi és uniós előírásoknak. Kifogást az érintett akkor terjeszthet elő, ha személyes adatainak kezelése során jogsértés történt vagy annak közvetlen veszélye áll fenn, illetve ha érintetti jogainak érvényesítésekor az adatkezelő jogszerűtlenül járt el. A kifogás elbírálása során a bíróság, amennyiben a kifogást alaposnak ítéli, megteszi a szükséges intézkedéseket a jogsérelem enyhítése vagy a jogsértés veszélyének megszüntetése érdekében, és erről tájékoztatja a kifogást előterjesztőt. Amennyiben az intézkedések ellenére az érintett továbbra is fenntartja kifogását, írásban nyilatkozhat erről az alapügyben eljáró bíróságnak. Ha az alapügyben eljáró bíróság nem intézkedett, vagy az érintett nyilatkozatot terjeszt elő, az alapügyi bíróság a kifogás elbírálására illetékes bírósághoz terjeszti a szükséges iratokat. A peres vagy nemperes eljárás lezárása után is érdemben kell elbírálni a kifogást.⁶³²

A kifogások elbírálása kapcsán a bíróság indokolt határozatot hoz, amely során vagy visszautasítja a kifogást, ha nem történt jogsértés, vagy elutasítja azt, ha a visszautasítási ok

⁶²⁹ Infotv.71./A.§ (1) (2)

⁶³⁰ Infotv. 71./A.§ (3)

⁶³¹ Infotv. 71./A.§ (4)

⁶³² Infotv.71./B.§ (1) - (6)

csak az érdemi vizsgálat megkezdését követően jutott a tudomására. Ha a kifogás jogos, a bíróság a következő intézkedéseket teheti: jogellenes adatkezelés megállapítása, a jogellenes művelet megszüntetésének vagy a jogsértés veszélyének elhárításának elrendelése, vagy az adatkezelés jogszerűségének helyreállítása, továbbá az érintetti jogok érvényesülését szolgáló intézkedések meghozatala az Infotv. alapján. Az eljárás során a bíróság a személyes adatok védelmére vonatkozó jogszabályok alkalmazásának egységessége érdekében kérheti az adatvédelmi hatóság véleményét.⁶³³ A bíróság kérelemre elrendelheti ítéletének – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt az adatvédelem, illetve az információszabadság érdekeinek és nagyobb számú érintett e törvényben védett jogainak védelme megköveteli.⁶³⁴

Összefoglalva a büntetőeljárások során az adatvédelem kiemelt jelentőségű az érintettek személyes adatainak kezelése szempontjából. A büntetőeljárásról szóló 2017. évi XC. törvény és az információs önrendelkezési jogról és az információszabadságról szóló törvény előírásai szerint a személyes adatok kezelése csak a büntetőeljárás céljainak megfelelően, az adattakarékosság elvét betartva lehetséges. A büntetőeljárás egyes fázisainak törvényi szabályozása megfelel az Infotv. által előírt szabályoknak, amely a keretrendszert adja ezen jogszabályok részére. Szabályozási szinten ez érvényesül, ennek ellenére felmerülnek adatvédelmi szempontból aggályos kérdések.

A büntetőeljárás alapvető szakaszai – a nyomozás és a bírósági eljárás – különböző adatvédelmi követelményeket támasztanak. A nyomozás során alapvetően a titkosság elve érvényesül, míg a bírósági eljárás szakaszában a nyilvánosság elvének figyelembevételével kell eljárni, ugyanakkor bizonyos esetekben itt is előfordulhatnak korlátozások, például a személyes adatok, különösen a különleges személyes adatok védelme érdekében. Az érintettek, úgy mint a sértettek, tanúk, vagy a vádlottak, személyes adatainak védelmében a nyomozó hatóság, az ügyészség, és a bíróság meghozhatja a szükséges intézkedéseket, így például a zárt tárgyalás elrendelését vagy a személyes adatok védelmét igénylő eljárások alkalmazását. A zárt adatkezelési eljárások során a személyes adatokat különös gondossággal kezelik, és csak az érintett beleegyezésével hozhatók nyilvánosságra vagy szüntethető meg a zárt kezelésük.

A bírósági döntések nyilvános meghozatala és kihirdetése biztosítja a társadalmi ellenőrzést és az igazságszolgáltatási folyamat átláthatóságát, miközben a személyes adatok védelme érdekében szükség esetén korlátozások is alkalmazhatók. Az adatvédelmi elveknek

⁶³³ Infotv.71./C.§ (1) - (3)

⁶³⁴ Infotv. 64. § (5)

megfelelően csak az eljárás céljának megvalósulásához szükséges személyes adatok kezelhetők, és ezek adatai a cél megvalósulásáig, szükséges mértékben és ideig kezelhetők.

A nyilvánosság tájékoztatása során az adatvédelmi szabályok betartása mellett kell egyensúlyt teremteni a közvélemény tájékoztatáshoz fűződő jog és az érintettek személyes adatainak védelme között. Az adatkezelési tevékenységekkel kapcsolatos kifogásokat az alapügyre vonatkozó eljárási szabályokkal összhangban, az Be. meghatározott⁶³⁵ rendelkezései alapján lehet előterjeszteni. A személyes adatok kezelésével kapcsolatos kifogások esetén az érintettek érvényesíthetik jogait, és panaszt tehetnek, amelyeket a bíróságoknak szabályozott eljárás keretében kell kivizsgálniuk és intézkedniük kell a jogsértések orvoslása érdekében.

8. A büntetésvégrehajtás adatvédelmi vonatkozásai

8.1 Általános megfontolások

A büntetés-végrehajtási szervezet, amely a Belügyminisztérium irányítása alá tartozik, az állam fegyveres rendvédelmi szerveinek egyike. Feladata a törvény által előírt, szabadságelvonással járó büntetések, intézkedések és büntetőeljárás kényszerintézkedések, valamint a szabálysértések miatt kiszabott pénzbírságok elzárásra való átváltoztatása során megállapított elzárások végrehajtása. Ezen felül, a törvényben meghatározott esetekben, az idegenrendészeti őrizetet is ellátja. Ez a szervezet tehát az állami fegyveres rendvédelmi szervek összességének részét képezi, különös tekintettel a jogszabályokban meghatározott feladataira. A büntetésvégrehajtási rendszer magában foglalja a Büntetés-végrehajtás Országos Parancsnokságát (a továbbiakban: BVOP), a büntetés-végrehajtási intézményeket, a büntetés-végrehajtási intézeteket, és a gazdasági társaságokat.⁶³⁶

A BVOP a büntetés-végrehajtási rendszer központi koordinációs és irányítási szerve, melynek az a szerepe, hogy felügyeleti, auditálási és szakmai útmutatást nyújtson a büntetés-végrehajtási intézmények, az azokhoz kapcsolódó gazdasági egységek, valamint az egyéb, büntetés-végrehajtás alá tartozó szervezetek számára. Ennek keretében a BVOP feladatai közé tartozik a fogvatartás körülményeinek biztonságának biztosítása, a fogvatartottak társadalmi reintegrációjának elősegítése, munkaerő-piaci reintegrációjuk, egészségügyi ellátásuk,

⁶³⁵ 2017. évi XC. törvény 143. § (3) bekezdését, valamint 144. § (3) bekezdését és (8) bekezdés *a*) pontja alapján.

⁶³⁶ Kondás Katalin. (2018.) "Adatok védelme a börtönökben." *Hadmérnök* XIII. évfolyam, 1. szám (március): 270.

logisztikai menedzselésük, valamint az adatkezelésük⁶³⁷ szabályozása és felügyelete. Emellett koordinálja a büntetés-végrehajtási pártfogói felügyeletet végző tevékenységeket.

A büntetés-végrehajtási intézmények funkcionalitásuk szerint elsősorban a fogvatartottak társadalmi reintegrációját, egészségügyi rehabilitációját és a kényszergyógykezelések alkalmazását szolgáló infrastruktúrákat foglalnak magukban. E struktúrák közé tartoznak a személyzet szakmai fejlődését elősegítő oktatási programok, valamint a fogvatartottak egészségügyi ellátására specializálódott létesítmények.

A büntetés-végrehajtási intézetek, mint az elhelyezésre szolgáló objektumok, infrastrukturális és logisztikai keretet biztosítanak a fogvatartottak számára, míg a hozzájuk kapcsolódó gazdasági társaságok a fogvatartottak munkaerő-piaci reintegrációját támogatják azáltal, hogy értékteremtő és társadalmilag hasznos munkalehetőségeket kínálnak számukra. A büntetés-végrehajtási szervezet a fenti célokat tekintve adatkezelési tevékenységet lát el, az GDPR és az Infotv. értelmében. Az intézmények és intézetek is természetesen ellátják az adatkezelési tevékenységet.⁶³⁸ A büntetés-végrehajtási rendszer egy integrált modellt képvisel, mely az igazságügyi szankciók végrehajtásától kezdve a társadalmi reintegrációig számos funkciót ölel fel.

Ebben a modellben értelmezendő a természetes személyek adatainak védelme. A büntetés-végrehajtási rendszeren belül a személyes adatok kezelése mind a büntetés-végrehajtásban dolgozó személyzetre, mind a fogvatartottakra vonatkozik. A fogvatartottak az Alaptörvény által biztosított alapvető jogokat, a bírósági határozatokban meghatározott specifikus korlátozásokkal és tilalmakkal összhangban, a büntetés-végrehajtási szabályoknak megfelelően gyakorolják.⁶³⁹ Ez a gyakorlatban azt jelenti, hogy bár a fogvatartottak jogosultak az alapvető emberi jogok gyakorlására, ezek gyakorlására azonban a vonatkozó jogszabályok által meghatározott, és a büntetés-végrehajtási rendszer sajátosságaiból eredő speciális szabályok és

⁶³⁷ 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről 4§.g) kezeli a büntetés-végrehajtási intézetek és intézmények kezelésében lévő közérdekű adatokat és közérdekből nyilvános adatokat, valamint a b)–f) pont szerinti irányítási jogkörök gyakorlásához szükséges, törvényben meghatározott személyes adatokat.

⁶³⁸ Infotv. 3.§. (10) a) „bűnüldözési célú adatkezelés(...)a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (..)ezen tevékenység keretei között és céljából (...) végzett adatkezelése” Lásd még: GDPR 1. cikk (2) és 4.cikk (2)

⁶³⁹ Magyarország Alaptörvényében a fogvatartottak jogait nem egy specifikus cikkely részletezi kifejezetten, hanem több általános rendelkezés érinti a fogvatartottak jogait közvetve, úgy mint az emberi méltósághoz, a szabadsághoz és a biztonsághoz való jog, valamint az egyenlő bánásmód elve.

korlátozások érvényesek. A szabályok és korlátozások a büntetés-végrehajtás céljainak megfelelő módon történő érvényesítését hivatottak szolgálni.

A büntetés-végrehajtási intézetek által kezelt személyes adatok jelentős része a személyes adatok különleges kategóriájába tartozik, ideértve az elítéltek és letartóztatottak adatait. A reintegráció kapcsán számos személyes adatot szükséges kezelni, mint például oktatási eredmények, pszichológiai értékelések, egészségügyi információk.

A büntetés-végrehajtási intézeteknek az információs rendszereikben tárolt adatokat illetően nem csak a fizikai biztonságot kell fenntartaniuk, hanem a digitális adatok és nyilvántartások védelmére is kiemelt figyelmet kell fordítaniuk.

A büntetés-végrehajtási szervezet biztonsági rendszerének értelmezése kritikus az adatkezelés kockázatainak megértéséhez. A biztonsági létesítmények, berendezések és technikai eszközök alkalmazása a büntetés-végrehajtásban elengedhetetlen a fogvatartottak biztonságának és a fogvatartás rendjének fenntartása szempontjából. Ezek az eszközök és berendezések széles skálán mozognak, beleértve a magas biztonságú cellákat, kamerarendszereket, mozgásérzékelőket, biztonsági záratokat és kapukat, valamint kommunikációs rendszereket.

A biztonsági létesítmények tervezésekor és kialakításakor figyelembe kell venni a biztonsági kockázatokat, a fogvatartottak elhelyezésének szükségességét, valamint a személyzet és a látogatók biztonságát. A kamerarendszerek és a mozgásérzékelők lehetővé teszik a folyamatos megfigyelést és az azonnali reagálást bármilyen rendellenesség vagy szökési kísérlet esetén. Fontosak a személyzet, a fogvatartottak és a külső szolgáltatások, például a mentőszolgálat vagy a rendőrség közötti gyors és hatékony kommunikáció biztosításához. Ezen rendszerekhez is számos adatvédelmi kérdés kapcsolható.

Az innovatív megoldások, mint például a biometrikus azonosítás vagy az intelligens videoanalitika, tovább növelhetik a biztonsági rendszerek hatékonyságát, ugyanakkor számos adatkezelési kérdést szintén felvethetnek.⁶⁴⁰

A büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény (a továbbiakban: Bv. Sztv.) alapján: „Az erre feljogosított szervezeti egység a biztonsági kockázatelemzés során a) a Bv. tv. 76. § (2) bekezdése szerinti személyes adatokat, b) a fogvatartotti nyilvántartás és a kapcsolattartói nyilvántartás adatait, c) a Bv. tv. szerinti biztonsági intézkedés alkalmazása és a fegyelmi eljárás lefolytatása során ismertté vált személyes adatokat, valamint d) az

⁶⁴⁰Kondás Katalin. (2021) "Biometria a börtönben." In: Biztonságtudományi Szemle, OE, 3. évfolyam 4. szám ISSN 2676-9042., pp. 1-10. <https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/185>

elektronikus megfigyelési eszköz által rögzített felvételt és az abban szereplő személyes adatot – a Bv. tv. 150. § (7) bekezdésében meghatározott korlátok között –kezeli⁶⁴¹.”

8.2. Jogszabályi háttér

A büntetés-végrehajtási jogviszony⁶⁴² kettős természetéből adódóan, ahol az egyik oldalon az elítélt és az egyéb jogcímen fogvatartott, a másik oldalon a végrehajtásért felelős szerv, valamint a végrehajtásban közreműködő más szervek és személyek állnak, a jogszabályi háttér mindkét jogviszonyt illetően kettős megközelítéssel bír. Az adatvédelmi szabályozás keretrendszerét az uniós szabályozás adja, egyrészt az általános adatvédelmi rendelet, másrészt a bűnüldözési célú adatkezelés esetén - beleértve a szankciók végrehajtását is - a bünyügyi adatvédelmi irányelv szerint az Infotv. biztosítja.

Általánosságban elmondható, hogy büntetés-végrehajtás során az egyes büntetés-végrehajtási tevékenységek mint adatkezelési célok, a 2013. évi CCXL. törvény⁶⁴³ (a továbbiakban Bvtv.) által kerülnek meghatározásra.. Az adatkezelési jogalap tekintetében, a fogvatartásra vonatkozó jogszabályi kötelezettségek esetében a Bvtv. szolgál alapként, míg más célok, például a munkavállalás vagy az oktatásban való részvétel esetében az általános adatvédelmi rendelet az irányadó. Az 1995. évi CVII. törvény, (továbbiakban BvSztv.)⁶⁴⁴ adatvédelmi rendelkezéseket tartalmaz a fogvatartottak nyilvántartására vonatkozóan a törvény V. fejezetében.

Ide sorolható továbbá, a 2009. évi XLVII. törvény⁶⁴⁵ (továbbiakban Bnytv.), amely a bünyügyi nyilvántartási rendszerről szól, amelynek IX. fejezete tartalmazza a vonatkozó adatvédelmi szabályokat. A Bnytv. szerint bünyügyi nyilvántartások a büntettesek személyek nyilvántartását, a büntetlen előéletű, mégis hátrányos jogkövetkezményekkel sújtott személyek nyilvántartását, a büntetőeljárás alatt álló személyek nyilvántartását és a külföldre utazási korlátozás alatt álló személyek nyilvántartását jelentik. A bünyügyi nyilvántartások kezelésének feladatát a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság végzi.

⁶⁴¹ Bvsztv 27/F.§

⁶⁴² Bvtv.7. §

⁶⁴³ 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról. A törvény az adatkezelés jogalapját szolgáltatja.

⁶⁴⁴ 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

⁶⁴⁵ 2009. évi XLVII. törvény a bünyügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bünyügyi és rendészeti biometrikus adatok nyilvántartásáról

A Bnytv. a bűnügyi nyilvántartások mellett külön rendelkezik a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, ami a daktiloszkópiai nyilvántartást és a DNS-profil nyilvántartást foglalja magában. Ezek a nyilvántartások elsősorban kriminalisztikai és szakértői jellegűek, és olyan speciális szakértelmet igénylő műveleteket tartalmaznak, amelyek az érintettek személyazonosságának pontos megállapítására irányulnak. Ebben az esetben, a biometrikus adatok nyilvántartásától eltérően, az adatkezelői feladatokat a Nemzeti Szakértői és Kutató Központ végzi.⁶⁴⁶

A Bnytv. IX. fejezet részletezi az érintettek tájékoztatására, valamint az adattovábbítási nyilvántartásra vonatkozó előírásokat a 87-88 szakaszok, valamint a 89-91/A. szakaszok alapján. Ezek a rendelkezések arra irányulnak, hogy a bűnügyi nyilvántartási rendszerben kezelt adatok felhasználása során is garantálják az érintettek jogainak védelmét, valamint elősegítsék az átláthatóságot és az adatkezelés jogi kereteinek betartását.

Jánosi Andrea elemezte a Bnytv. módosításait.⁶⁴⁷ Az elemzés világosan rámutat, hogy a Bűnügyi Nyilvántartásokról szóló törvény (Bnytv.) hatálybalépése óta több jelentős módosításon ment keresztül, amelyek nagy részét a jogharmonizációs kötelezettségek határozták meg. Megállapítja a Bnytv. által 2009-ben létrehozott keretrendszer alkalmasságát, amely továbbra is képes megfelelni az uniós elvárásoknak, és sikeresen integrálja az új jogintézményeket a magyar bűnügyi nyilvántartási rendszerbe. A legfrissebb módosítások között kiemelkedik az Európai Bűnügyi Információs Rendszer Harmadik Országok Állampolgárainak (ECRIS-TCN) bevezetése, amely a Bnytv.-ben megfogalmazott, az uniós jogforrások által előírt változtatásokat tartalmazza.

⁶⁴⁶ Nyeste, Péter. (2019.) "A bűnüldözési tevékenység során használt fontosabb nyilvántartások." In *A bűnügyi hírszerzés kézikönyve*, edited by Sub Lege Libertas, 181-199. Budapest: Nordex Nonprofit Kft.; Dialóg Campus Kiadó. ISBN 978-615-5945-79-3 (nyomtatott); 978-615-5945-84-7 (Online).

https://real.mtak.hu/128819/1/Web_PDF_A_bunugyi_hirszerzes_kezikonyve.pdf

Nem tartozik a büntetés-végrehajtáshoz, de megemlítem a rendőrség eModus rendszerét, melynek jelentős szerepe van a nyomozati munkában.

⁶⁴⁷ Jánosi, Andrea. (2022.) "A Magyar bűnügyi nyilvántartási rendszer az Európai Unió által megfogalmazott elvárások tükrében." *Miskolci Jogi Szemle* 16,(5), pp. 247-258. <https://doi.org/10.32980/MJSz.2021.5.1470>.

Speciális egészségügyi adatok kezelésével kapcsolatos esetekben az 1997. évi XLVII. törvény (továbbiakban Eüak. tv) ⁶⁴⁸, valamint az 1997. évi CLIV. törvény (továbbiakban Eü.tv) ⁶⁴⁹ az irányadók.

8.3. Adatkezelési elvek a büntetésvégrehajtás során

8.3.1.A Bv.tv. alapvető rendelkezései

A Büntetés-végrehajtási törvény alkalmazási köre magában foglalja a Büntető törvénykönyv által előírt büntetéseket és intézkedéseket, az előzetes letartóztatást, mint a Büntetőeljárás törvényben meghatározott szabadságkorlátozó kényszerintézkedések egyikét, továbbá a szabálysértések esetén alkalmazott büntetéseket, így a pénzbüntetést, helyszíni bírságot, és a közérdekű munkát helyettesítő szabálysértési elzárást. Emellett rendelkezik az utógondozás szabályairól is. Konkrétan a törvény hatálya⁶⁵⁰ a következő területeket öleli fel:

- A 2012. évi C. törvény, azaz a Büntető Törvénykönyv által meghatározott büntetések és intézkedések, továbbá a szabadságvesztésből és javítóintézeti nevelésből szabadulók utógondozása.
- A 2017. évi XC. törvény, a büntetőeljárásról szóló törvény alapján kiszabott letartóztatás, előzetes kényszergyógykezelés, őrizet és a Be. 128. § (2) szerinti rendbírság helyébe lépő elzárás.
- Az Európai Unió tagállamaival való bűnügyi együttműködés keretében, a 2012. évi CLXXX. törvény alapján történő őrizet, átadási és ideiglenes átadási letartóztatás, valamint az 1996. évi XXXVIII. törvény, a nemzetközi bűnügyi jogsegélyről szóló törvény szerinti kiadatási és ideiglenes kiadatási letartóztatás.
- A 2012. évi II. törvény, a szabálysértésekről és szabálysértési eljárásról szóló törvény értelmében végrehajtandó szabálysértési elzárások, továbbá a pénzbírság, helyszíni bírság és a közérdekű munkát helyettesítő szabálysértési elzárások végrehajtása.

A Bv.tv. meghatározza az állam feladatait is büntetésvégrehajtás során.⁶⁵¹ Ennek alapján az állam felelős a büntetések, intézkedések és szabálysértési elzárást érintő végrehajtásért,

⁶⁴⁸ 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

⁶⁴⁹ 1997. évi CLIV. törvény az egészségügyről. Különösen a 24. §, 137. § szakaszok.

⁶⁵⁰ 2013. évi CCXL, 2. §

⁶⁵¹ 2013. évi CCXL, 5. §

beleértve az utógondozást is. Az elítéltekre és más jogcímen fogvatartottakra a törvények és határozatok által meghatározott korlátozások alkalmazandók. Ezenkívül az állam a büntetés-végrehajtást többek között a bíróságok, ügyészség és rendőrség bevonásával hajtja végre, a törvényben meghatározott egyéb szervek segítségével. A végrehajtásért felelős szerv együttműködik oktatási intézményekkel és civil szervezetekkel a fogvatartás és a társadalmi reintegráció területein.

A végrehajtás során az elítéltet az alávetési, együttműködési és a lakcím-bejelentési kötelezettség terheli.⁶⁵² A törvény 8. szakaszának (3) bekezdése szerint az elítélt köteles minden, a büntetőeljárás lezárása után bekövetkezett változást, ami érinti lakcímét, értesítési, kézbesítési, vagy tényleges tartózkodási helyét, valamint elektronikus kommunikációs elérhetőségeit (pl. email, elektronikus kapcsolattartási cím, hangkapcsolatot biztosító elérhetőség), három munkanapon belül bejelenteni a végrehajtásért felelős szervnek vagy, ha ez nem lehetséges, a büntetőügyben első fokon eljáró bíróság területileg illetékes büntetés-végrehajtási bírójának. Ez magában foglalja a kézbesítési cím bejelentését és annak változását, valamint a lakcímtől eltérő tartózkodási hely és annak változása esetén történő bejelentést is. E rendelkező rész kifejezetten érinti az elítélt személyes adatait.

Az elítéltnak jogérvényesítése lehetősége van,⁶⁵³ valamint joga van a tájékoztatási joghoz is, amelyet az adatvédelmi jogtól elkülönítve is szabályoz a törvény. Ennek alapján az elítélteknek és más jogalapon fogvatartottaknak írásos formában kell megkapniuk a kötelező információkat, beleértve a panasztevési lehetőségeket, a jogorvoslati útmutatást, a védelmi jogokat, az iratokhoz való hozzáférés jogát, valamint a kapcsolattartási módokat. A tájékoztatási folyamat átláthatóságát és a jogok érvényesülését az biztosítja, hogy a tájékoztatás tényét és annak fogadását írásban kell dokumentálni.⁶⁵⁴

A Bv.tv. 17. szakasza a megkeresés és az adatkérés szabályait rögzíti. A büntetések, intézkedések és szabálysértések végrehajtásához, valamint az elítéltek és más jogalapon fogvatartottak kérelmeinek értékeléséhez a büntetés-végrehajtási bíró, az ügyészség, és a releváns minisztériumok jogosultak információ kéréssel fordulni állami és önkormányzati szervekhez, valamint civil szervezetekhez. Az ilyen információkérések adatszolgáltatást, adattovábbítást és dokumentumok megosztását célozhatnak, nyolc és harminc nap közötti határidővel. Amennyiben a kérés személyes adatokra terjed ki, az csak a cél eléréséhez

⁶⁵² 2013. évi CCXL, 8.§

⁶⁵³ 2013. évi CCXL, 10.-11.§

⁶⁵⁴ 2013. évi CCXL, 12.§. A törvény tételesen felsorolja a tájékoztatás tartalmi elemeit.

nélkülözhetetlenül szükséges adatokra korlátozódhat, az adatkezelés céljának és a kért adatok körének pontos megjelölésével. Ezenkívül amennyiben feladataik megkövetelik, a büntetés-végrehajtási bíró, az ügyészség, valamint az igazságügyi, a gyermekek és ifjúság védelméért, és a büntetés-végrehajtásért felelős miniszterek, továbbá a végrehajtásért felelős szerv jogosult információ, dokumentum és tájékoztatás beszerzésére egymástól, a büntetőügyekben és szabálysértési ügyekben eljáró vagy eljáró bíróságoktól, ügyészségektől és nyomozó hatóságoktól. A halasztás, részletfizetés megítéléséhez és a kegyelmi eljárás során a bíróság a Büntetőeljárásról szóló törvény adatkéréssel kapcsolatos szabályai alapján kérhet adatszolgáltatást.

A sértett jogairól is rendelkezik a Bv.tv. A sértettek jogosultak arra, hogy értesítést kapjanak bizonyos jogilag meghatározott események bekövetkeztekor. Ez kiterjed az életet, testi épséget, és egészséget szándékosan veszélyeztető cselekményekre, amelyekért az elkövetőt öt évnél hosszabb szabadságvesztés büntetéssel sújthatják⁶⁵⁵ valamint a nemi élet szabadságát és nemi erkölcsöt sértő bűncselekményekre.^{656,657} A bíróság, az ügyészség, a BVOP, a büntetés végrehajtási intézet és a javítóintézet a kérelmező kérelmét, nevét és lakcímét zártan kezeli és biztosítja, hogy ezek az adatok ne jussanak az elítélt vagy az egyéb jogcímen fogvatartott tudomására.⁶⁵⁸

A büntetés-végrehajtás során az elítéltek, vagy egyéb jogcímen fogvatartottak, valamint azok védői, képviselői, és bizonyos esetekben családtagjai jogosultak a végrehajtás során keletkezett dokumentumok megismerésére.⁶⁵⁹ Ez magában foglalja az iratokba való betekintést, jegyzetelést, és bizonyos feltételek mellett másolatkérési jogot, kivéve amikor minősített adatokat tartalmaznak. A minősített adatot tartalmazó irat megismerésére a Be. 105–106. szakaszait értelemszerűen alkalmazni kell. A végrehajtásért felelős szerv köteles a kérelemre nyolc munkanapon belül válaszolni. Az iratban fel kell jegyezni, vagy a fogvatartotti nyilvántartásban, illetve a belső elektronikus ügykezelő rendszerben rögzíteni kell, hogy mely

⁶⁵⁵ Btk. XV. fejezet

⁶⁵⁶ Btk. XIX. fejezet

⁶⁵⁷ 2013. évi CCXL, 13.§. Az értesítési kötelezettség az alábbi körülményekre vonatkozik: az elítélt szabadon bocsátása (akár véglegesen, akár feltételesen), az előzetes letartóztatásból történő szabadon bocsátás, a szabadságvesztés végrehajtásának félbeszakítása, az elítélt vagy előzetesen letartóztatott szökése, fiatalkorúak javítóintézeti nevelésből való végleges vagy ideiglenes kiengedése, illetve a javítóintézetből való engedély nélküli távozás

⁶⁵⁸ 2013. évi CCXL, 13.§ (5)

⁶⁵⁹ 2013. évi CCXL, 26.§

iratról, mely időpontban, kinek a részére, hány példányban készült másolat. Bizonyos dokumentumok, mint például előkészítő tervezetek, kockázatelemzések, biztonsági iratok és egyéni feljegyzések, kivételt képeznek a megismerési jog alól. Másolatkérés esetén a nem jogosult adatokat ki kell zárni. A megismerési jog megtagadása esetén indoklás kötelező, ellenében bírósági felülvizsgálat kérhető. Egészségügyi dokumentáció esetében külön jogszabályok érvényesülnek.⁶⁶⁰

Az elektronikus kapcsolattartás szabályai kapcsán a Be. szabályai az irányadók.⁶⁶¹

A Védelmi Programban való részvétellel kapcsolatos rendelkezések több olyan személyes adatot jelölnek meg, melyet zártan kell kezelni. A Védelmi Program résztvevőinek büntetés-végrehajtási jogviszonyából eredő jogai és kötelezettségei változatlanok maradnak, azonban a részvételükhöz kapcsolódóan különös szabályok vonatkoznak rájuk: az érintettek ügyiratait zártan kell kezelni, értesítések és hivatalos iratok kézbesítése csak a védelmet ellátó szervezeten keresztül történik, a védett személyek azonosító adatait és az eljárások során azok kezelése szigorúan szabályozott, a védett személy lakcím helyett a védelmet nyújtó szerv címét használhatja, a védelmet ellátó szerv tagjai jelen lehetnek minden releváns eljárásban, és a fogvatartott védett személyek kommunikációja és kapcsolattartása a védelmet ellátó szervezeten keresztül zajlik.⁶⁶²

8.3.2. Bv.tv. - Az adatkezelésre vonatkozó rendelkezések

Az adatkezelési rendelkezések a Büntetés-végrehajtásról szóló törvény alapján meghatározzák az adatkezelésre jogosultak körét és a kezelt adatok körét. Az előírások célja a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési eljárás végrehajtásához kapcsolódóan kezelt adatok szigorú szabályozása, biztosítva ezzel a személyes adatok védelmét és a törvényesség elvét.⁶⁶³

A büntetés-végrehajtásra vonatkozó adatkezelési rendelkezések a büntető igazságszolgáltatás és a szabálysértési eljárások keretében keletkező adatok komplex kezelési keretét határozzák meg. Ezek a rendelkezések biztosítják, hogy a bíróság, az ügyészség és a végrehajtásért felelős

⁶⁶⁰ Az egészségügyi dokumentációval kapcsolatos iratbetekintésre és másolat kiadására az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló törvény, valamint az egészségügyről szóló törvény rendelkezéseit kell megfelelően alkalmazni.

⁶⁶¹ 2013. évi CCXL. 26/A. §

⁶⁶² 2013. évi CCXL. 26/B. §

⁶⁶³ 2013. évi CCXL IV. fejezet 76 §

szerv számára lehetővé váljon a büntetések, intézkedések, bizonyos kényszerintézkedések és a szabálysértések elzárásának végrehajtásához szükséges adatok hatékony kezelése.⁶⁶⁴ Ebben a kontextusban a törvény kiterjed az alábbi adatkörök kezelésére:

1. Alapadatok: ide tartoznak a büntetőügyekben és kényszerintézkedések esetében releváns alapadatok, mint például az eljáró bíróság vagy ügyészség azonosítója, a határozatok száma, kelte és jogerősítésének napja, valamint a kiszabott büntetések vagy intézkedések részletei.⁶⁶⁵
2. Személyes adatok: az elítéltek és egyéb jogcímen fogvatartottak személyazonosító adatai, állampolgársága, lakcíme, elektronikus kapcsolattartási adatai és egyéb releváns személyes információk.⁶⁶⁶
3. Speciális adatkörök: A családi állapot, iskolai végzettség, szakképzettség, valamint a kényszergyógykezeltekkel kapcsolatos adatok kezelése.⁶⁶⁷ Ezen túlmenően a törvény előírja a törvényes képviselők, védők, és az elítéltek családtagjaik személyes adatainak kezelését is, amennyiben az szükséges.⁶⁶⁸
4. Az adatkezelés korlátozásai: A törvény meghatároz bizonyos korlátozásokat és kivételeket, melyek meghatározzák, hogy mely adatok nem tekinthetők meg, illetve mely esetekben korlátozódik az adatokhoz való hozzáférés.⁶⁶⁹
8. Biztonsági intézkedések: A törvény előírja a személyes adatok védelmére vonatkozó biztonsági intézkedéseket, amelyek célja az adatok illetéktelen hozzáférés elleni védelem, az adatvesztés, adattörlés vagy adatmegsemmisítés megelőzése és az adatintegritás megőrzése.⁶⁷⁰
9. Elektronikus megfigyelés: A törvény részletezi az elektronikus megfigyelési eszközök által rögzített adatok kezelésére vonatkozó szabályokat, beleértve az ilyen adatok felhasználását biztonsági kockázatelemzés során.⁶⁷¹

⁶⁶⁴ 2013. évi CCXL 76. § (1)

⁶⁶⁵ 2013. évi CCXL 76. § (2) a.

⁶⁶⁶ 2013. évi CCXL 76. § (2) b.

⁶⁶⁷ A Büntetés-végrehajtási törvény 76. § (2) bekezdés m) pontja kiterjeszti az adatkezelést az elítéltek vagy más jogcímen fogvatartottak személyes adataira, különösen az egészségi állapotukra, káros szenvedélyeikre és bűnügyi adataikra, a jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges információkra.

⁶⁶⁸ 2013. évi CCXL 76. § (2) c).- (uf).

⁶⁶⁹ 2013. évi CCXL 78. § (1)-(4)

⁶⁷⁰ 2013. évi CCXL 79. §

⁶⁷¹ 2013. évi CCXL 76. § (3) a.)

10. Arcképfelismerő rendszerek: A törvény lehetővé teszi az arcképfelismerő rendszerek alkalmazását bizonyos körülmények között, például a fogvatartottak mozgásának és tevékenységének ellenőrzése, vagy bűncselekmények, szabálysértések és fegyelmi vétségek elkövetőinek azonosítása céljából.⁶⁷²
11. Speciális adatkezelési körülmények: A törvény részletezi a különleges adatkezelési körülményeket, mint például a kegyelmi eljárások, a nemzetközi bűnügyi jogsegély, a reintegrációs őrizet, vagy a javítóintézeti nevelés során keletkező adatkezelési gyakorlatokat.⁶⁷³
12. Adatok törlése: Előírja, hogy bizonyos esetekben, mint például a büntetés-végrehajtás befejezésekor vagy a végrehajthatóság megszűnésekor, a kezelt személyes adatokat törölni kell, hacsak törvény másképp nem rendelkezik.⁶⁷⁴
13. Statisztikai és tudományos felhasználás: Megengedi az anonimizált adatok statisztikai és tudományos célú felhasználását, biztosítva az érintettek magánéletének védelmét és az adatok személyazonosításra való alkalmatlanságát.⁶⁷⁵

A büntetés-végrehajtás során keletkezett irat megismerésének joga⁶⁷⁶ - megfeleltethető az Infotv. szerinti hozzáférés jogának - alapvető a személyes adatok védelme szempontjából. A büntetőeljárás során keletkező dokumentumokhoz bizonyos feltételek mellett hozzáférhetnek az érintettek, védőik, valamint egyéb jogosultak. Ez magában foglalja a dokumentumokba való betekintést, feljegyzések készítését, és másolatkérési jogot is, amennyiben nincs jogszabályi akadálya. Az adatok kezelése szigorúan szabályozott, és bizonyos esetekben korlátozások alá esik, mint például a döntés-előkészítés vagy biztonsági vizsgálatok dokumentumai. A hozzáférés megtagadása esetén indokolt határozat szükséges, amely ellen bírósági felülvizsgálati kérelmet lehet benyújtani. Az egészségügyi dokumentáció esetében külön törvényi szabályozás vonatkozik a hozzáférésre.⁶⁷⁷

Összefoglalva a törvény részletezi a kezelhető adatokat, beleértve a személyes adatokat, bűnügyi személyes adatokat és különleges adatokat. Ezen adatkategóriák széles körűek, tartalmazva az elítéltek és fogvatartottak nevét, lakcímét, értesítési címét, elektronikus elérhetőségeit, egészségügyi adatait, bűnügyi előéletre vonatkozó információkat és más

⁶⁷² 2013. évi CCXL 76.§ 3.a

⁶⁷³ 2013. évi CCXL 77.§ - 78. §

⁶⁷⁴ 2013. évi CCXL 79. §

⁶⁷⁵ 2013. évi CCXL 81. §

⁶⁷⁶ Megállapította a 2017.évi CXCVII törvény 421.§ (1) , hatályos 2018.VVI.1 -től

⁶⁷⁷ Eüak.tv és Eü.tv.

személyes jellemzőket. Új elemként a törvény kiterjesztette az adatkezelést az elektronikus kapcsolattartási adatokra is.⁶⁷⁸ A büntetésvégrehajtás során szükséges az elektronikus megfigyelési eszközök és az arcképfelismerő rendszerek használata. Az elektronikus megfigyelési eszközök alkalmazása kiterjedhet az elítélt vagy fogvatartott személyek mozgásának nyomon követésére, míg az arcképfelismerő rendszerek az azonosításukat és tevékenységeik ellenőrzését szolgálják.⁶⁷⁹

A Bv.tv.150. szakasza az elektronikus megfigyelési eszközök használatára vonatkozóan az adatkezelés céljait részletezi, amelyek elsősorban a végrehajtás rendjének és a fogvatartás biztonságának fenntartására irányulnak. Ezek közé tartozik az elítéltek mozgásának nyomon követése, a büntetés-végrehajtás rendjének fenntartása, bűncselekmények, szabálysértések és fegyelmi vétségek megelőzése, valamint különös figyelemmel kíséri azokat az elítélteket, akik korábban öngyilkosságot kíséreltek meg, biztonsági elkülönítőben, HSR-részlegen⁶⁸⁰ vagy magánzárkában helyezkednek el. Az elektronikus megfigyelőeszközök alkalmazása ezen célok elérése érdekében történik, biztosítva ezzel a büntetés-végrehajtási intézmények biztonságos és zavartalan működését. A jogszabály az elektronikus megfigyelés során rögzített felvételek és az azokban szereplő személyes adatok felhasználásának céljait is pontosan körvonalazza. Ezek magukban foglalják a bűncselekményekkel, szabálysértésekkel és fegyelmi vétségekkel kapcsolatos eljárásokban való felhasználást, továbbá az alkalmazott kényszerítő eszközök jogszerűségének értékelését. Emellett lehetőséget biztosít az érintett személyek számára, hogy jogi jogosultságaik gyakorlása érdekében más eljárások keretében is hivatkozzanak ezekre az adatokra. Ennek a szabályozása fontos a biztonsági kockázatelemzés és az intézetek biztonságának növelése szempontjából, amelynek jogszabályi alapját a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény 27/A. § (1) bekezdése alapján folytatott biztonsági kockázatelemzési kötelezettség biztosítja.⁶⁸¹ Bizonyos esetekben a büntetésvégrehajtás során az annak végrehajtását érintő eljárások kapcsán - különösen a kegyelmi eljárások és a nemzetközi bűnügyi jogsegély keretében- az igazságügyért felelős miniszter is kezel bizonyos adatokat. Kizárólag azokat a személyes adatokat ismerheti meg és kezelheti, amelyek kegyelem

⁶⁷⁸ 2013. évi CCXL 76 § (2)

⁶⁷⁹ 2013. évi CCXL 76 § (3b)

⁶⁸⁰ Hosszúidős Speciális részleg

⁶⁸¹ 2013. évi CCXL 76 § (3a) Az elítélt vagy más jogcímen fogvatartott személyek adatai, valamint az elektronikus megfigyelési eszközök által rögzített felvételek, szigorú jogi keretek között, felhasználhatók a büntetés-végrehajtási szervezet által végzett biztonsági kockázatelemzés céljából. Ez a gyakorlat a 1995. évi CVII. törvény 27/A. § (1) bekezdése és a 150. § (7) bekezdésében meghatározott korlátoknak megfelelően történik.

iránti előterjesztéshez, továbbá a jogsegélykérelem elintézéséhez és a bűnügyi jogsegélyről szóló jogszabályokban meghatározott vagy nemzetközi egyezményből eredő egyéb feladatai teljesítéséhez szükségesek.⁶⁸²

A büntetésvégrehajtás során a rendőrség is jogosult az érintettek adatainak kezelésére, tekintettel arra, hogy az általuk fogatosított kényszerintézkedések beleszámítanak a kiszabott büntetés időtartamába. Jogosultságuk vonatkozik az őrizetbe vett személyek, letartóztatottak, szabálysértési elzárás alatt állók, pártfogó felügyelet alatt állók, valamint az előállított vagy szállított személyek adatainak kezelésére.⁶⁸³

Amennyiben törvény eltérően nem rendelkezik, az adatokat a büntetés, az intézkedés, a kényszerintézkedés vagy a szabálysértési elzárás végrehajtásának befejezésekor, vagy végrehajthatóságának megszűnésekor törölni kell.⁶⁸⁴ A Bv.Szvtv. 32. szakasza (1) bekezdése alapján a fogvatartottról szóló adatokat 25 évig kell megőrizni. A (2) és (3) bekezdés szerint azonban a kapcsolattartói és sértettel kapcsolatos adatokat a szabadulásakor törölni kell a nyilvántartásból. Az egészségügyi dokumentációk esetében a külön törvény hosszabb, akár 30 vagy 50 éves megőrzési időt ír elő. Adott esetben ellentmondás állhat fenn, főként, ha sor került egészségügyi adatok kezelésre.

A büntetésvégrehajtás kapcsán megemlítendő a pártfogó felügyelet intézménye.⁶⁸⁵ A törvény meghatározza, hogy a pártfogó felügyelő milyen bűnügyi személyes adatokat igényelhet és vehet át a bűnügyi nyilvántartó szervtől. Ez a rendelkezés biztosítja a pártfogó felügyelet hatékony ellátásához szükséges adatok hozzáférhetőségét, ugyanakkor szigorú keretek között tartja az adattovábbítást.⁶⁸⁶

A törvény lehetővé teszi az elítéltek, fogvatartottak, pártfogó felügyelet alatt állók és utógondozottak adatainak statisztikai és tudományos célú felhasználását, amennyiben ez az

⁶⁸²2013. évi CCXL. 77 § (1)

⁶⁸³ 2013. évi CCXL 78 § (1) A rendőrség „, a Be. szerinti őrizet, ha a letartóztatást, a szabálysértési elzárást rendőrségi fogdában hajtják végre, a letartóztatás, a szabálysértési elzárás, a pártfogó felügyelet, az elítélt vagy az egyéb jogcímen fogvatartott más ügyben történő előállítás, szállítása, és a reintegrációs őrizet végrehajtásához szükséges adatokat ismerheti meg és kezelheti.

⁶⁸⁴ 2013. évi CCXL 79 § (1)

⁶⁸⁵ 2013. évi CCXL 68 § (1) „A bv. intézet a pártfogó felügyeletnek a feltételes szabadságra bocsátáskor való elrendelése [Btk. 69. § (1) bekezdés b) pont] iránt a feltételes szabadságra bocsátás esedékessége előtt az 57. § (1) bekezdésében írt előterjesztéssel együtt tesz előterjesztést a büntetés-végrehajtási bíróhoz.”

⁶⁸⁶ 2013. évi CCXL 80 § (1)

azonosításra alkalmatlan módon történik. Ez a bekezdés kiterjeszti az adatkezelés lehetőségeit kutatási és elemzési célokra, azonban kizárólag anonim formában.⁶⁸⁷

Véleményem szerint a személyes adatok kezelése során a büntetésvégrehajtás területén a jogi keretek szigorúak, a törvényi szabályozás a GDPR és Infotv. szabályait lefedi. A jogszabályi háttér tekintetében nem csak törvényi szabályozás, hanem rendeletek, utasítások, szabályzatok is tartalmaznak adatvédelmi előírásokat az egyes területeknek megfelelően. A jogszabályok hierachiájában azonos szintű törvények - Bvtv. és Eüaktv. ellentmondásait a jogalap meghatározása oldhatja fel.

F Az adatkezelők felelőssége nagy, károkozás esetén kártérítésre és sérelemdíj fizetésére kötelezhetők. A bizonyítási teher az adatkezelőre hárul, aki köteles igazolni, hogy az adatkezelés jogszabályoknak megfelelt.⁶⁸⁸

A büntetésvégrehajtási intézményekben folytatott különböző tevékenységek, mint például oktatási programok, munka, vagy rehabilitációs kezdeményezések, szintén adatkezelési tevékenységeket vonnak maguk után. Az elítéltek részvétele önkéntes alapon történik, és az adatkezelés ezen kontextusban is az adatvédelmi szabályoknak - ebben az esetben a GDPR – nak megfelelően kell, hogy történjen.

8.4. A fogvatartott nyilvántartása

A fogvatartottak nyilvántartásáról a Bv.Szvtv. V. fejezete rendelkezik. A büntetés-végrehajtási intézmények helyi és központi nyilvántartással rendelkeznek, előbbi a fogvatartó büntetés-végrehajtási (Bv.) szerv, utóbbi az Országos Parancsnokság hatásköre. Ezek a nyilvántartások átfogó adatokat tartalmaznak a fogvatartottakról, beleértve azonosító adatokat, Társadalombiztosítási Azonosító Jelet (TAJ), fényképeket, lakcímeiket, valamint a büntetés-végrehajtás során keletkező, a fogvatartott jogainak gyakorlásához szükséges adatokat és iratokat. Ezen kívül magukban foglalják a büntetőeljárás során, illetve a fogvatartottal kapcsolatos egyéb eljárásokban keletkezett, a büntetés-végrehajtási szervezet részére megküldendő iratokat is.⁶⁸⁹

⁶⁸⁷ 2013. évi CCXL 81 § (1)

⁶⁸⁸ Büntetés-végrehajtás Tudományos Tanácsa. 2015. "Korszakváltás a büntetés-végrehajtásban: Útmutató a 2013. évi CCXL (Bv.) törvény megismeréséhez." Budapest: 37. https://bm-tt.hu/wp-content/uploads/2022/02/Korszakvaltas_LO-RES.pdf.

⁶⁸⁹ Bvszvtv 28.§, (1)

A bv. szervezet külön nyilvántartást vezet azokról a személyekről, akikkel a fogvatartott kapcsolatot tart fenn. Ez magában foglalja a kapcsolattartók személyes adatait, mint például név, lakcím vagy értesítési cím, telefonszám, amennyiben ez a kapcsolattartás formája miatt szükséges, továbbá a kapcsolattartói minőséget, születési helyet és időt, anya születési nevét, valamint az elektronikus kapcsolattartás érdekében szükséges adatokat, mint az elektronikus levelezési cím és a telekommunikációs alkalmazásban regisztrált azonosító név. Ezenfelül nyilvántartásba veszik a hivatalos minőségben kapcsolatot tartó személyeket is, beleértve a személyes adatokat és a hivatalos kapcsolatot igazoló okmányok adatait.⁶⁹⁰

Elektronikus kapcsolattartás esetén, amely telekommunikációs eszközök segítségével történik, minden érintettnek, beleértve a kapcsolattartó személyeket és az hivatalos minőségben eljáró személyeket is, személyazonosságuk igazolására alkalmas okmányt kell felmutatniuk.⁶⁹¹ Ez magában foglalja a hivatásuk gyakorlására jogosító igazolványokat is, különösen, ha ez az első kapcsolatfelvétel alkalmával történik.

A bv. szerv, a bíróság vagy az ügyészség értesítése alapján nyilvántartja azon sértettek adatait, akik a fogvatartott szabadulásáról vagy szökéséről szeretnének értesítést kapni. Ezen adatok magukban foglalják a kérelmező nevét és a megadott értesítési címet.⁶⁹²

Az adatkezelő szerv – bizonyos kivételekkel – továbbítja az általa kezelt adatokat és teljes körű tájékoztatást biztosít az illetékes állami szervek, nemzetbiztonsági szolgálatok, és állampolgárok számára, amennyiben ez szükséges feladataik ellátásához vagy jogos érdekeik érvényesítéséhez. Az adatszolgáltatási kérelemnek tartalmaznia kell az adatkérés indokát és jogalapját.⁶⁹³

A fogvatartottak adatai – személyazonosításra alkalmatlan formában – statisztikai és tudományos célokra is felhasználhatók.⁶⁹⁴

A BvSztv. szabályozza az adatok nemzetközi továbbítását is. A büntetés-végrehajtási szervezet által kezelt személyes adatok, a sértettekkel kapcsolatos kivételezett információkon kívül, átadhatók az Európai Unió tagállamainak, az EU által alapított nemzetközi bűnüldöző szervezeteknek, amennyiben ez az EU jogi aktusainak végrehajtását szolgálja, vagy két- vagy

⁶⁹⁰ Bvsztv 28.§ A. (1)- (3)

⁶⁹¹ Bvsztv 28.§ (4). Amennyiben a felmutatott okmányok és a bv. szerv nyilvántartásában szereplő adatok között eltérés tapasztalható, vagy az arckép alapján kétségek merülnek fel az azonosságot illetően, és a kapcsolattartásra jelentkező személy nem tesz eleget a felmutatási kérésnek, az elektronikus kapcsolattartásra nem kerülhet sor.

⁶⁹² Bvsztv 28/B. § (1) 2017. évi XC. törvény 52. §-a alapján

⁶⁹³ Bvsztv 29.§ (1) - (3)

⁶⁹⁴ Bvsztv 29.§ (4)

többoldalú nemzetközi megállapodások alapján szükséges. Az adatok átadása során biztosítani kell, hogy az átvevő fél számára rendelkezésre álljanak azok az információk, melyek az adatok pontosságának, teljességének, frissességének és megbízhatóságának értékelését teszik lehetővé.⁶⁹⁵

Az adattovábbítás során ki kell emelni azokat a korlátozásokat, amelyek az adatkezelés során érvényesülnek, valamint az adatkezelés időtartamát, amit az adatkezelő szerv határoz meg. Nemzetközi szerződés alapján.⁶⁹⁶

Harmadik országok hatóságainak vagy az említett nemzetközi szervezeteken kívüli egyéb nemzetközi szervezetek részére adatok csak akkor továbbíthatók, ha az átvevő fél tevékenysége a bűncselekmények megelőzésére, nyomozására, felderítésére, büntetőeljárás lefolytatására vagy büntetőjogi szankciók végrehajtására irányul. Ez a szabályozás nem vonatkozik a sértettekkel kapcsolatos információkra, amelyeket nem lehet harmadik országok vagy az említett nemzetközi szervezeteken kívüli szervezetek részére továbbítani.⁶⁹⁷

Az Európai Unió tagállamaihoz, az EU által létrehozott nemzetközi bűnüldöző szervekhez, harmadik országok illetékes hatóságaihoz, valamint a szabályozásban külön meghatározott nemzetközi szervezeteken kívüli egyéb nemzetközi szervezetekhez korábban továbbított vagy hozzáférhetővé tett személyes adatok - harmadik országok vagy a fent említett nemzetközi szervezeteken kívüli nemzetközi szervezetek részére csak akkor adhatók át, ha azt az átadó hatóság vagy szervezet kifejezetten engedélyezte, amihez az adott hatóságnak vagy szervezetnek természetesen a nemzeti jogszabályaival vagy az alkalmazandó nemzetközi szerződésekkel összhangban kell eljárnia.⁶⁹⁸

A büntetés-végrehajtási szervezet, valamint az adatokra szolgálati-, jogi-, vagy egyéb okból jogosult szervek, szervezetek és magánszemélyek kizárólag a törvényben meghatározott céljaik elérése érdekében, illetve a jogos érdekeik érvényesítése céljából használhatják fel a fogvatartottak adatait. Ezen adatok felhasználása tehát szigorúan korlátozott, célhoz kötött, és csak a jogszabályban meghatározott feladatok ellátásához vagy jogok gyakorlásához igazodik. A fogvatartott jogosult a róla nyilvántartott adatokhoz való hozzáférésre, azok helyesbítésére vagy jogellenesen kezelt adatok törlésére irányuló kérelmének benyújtására, amelyeknek a büntetés-végrehajtási szervnek eleget kell tennie. Ez a jog azonban korlátozás alá eshet,

⁶⁹⁵Bvsztv 9/A. § (1)

⁶⁹⁶ Bvsztv 9/A. § (3)

⁶⁹⁷ Bvsztv 9/A. § (4)

⁶⁹⁸ Bvsztv 9/A. § (5)

amennyiben bizonyos adatok, például a fogvatartás biztonságával kapcsolatos információk, az intézkedés jellegéből fakadóan nem tehetők közzé. Azonban a fogvatartott szabadulásakor, bizonyos minősített adatok kivételével, kérésre ezek az információk is megismerhetővé válnak számára.⁶⁹⁹

A fogvatartottnak az adataival való rendelkezés jogát nem lehet úgy értelmezni, hogy az sérti az igazságszolgáltatás, a bűnüldözés vagy az állami és önkormányzati feladatok ellátásához szükséges adatkezelési követelményeket. Az adatkezelő szerv köteles gondoskodni az adatok védelméről, az adatokhoz való hozzáférés, azok illetéktelen kezelése elleni védelemről, valamint az adatok pontosságának és aktualitásának megőrzéséről.

Kondás az adatvédelem kapcsán, a börtönökben az információs rendszerekben tárolt adatok védelmét vizsgálta, mind a hozzáférési szerepkörök, mind az adatbiztonság szemszögéből.⁷⁰⁰

Tapasztalatai szerint a gyakorlatban jól működik a jogosultsági mátrix alkalmazása. A felhasználók jogosultságainak kiosztása a vezető vagy az adatgazda engedélyével történik, és ez az informatikai rendszergazda feladatkörébe tartozik.⁷⁰¹

A Büntetés-végrehajtás Informatikai Biztonsági Szabályzatának (IBSZ) fő célja az, hogy az informatikai rendszerek használata közben garantálja az információk védelmét és megelőzze a jogosulatlan hozzáféréseket. Az adatok bizalmassága, hitelessége, sértetlensége és elérhetősége alapvető követelmények, melyeket a rendszernek folyamatosan kell biztosítania.⁷⁰²

A büntetés-végrehajtási szerv kötelezettsége, hogy a fogvatartottról gyűjtött adatokat a büntetés vagy intézkedés végrehajtásának befejezését követően, vagy annak végrehajthatatlansága esetén, huszonöt éven át megőrizze. A fogvatartott szabadulásakor a kapcsolattartói adatokat és a sértettel kapcsolatos, értesítési kérelem alapján nyilvántartott adatokat a nyilvántartásból törölni kell. Amennyiben újabb büntetőeljárás indult a fogvatartott ellen, és ez megszűnik – például felmentés vagy az eljárás megszüntetése miatt – az ezzel kapcsolatos adatokat szintén törölni kell a nyilvántartásból, biztosítva ezzel az érintett jogainak védelmét.⁷⁰³

Összefoglalva az itt tárgyalt adatkezelési és nemzetközi adattovábbítási szabályozások összhangban állnak a bűnügyi irányelv előírásaival és az Infotv. törvény releváns szakaszaival. A szabályozás különös figyelmet fordít arra, hogy az adattovábbítás csak meghatározott

⁶⁹⁹ Bvsztv 30.§

⁷⁰⁰ Kondás, Katalin. "Adatok védelme a börtönökben." *Hadmérnök* 13, no. 1 (2018 március): 269-277.

⁷⁰¹ Ibid., 274.o

⁷⁰² A büntetés-végrehajtás országos parancsnokának 9/2016. (II.16.) OP szakutasítása a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról

⁷⁰³ Bvsztv 31.§ - 32.§

célokra, mint a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából történhessen. Az adattovábbítás csak akkor lehetséges, ha a harmadik országok vagy a nemzetközi szervezetek illetékes hatóságai megfelelnek bizonyos adatvédelmi és jogállamisági követelményeknek, amelyek összhangban állnak az EU és az Infotv. előírásaival. Az adatkezelő szervek kötelesek gondoskodni az adatok biztonságáról, az adatokhoz való illetéktelen hozzáférés megakadályozásáról, valamint az adatok pontosságának, teljességének és naprakészségének ellenőrzéséről. Az adatszolgáltatásra irányuló kérelemnek tartalmaznia kell az adatkérés indokát és jogszabályi alapját, így biztosítva az adatkezelés átláthatóságát és célhoz kötöttségét, lehetővé téve az adatok hatékony felhasználását a bűnüldözés és az igazságszolgáltatás területén.

8.5. Mesterséges intelligencia rendszerek és a büntetésvégrehajtás kapcsolata és annak hatása a személyes adatok védelmére

A 2021. október 6-i dátummal kiadott Európai Parlament állásfoglalása⁷⁰⁴ kiemeli, hogy a mesterséges intelligencia már széles körben alkalmazásra kerül a bűnüldözés területén. Az állásfoglalás olyan technológiák használatát sorolja fel, mint az arcfelismerés, a gyanúsítottak adatbázisainak átkutatása, az emberkereskedelem és a gyermekbántalmazás áldozatainak felkutatása, az automatikus rendszámfelismerő rendszerek, a hangfelismerés, azonosítás, a szájról olvasás, a lövésdetektáló algoritmusok, adatbáziselemzések, prediktív rendőrségi munka, viselkedésmegfigyelő eszközök, virtuális boncolás, pénzügyi csalás és terrorizmusfinanszírozás felderítése, közösségimédia-elemzés, valamint különféle megfigyelési rendszerek, mint például a szívritmus és hőképeségű kamerák használata. Az állásfoglalás továbbá megjegyzi, hogy a mesterséges intelligencia eszközeit és alkalmazásait globális szinten már az igazságszolgáltatás is felhasználja, így például letartóztatási határozatok, ítélethirdetések, visszaesés valószínűségének becslése, próbaidő meghatározása, online vitarendezés, ítélezési gyakorlatok kezelése és a joghoz való hozzáférés javítása terén.

⁷⁰⁴ Európai Parlament. 2021. október 6. "Állásfoglalás a mesterséges intelligenciáról a büntetőjogban, és annak a rendőrség és az igazságügyi hatóságok általi felhasználásáról büntetőügyekben (2020/2016(INI))."

Az állásfoglalással egyetértve, Herke is hangsúlyozza, hogy a mesterséges intelligencia alkalmazása során szigorúan be kell tartani az etikai és jogi kereteket.⁷⁰⁵

Hazánkban a büntetés végrehajtásban használnak MI alapú eszközöket. Különösen óvatosak vagyunk a mesterséges intelligencia igazságszolgáltatásban betöltött szerepének értékelésében.⁷⁰⁶

A modern technikai eszközök bevezetése a büntetés-végrehajtásban azt célozza, hogy egyszerűsítse és hatékonyabbá tegye a napi munkát, csökkentve a hibázási lehetőségeket és az időgazdálkodást optimalizálva. Okoseszközök és mesterséges intelligencia alapú fejlesztések támogatják a személyi állományt stabil, könnyen kezelhető, adminisztrációs terheket csökkentő és felhasználóbarát technikai háttérrel biztosítva.

A SAFE rendszer egy mobiltelefon méretű, chip alapú információs készülék, amit a büntetés-végrehajtási szervezet használ. Célja a gyors és egyszerű adatlekérés, amely a Fogvatartotti Alap nyilvántartásból⁷⁰⁷ származó adatokhoz nyújt hozzáférést. A rendszer bevezetésével a büntetés-végrehajtási személyzet adminisztrációs feladatainak hatékonysága növekszik. A SAFE nem csak egy eszköz, hanem egy adatbázis-kezelő rendszer is, ami kifejezetten a büntetés-végrehajtás egyedi igényeire lett szabva. A rendszer WiFi vagy APN technológián keresztül kapcsolódik a központi szerverhez, lehetővé téve az adatok offline elérését is.⁷⁰⁸

A SAFE rendszer továbbfejlesztésére irányuló tervek a büntetés-végrehajtási szervezeteken kívüli előállításokat - mint bírósági, ügyészségi és egészségügyi előállításokat - is magukban foglalják. Az új modul célja, hogy a fogvatartottak előállítási folyamatát egy integrált, ellenőrzőpontokra épülő rendszer segítségével nyomon követhesse a kezdetektől az befejezésig, így javítva a folyamat átláthatóságát és hatékonyságát. Ezáltal a személyi állomány papírintésen, hatékonyabban tudja ellátni feladatait, teljes figyelmét az őrzési feladatra összpontosítva.⁷⁰⁹ ⁷¹⁰

⁷⁰⁵ Herke Csongor. (2023.) "Mesterséges intelligencia a büntetőjogi döntéshozatalban." *Jogtudományi Közlöny* 78, (4) pp. 165-176.

⁷⁰⁶ Ibid. p.165.

⁷⁰⁷ Büntetés-végrehajtási Szervezet Fogvatartotti Alap Nyilvántartás (a továbbiakban: FANY)

⁷⁰⁸ Hinkel Tamás. 2020. "A mesterséges intelligencia térhódítása a büntetés-végrehajtásban." *Börtönügyi Szemle*, (4),pp. 13-29.

⁷⁰⁹ Hinkel Tamás. (2020.)"A mesterséges intelligencia térhódítása a büntetés-végrehajtásban." p.16.

⁷¹⁰ Schmechl Gábor Dániel. (2020.) "SMART eszközök és egyedi alkalmazások a magyar büntetés-végrehajtásban." *Börtönügyi Szemle*, (4),pp. 49-69.

http://epa.niif.hu/02700/02705/00124/pdf/EPA02705_bortonugyi_szemle_2020_4.pdf

A Navigator rendszer a büntetés-végrehajtás legfejlettebb technológiai alapú adatbázisaként szolgál, amelynek fő célja a Büntetés-végrehajtás Országos Parancsnoksága és a bv. szervek ügyeleti munkájának támogatása. Az adatbázis egységesen és hatékonyan prezentálja a felhasználóknak a különböző adatforrásokból származó információkat. A rendszer, amely 2018-ban fejlesztések során a jelenlegi formáját nyerte el, dinamikusan fejlődik, jelenleg öt modullal rendelkezik. Kiemelkedő funkciója a "Jelenlévők keresése" felület, amely gyors hozzáférést biztosít a fogvatartottak adataihoz, ezáltal növelve a hatékonyságot rendkívüli események kezelésekor. A szállítások követése modul lehetővé teszi a fogvatartottak szállításának valós idejű nyomon követését GPS-segítséggel. Ezzel pontos helymeghatározás és esetleges problémák gyors észlelése lehetséges. A rendszer további funkciói közé tartozik az ülésrend rögzítése, kapcsolattartás a személyzettel, és riasztások küldése. Az E-naplók modul digitális nyilvántartást vezet a területről be- és kilépő személyekről és járművekről, növelve az adatok hozzáférhetőségét és elemzésének hatékonyságát.⁷¹¹ A 24 órás adatszolgáltatás modul egységesíti az adatrögzítést, megkönnyítve az adatszolgáltatást és a tovább jelentést.⁷¹²

A KIOSZK rendszer, egy büntetés-végrehajtási szakrendszer, lehetővé teszi a fogvatartottak számára, hogy jelentős részben saját maguk végezzék el az adatrögzítéseket és lekérdezéseket, ezzel csökkentve a személyi állomány adminisztratív terheit. A rendszer tesztelése pozitív visszajelzéseket kapott, és további tervek között szerepel a videotelefon szolgáltatás bevezetése és a biometrikus azonosítás integrálása.⁷¹³

A büntetés-végrehajtási MI alapú rendszerek, mint a SAFE, Navigator és KIOSZK, adatvédelmi kihívásokat vetnek fel, különösen a személyes adatok nagy mennyiségű kezelése és azok biztonsága kapcsán. Az adatgyűjtés és -kezelés során fontos az adatvédelmi szabályok szigorú betartása, különös figyelemmel a diszkrimináció elkerülésére és az érintettek jogainak védelmére. Az MI alapú rendszerek adatvédelmi problémái közé tartozik a személyes adatok bizalmas kezelése, az adatok szükségtelen gyűjtése és tárolása, valamint a diszkrimináció

⁷¹¹ Az "E-naplók" modul továbbfejlesztése során egy új online platformot vezetnek be, amely a tiltott tárgyak előkerülésének jelentését egyszerűsíti. E platform segítségével a jelentést tevők úrlapon keresztül, előre meghatározott válaszokat adva rögzíthetik az eseményeket, csökkentve ezzel a jelentéstétel időigényét. A rendszer automatizált kimutatásokat és táblázatokat generál a tiltott tárgyokról, elősegítve az elemző-értékelő munkát. Ez a fejlesztés javítani fogja az információáramlást és megkönnyíti az adatkezelést a büntetés-végrehajtási szervekben.

⁷¹² Hinkel Tamás. "A mesterséges intelligencia térhódítása a büntetés-végrehajtásban," pp. 17-20.

⁷¹³ Ibid., Hinkel Tamás p.20

lehetősége⁷¹⁴ az adatelemzés során.⁷¹⁵ Szükséges az adatminimalizálási elv betartása, a megfelelő jogalap megléte az adatkezelésre, és az adatbiztonsági intézkedések megerősítése. A rendszereknek tiszteletben kell tartaniuk az érintettek jogait, mint az adathoz való hozzáférés, helyesbítés, törlés, és az adatkezelés korlátozásának jogát. Az adatvédelmi szempontból kockázatos tevékenységek esetén előzetes adatvédelmi hatásvizsgálat szükséges. Eszteri mindezekon kívül kulcselemnek tartja a rendszer megismerhetőségét, azon belül is az alkalmazott logikáról való tájékoztatást tartja az egyik legfontosabbnak.⁷¹⁶

Az MI alkalmazása adatokra támaszkodik, melyek kezelésének adatvédelmi normáknak kell megfelelnie. Szükséges az adatok védelme az EU⁷¹⁷ és Magyarország jogszabályai szerint, biztosítva az adatok zavartalan áramlását. Adatkezeléskor csak hiteles, megbízható forrásból származó adatok használata javasolt, készen állva a nemzetközi bűnügyi vonatkozásokkal kapcsolatos MI-adatigénylések támogatására.⁷¹⁸

V. Az adatvédelem és a kiberbűnözés kapcsolata

„Mai világunk nagymértékben függ a különféle információs rendszerek megfelelő működésétől, az egyes államok léte és zavartalan működése pedig attól, hogy milyen mennyiségű, de legfőképpen milyen minőségű információval rendelkeznek.”⁷¹⁹

A gyors technológiai fejlődés és a hálózati infrastruktúrák expanziója következtében a kiberbűnözés, mint a számítástechnika negatív következménye, korunk egyik jelentős globális problémájává vált. A modern technológiai fejlesztések alkalmazásával az információs

⁷¹⁴ Mezei Kitti. (2022.) "Diszkrimináció az algoritmusok korában." *Magyar Jog*, (6), pp. 336-337.

⁷¹⁵ Eszteri Dániel, és Péterfalvi Attila. (2022.) "Amikor a gépeink tanulnak minket, avagy a mesterséges intelligencia alapú döntéshozatal és profilozás szabályozásának európai unió törekvéseiről." *Századvég* 2022, (1),p. 96.

⁷¹⁶ Ibid., p.118.

⁷¹⁷ A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Mesterséges intelligencia Európa számára.

⁷¹⁸ Nagy Zoltán András.(2021.) "Mesterséges intelligencia a bűnügyi munkában." In *Sokszínű Kar Konferencia III.: Absztraktfüzet*, szerk. Ürmösné Simon Gabriella és Kudar Mariann, 9. Budapest, Magyarország: Nemzeti Közszerzői Egyetem Rendészettudományi Kar.

⁷¹⁹ Gál István László. (2021.)"A minősített adattal visszaélés néhány kriminológiai problémaköre." In *Ünnepi tanulmányok a 75 éves Németh Zolt tiszteletére: Navigare necesse est*, szerk. Barabás Andrea Tünde és Christián László, 179. Budapest, Magyarország: Ludovika Egyetemi Kiadó.

technológia eszközein keresztül számos bűncselekmény megvalósítása válik lehetővé, így a kiberbiztonság a modern ember és társadalom számára elengedhetetlen alapkövetelménnyé vált.⁷²⁰ A digitális forradalom exponenciális növekedést eredményezett a technológiai fejlődésben. Ez a jelenség nem csak a technológia terén mutatkozott meg, hanem kihatással volt a számítástechnikai bűncselekményekre is.^{721,722,723,724,725}

A statisztikai adatok szerint a kibertámadások számának növekedése a világhálón tárolt adatok mennyiségével arányosan növekszik, 2025-re a világ 200 zettabájtnyi adatot fog tárolni.⁷²⁶

A kiberbűnözés becsült globális költségei a kiberbiztonsági piacon várhatóan 2023 és 2028 között folyamatosan növekedni fognak, összességében 5,7 billió dollárral, ami 69,94 százalékos emelkedést jelent. 2028-ban a kiberbűnözés becsült költsége várhatóan eléri a 13,82 billió dollárt, ezzel új rekordot állítva fel.⁷²⁷

1. A kiberbűnözés fogalma

A számítógépes bűnözés fogalmának meghatározása nem egységes, számos definiálása ismert a szakirodalomban, gyakran szinonimaként használják az informatikai bűnözéssel.⁷²⁸

⁷²⁰ Brown, A. (2020). "Enhancing Cybersecurity Through Data Protection Measures." *International Journal of Cybersecurity*, 12(4), 321-335.

⁷²¹ Dumitrescu, Mihaela-Sorina, & Marica, Mihaela-Emilia. (2019). "Cybercrime in the Digital Era." In Basic International Conference (Ed.), *New Trends in Sustainable Business and Consumption* (pp. 433-440). Bucharest: Editura ASE.

⁷²² Datareportal. (2019). "Digital 2019: Global Digital Overview." Retrieved from <https://datareportal.com/reports/digital-2019-global-digital-overview>.

⁷²³ Holt, Thomas J., and Bossler, Adam. (2015). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Edited by Richard Wortley. London: Routledge. <https://doi.org/10.4324/9781315775944>

⁷²⁴ Wall, David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.

⁷²⁵ Holt, Thomas J., Bossler, Adam M., and Seigfried-Spellar, Kathryn C. (2022). *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. London: Routledge.

⁷²⁶ Gáti, Balázs.(2023) "A gazdasági válság hatásai a személyes adatok védelmére és annak büntetőjogi aspektusaira." In *Válságok és büntetőjog: Fiatal büntetőjogászok első konferenciája*, szerkesztette Nagy, Melánia; Ripszám, Dóra, 67-92. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar

⁷²⁷ Statista. "Annual cost of cybercrime worldwide 2017-2028." 2023. <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>

⁷²⁸ Kiss, Tibor. "Kiberbűnözés." In *Alkalmazott Kriminológia*, szerkesztette Barabás A. Tünde, p.445.

A kiberbűnözést több szerző, mint Jonathan Clough⁷²⁹, Peter Grabosky⁷³⁰ és Susan W. Brenner,⁷³¹ gyűjtőfogalomként kezeli. Grabosky a kiberdeviancia kapcsán az "old wine in new bottles" kifejezést használta, jelezve, hogy a kibertérben megjelenő eltérő magatartásformák valójában hagyományos normasértések, csak más környezetben.⁷³² A magyar szakirodalomban számos szerző vizsgálta az informatikai bűnözés fogalmát, köztük Polt Péter, Pusztai László, Nagy Zoltán András.⁷³³ Később Parti Katalin és Kiss Tibor,⁷³⁴ Szathmáry Zoltán,⁷³⁵ valamint Szabó Imre⁷³⁶ is kifejtették saját értelmezéseiket, melyek összhangban vannak a nemzetközi szakirodalom definícióival.

Alapvetően kétféle értelemben használatos, egyrészt ezen értve a számítógéppel, mint eszközzel elkövetett cselekményeket⁷³⁷, másrészt azokat az informatikai bűncselekményeket, amelyeket az információs rendszer, a hálózatok, illetve adattartalom ellen követnek el.

A "tisza" kiberbűncselekmények (angolul: 'cyber-dependent crime' vagy 'computer-focused crime') olyan bűncselekmények, amelyek kizárólag vagy főként számítógépeken vagy azok hálózatain keresztül valósulnak meg. Ezek a bűncselekmények szorosan kapcsolódnak az információs technológiához, és különböző típusú adatokkal, rendszerekkel vagy hálózatokkal

„A kiberbűnözés létezése több mint két évtized óta ismert, azonban a jelenség precíz meghatározására irányuló törekvések csak az elmúlt tizenöt év során alakultak ki. Ez a folyamat a web 2.0 által teremtett szimmetrikus kommunikációs lehetőségeknek tulajdonítható, amelyeken keresztül a normasértő magatartásformák egyre szélesebb felhasználói köröket értek el, és fokozottabban váltak láthatóvá a globális hálózatokban”

⁷²⁹ Clough, J. (2015.) *Principles of Cybercrime*. Cambridge: Cambridge University Press, pp.10-11.

⁷³⁰ Grabosky, Peter. (2016.) *Cybercrime*. Oxford: Oxford University Press, pp. 8-9.

⁷³¹ Brenner, W. S. (2010.) *Cybercrime – Criminal Threats From Cyberspace*. Santa Barbara: Praeger, pp.39-47.

⁷³² Grabosky, Peter. (2001.) "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2: pp.243-249.

⁷³³ Sieber, U. (1993.) "A számítógépes bűnözés és más bűncselekmények az információtechnológia területén." *Magyar Jog*, no. 2: pp.105–109.

⁷³⁴ Parti K. és Kiss T. (2017.) "Az informatikai bűnözés." In *Kriminológia*, szerk. Borbíró A., Gönczöl K., Kerezsi K., és Lévay M., Budapest: Wolters Kluwer. pp.491–493.

⁷³⁵ Szathmáry, Zoltán. (2012.) "Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban." Doktori értekezés, Pécsi Tudományegyetem ÁJK Doktori Iskolája Informatikai és Kommunikációs Jog Program, Budapest, pp. 79–80.

⁷³⁶ Szabó I. (2008.) "Informatikai bűncselekmények." In *Az informatikai jog nagy kézikönyve*, szerk. Dósa I., Budapest: Complex pp.547.

⁷³⁷ Tóth Dávid és Nagy Zoltán András. (2015.) "Computer related economic crimes in Hungary." *Journal of Eastern-European Criminal Law*, no. 2: pp. 165-174.

kapcsolatosak. (IKT eszközök) Például a számítógépes adathalászat vagy a rosszindulatú kártevőkkel való fertőzés "tisztá" kibercselekményeknek számítanak.⁷³⁸

A kibercselekmények egy szűkebb kategóriáját alkotják azok az esetek, amikor a bűncselekmények kizárólagos eszközei a számítógépek, de a cselekmények céljai már nem feltétlenül kapcsolódnak az információs technológiához.⁷³⁹ Például a számítógépes csalás vagy az internetes zaklatás olyan bűncselekmények, amelyekben a számítógépet az elkövetők a cselekmények végrehajtásának eszközeként használják, de maguk a cselekmények nem kizárólagosan az IT-technológiához kötődnek. Ehhez kapcsolódik Ambrus István felosztása, amely a digitális bűncselekmények szorosabb és tágabb értelmű kategóriáit különbözteti meg. A „szűkebb” kategóriába tartoznak azok a deliktumok, amelyek kizárólag a virtuális térben, elektronikus formátumban vagy digitális eszközökön keresztül követhetők el, például az információs rendszerekkel, elektronikus fizetőeszközökkel vagy adatokkal kapcsolatos bűncselekmények. Ezzel szemben a tágabb kategória olyan bűncselekményeket foglal magában, amelyek eredetileg nem digitális környezetben is előfordulhatnak, de napjainkban egyre gyakrabban valósulnak meg a digitális világban, mint például a gyermekpornográfia, pénzmosás, zaklatás vagy közzététellel megvalósuló bűncselekmények.⁷⁴⁰

Fontos megjegyezni, hogy számos olyan bűncselekmény létezik, amelyeknél a számítógép vagy az internet csak részben vagy közvetetten vesz részt az elkövetésben. Ezeket a bűncselekményeket általában "számítógép segítségével elkövetett bűncselekményeknek" (angolul: 'cyber-enabled crime' vagy 'computer-assisted crime') nevezzük. Ez a kategória szélesebb skálát ölel fel, és magában foglalhatja például az online csalásokat, a digitális adatlopásokat vagy a számítógépes kártevők által okozott károkat.⁷⁴¹

A kibercsünyözés tehát új típusú bűncselekményeket foglal magában, speciális védett jogi tárgyakkal rendelkeznek, mint az információs rendszer vagy az adat. Emellett magában foglalja a hagyományos bűncselekményeket is, amelyek az új eszközök segítségével könnyebben

⁷³⁸ Mezei Kitti. (2019). "Szervezett bűnyözés az interneten." *A bűnygyi tudományok és az informatika*, 125. Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, p.125.

⁷³⁹ Knoop, Bert-Jaap. (2011). "The Internet and its Opportunities for Cybercrime." *Tilburg Law School Legal Studies Research Paper Series*, 9, p. 739.

⁷⁴⁰ Ambrus, István. *Digitalizáció és büntetőjog*. Budapest: Wolters Kluwer, 2021, p.290.

⁷⁴¹ Grund, Borbála. (2021). "A kibertér bűncselekményeiről és a kibercsünyözés hazai gyakorlatáról." *MTA LAW WORKING PAPERS*, 20212, 1-37.p.37

elkövethetők.⁷⁴² Adatvédelmi szempontból két kapcsolódási pont adódik: az egyik esetben a személyes adatok maguk képezik a bűncselekmény tárgyát, a másik szempont pedig azt vizsgálja, hogy a személyes adatok védelme milyen mértékben járul hozzá a kiberbűnözés elleni védelemhez.

2. A kiberbűncselekmények jellegzetességei

2.1 Hacking és adathalászszerű bűncselekmények

A hálózati kapcsolódás a termékek és szolgáltatások központi eleme lett, ami felveti a biztonság hagyományos koncepciójának újraértékelését. A hálózatokon keresztüli kapcsolódás közvetlen veszélyt jelenthet a termékek biztonságára, és indirekt veszélyeket is hordozhat, például az ún. „hackelhetőség⁷⁴³”, vagyis az integritás egy relatíve alacsony szintje révén, ami további kiberfenyegetéseket eredményezhet. Ezért a támadók gyakran az IoT-eszközök sebezhetőségeit célozzák meg, mint például a routereket, biztonsági kamerákat, okos televíziókat vagy egészségügyi eszközöket, amelyeket a támadások során használnak fel. A meghekkelhető IoT-eszközök segítségével a támadók érzékeny adatokat gyűjthetnek a felhasználókról. Az okosotthonok is hasonló veszélyeknek vannak kitéve, az autonóm járművek is potenciális célpontokká válhatnak a hackertámadások számára.⁷⁴⁴

A hacking-jellegű cselekmények mögötti motivációk között szerepel az információhoz való hozzáférés, az adat megváltoztatása vagy törlése, valamint az információs rendszer használata.

⁷⁴² Mezei, Kitti. (2019) "A kiberbűnözés szabályozási kihívásai a büntetőjogban." (Hozzáférés: 2023.02.11) https://real.mtak.hu/104974/1/Mezei_UL_201945.pdf, p. 22.

⁷⁴³ Furnell, S. (2010). "Hackers, viruses and malicious software." In *Handbook of Internet Crime*, edited by Y. Jewkes and M. Yar, Willan Publishing. pp. 43–45.

A számítógépbe történő jogosultalan belépés. A "hacker" fogalmát gyakran az informatikában magas szintű tudással rendelkező szakemberekre alkalmazzák. Megkülönböztetünk feketekalapos (black hat) hackereket, akik károkat okozhatnak vagy információkat lophatnak, szürkekalapos (grey hat) hackereket, akik jó szándékkal, de jogosultság nélkül kutatnak biztonsági részeket, és fehérkalapos (white hat) hackereket, akik hivatalos megbízás alapján tesztelik a rendszereket. Az etikus hackelés kifejezetten megbízásra történik, ahol a hacker jogosultsággal rendelkezik a tesztelésre.

⁷⁴⁴ Herke Csongor (2021). "A kiberbűnözés és a teljesen önvezető járművek." In *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est*, szerk. Barabás Andrea Tünde és Christián László, 211–221. Budapest, Magyarország: Ludovika Egyetemi Kiadó.

Az illetéktelen hozzáférés nem csak önmagában jelent veszélyt, hanem más bűntettek előkészítésére is alkalmazható, így például lehetőséget nyújthat az érintettek adatainak felhasználásával történő zsarolására vagy azok felhasználására. Az adatok megszerzését követően az elkövetők gyakran nem saját céljaikra használják fel ezeket, hanem tovább értékesítik azokat a Darknet fórumokon.^{745,746}

2.2. Online térben elkövetett zsarolás jellegű bűncselekmények

Az információs rendszerek felhasználásával történő zsarolás a hagyományos zsarolási módszerek modern változata, ahol az elkövetők az online térben fenyegetik meg a sértetteket. Gyakran előfordul, hogy az elkövetők jogosulatlanul behatolnak a sértett számítógépére, zsaroló szoftverek (ransomware)⁷⁴⁷ felhasználásával, és hozzáférnek bizalmas, személyes adatokhoz vagy üzleti titkokhoz. Ezeket az adatokat felhasználva, a zsarolók azzal fenyegetik a sértetteket, hogy az információkat nyilvánosságra hozzák vagy továbbítják, amennyiben nem teljesítik a követeléseiket.⁷⁴⁸

Újszerűbb zsarolási formának tekinthető a Darknet-fórumokon megszerzett adatbázisok felhasználása. Ezekben az esetekben az elkövetők személyes adatokat tartalmazó adatbázisokat használnak fel, például e-mail címeket, és az érintetteknek azt állítják, hogy kompromittáló kép- vagy videófelvételük van a birtokukban. Ezt követően fenyegetéssel próbálják kikényszeríteni a fizetést.

DDoS-támadásokat⁷⁴⁹ is felhasználnak zsarolási célokra, ahol az elkövetők a célpont weboldalának vagy hálózatának leállításával, vagy annak működésének megzavarásával

⁷⁴⁵ Bartlett, Jamie. (2014). *The Dark Net: Inside the Digital Underworld*. London: Heinemann p.303

⁷⁴⁶ Mezei Kitti. (2020). "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre." *Állam- és Jogtudomány* 61,(4), p.70.

⁷⁴⁷ Bart Custers, Jan-Jaap Oerlemans, és Ronald Pool. (2020). "Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies." *European Journal of Crime, Criminal Law and Criminal Justice*: pp.121–152.

⁷⁴⁸ McGuire, M., and Dowling, S. (2013). Cyber-dependent crimes. In *Cyber crime: A review of the evidence* (Research Report 75, Chapter 1). Law, Computer Science.

⁷⁴⁹ Council of Europe. (2001). *Explanatory Report to the Convention on Cybercrime*. European Treaty Series – No. 185, p. 12. Accessed March 5, 2021. <https://rm.coe.int/16800cce5b>.

fenyegetnek. Ezek a támadások különösen veszélyesek lehetnek, hiszen jelentős anyagi és reputációs károkat okozhatnak a cégeknek vagy szervezeteknek.⁷⁵⁰

Ezek a modern zsarolási módszerek rávilágítanak az információs rendszerek és az online adatok védelmének fontosságára.

2.3 Jogsabályi háttér⁷⁵¹

A kibercbűncselekmények elleni küzdelem érdekében számos jogi kezdeményezés született, az Európai Unióban 2001-ben jött létre az együttműködésről szóló egyik legátfogóbb szabályozás, a Számítástechnikai Bűnözésről Szóló Egyezmény – Budapesti Egyezmény (Budapest Convention)⁷⁵², amely 2004-ben lépett hatályba. Ez volt első nemzetközi szerződés, amely kifejezetten a számítógépes bűnözésre összpontosított.⁷⁵³ Ide sorolhatók továbbá a számítástechnikai bűnözés elleni küzdelem területén a nemzetközi együttműködésekkel kapcsolatos kezdeményezések – az ENSZ, az OECD, az Európai Unió és a G8-ak által – és az

⁷⁵⁰ Nagy Zoltán András. (2009.) *Bűncselekmények számítógépes környezetben*. Budapest: Ad Librum, p.115.

A DDoS-támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében (pl. e-mail, banki vagy egyéb fiókokhoz való hozzáféréshez, vagy a weboldal elérésében).

⁷⁵¹ Gáti Balázs.(2021) "Az adatvédelem számítástechnikai bűnözéssel összefüggő aktuális kérdései - Adatvédelmi kérdések a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv Tervezetével kapcsolatban." In: Köhalmi, László (szerk.) PhD Tanulmányok 15. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola pp.23-58.

⁷⁵² Council of Europe. 2001. "Convention on Cybercrime." *European Treaty Series – No. 185*. <https://rm.coe.int/1680081561>.

⁷⁵³A 185. szerződés aláírása és megerősítése, A számítógépes bűnözésről szóló egyezmény

Állapot: 20.05.05, Szerződés Hivatala, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>

ehhez kapcsolódó egyezmények, illetve ajánlások.^{754,755,756,757,758} Az első fontos nemzetközi jogi dokumentum a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) által kibocsátott 1986-os jelentés volt.^{759,760} A következő fontos dokumentum az Európa Tanács 1989-es ajánlása,⁷⁶¹ az Európa Tanács 1995-ben adott ki egy újabb ajánlást, amely többek között az információs technológiával kapcsolatos büntető eljárásjogi problémákat gyűjtötte egybe.⁷⁶²

2005-ben került elfogadásra az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat.⁷⁶³ A kerethatározat büntetőjogi intézkedéseket, szankciókat és információcserére vonatkozó eljárásokat is tartalmaz.

⁷⁵⁴ Recommendation No. R (85) 10 to Member States Concerning the Practical Application of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the Interception of Telecommunications. <https://rm.coe.int/09000016804e6b5e>. [01.06.2019].

⁷⁵⁵ Recommendations and Declarations in the field of media and information society. In *Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society*, 30-33. <https://rm.coe.int/1680645b44>. [01.06.2019].

⁷⁵⁶ Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector. <https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal>. Accessed [01.06.2019].

⁷⁵⁷ Recommendation No. R (95) 4 to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e>. Accessed [01.06.2019].

⁷⁵⁸ Recommendation No. R (95) 13 to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>. Accessed [01.06.2019].

⁷⁵⁹ Gyarakai Réka. (2012). "A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN-kód megadása sikeres vagy biztonságos az internet?!" *Pécsi Határőr Tudományos Közlemények* XIII:pp. 237–238.

⁷⁶⁰ Mezei Kitti. (2018) "Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására." *JURA* 24, no. 1, pp. 349–360.

⁷⁶¹ Recommendation No. R (89) 9 to Member States on Computer-Related Crime., Accessed June 1, 2019. <https://rm.coe.int/09000016804f1094>.

⁷⁶² Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology. <https://rm.coe.int/16804f6e76>. Accessed [01.06.2019].

⁷⁶³ A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról." *Hivatalos Lap* L 69/67,

Fontos megemlíteni a 460/2004/EK európai parlamenti és tanácsi rendeletet, amely megalkotta az Európai Hálózat és Információbiztonsági Ügynökséget (European Union Agency for Cybersecurity- ENISA).⁷⁶⁴

2013 augusztusában az Európai Parlament és Tanács elfogadta a 2013/40/EU irányelvet az információs rendszerek elleni támadásokról, amely egyúttal felváltotta a 2005/222/IB tanácsi kerethatározatot.^{765,766}

Az (EU) 2016/1148 irányelv (Network and Information Systems ,NIS)⁷⁶⁷ mint a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv 2016-ban került elfogadásra. Ez az irányelv a belső piac működésének javítása érdekében intézkedéseket állapít meg a hálózati és információs rendszerek egységesen magas szintű biztonságának az Unión belüli megvalósítása céljából.⁷⁶⁸

Az Európa Tanács 2017-ben bízta meg az Egyezmény Bizottságát a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv⁷⁶⁹ tervezetének megalkotására, elsősorban az elektronikus bizonyítékok, a számítógépen tárolt adatok büntetőeljárás során történő hozzáféréseivel kapcsolatosan. A Második Kiegészítő Jegyzőkönyv (ETS No. 185) a domain névvel kapcsolatos regisztrációs információk közzétételét engedélyezi, továbbá elősegíti a szolgáltatókkal való közvetlen együttműködést az előfizetőkkel kapcsolatos adatok hatékony begyűjtése érdekében. Ez magában foglalja az előfizetői információk, forgalmi adatok beszerzését, az azonnali együttműködést sürgősségi helyzetekben, kölcsönös segítségnyújtást, valamint a személyes adatok védelmének biztosítására vonatkozó biztonsági intézkedések meghatározását.

⁷⁶⁴ 460/2004/EK Rendelet , Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. *Hivatalos Lap* L 77 (13 március 2004).

⁷⁶⁵ 2013/40/EU Irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

⁷⁶⁶ Nagy Zoltán András.(2020) "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor, Budapest: Dialóg Campus. p.49.

⁷⁶⁷ Irányelv (EU) 2016/1148 a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. *Hivatalos Lap* L 194/1 (19 augusztus 2016).

⁷⁶⁸ (EU) 2016/1148 1. cikk (1)

⁷⁶⁹"A Számítástechnikai Bűnözésről szóló Egyezményhez csatolt második kiegészítő jegyzőkönyv a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról." *Hivatalos Lap* L 63 (28 február 2023): 28–47.

A 2016-ban bevezetett uniós kiberbiztonsági szabályokat a 2023-ban hatályba lépett (EU) 2022/2555 irányelv (NIS2) módosította.⁷⁷⁰ Az irányelv jogi keretet hozott létre az Unióban a kiberbiztonsági képességek növelésére, mint például a tagállamok készenléti szintjének növelése céljából tett kötelezettségvállalások. Ezek biztosítják, hogy a nemzetek megfelelő technológiai eszközökkel és képességekkel rendelkezzenek, beleértve a számítógépes biztonsági eseményekre reagáló csoportokat (Computer Security Incident Response Team, CSIRT) és a nemzeti hálózati és információs rendszerekkel (NIS) foglalkozó illetékes hatóságokat. A NIS 2 irányelv kiemelten foglalkozik az információmegosztással és a tagállamok közötti együttműködéssel, létrehozva egy koordinációs csoportot, amely segíti a tagállamokat a kiberbiztonsági események kezelésében. Az irányelv célja továbbá az, hogy harmonizálja a kiberbiztonsági előírásokat az EU egészében, így biztosítva a belső piac zavartalan működését és az állampolgárok magas szintű védelmét a kiberfenyegetésekkel szemben.

3. Személyes adatok - mint a kiberbűncselekmények elkövetési tárgyai

Az Európai Parlament és Tanács 2013/40/EU irányelve⁷⁷¹, amely az információs rendszerek elleni támadásokkal foglalkozik elsőként hívta fel a figyelmet arra, hogy a kiberbűnözés elleni integrált megközelítés fontos eleme a személyazonosság-lopás és a személyazonossághoz kapcsolódó bűncselekmények elleni hatékony fellépés, mivel a felhasználók gyakran nincsenek tudatában az online kockázatokkal, és az ilyen módon megosztott információk és képek veszélyeivel.⁷⁷² Ennek eredményeként az illetéktelen személyek egyre könnyebben szerezhetik meg a személyes adatokat, például malware, phishing és egyéb módszerek segítségével.

⁷⁷⁰ Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union* L 333 (2022): 80–152.

NIS 2 irányelv preambulum (3) : a „ hálózati és információs rendszerek a mindennapi élet központi jellemzőjévé fejlődtek a társadalom gyors digitális átalakulásával és összekapcsolódásával, beleértve a határokon átnyúló információmegosztást is. Ez a fejlődés a kiberfenyegetettség bővüléséhez vezetett, új kihívások támasztásával, amelyek minden tagállamban kiigazított, összehangolt és innovatív reagálást igényelnek. Az események száma, nagysága, kifinomultsága, gyakorisága és hatása növekszik, és komoly veszélyt jelentenek a hálózati és információs rendszerek működésére.(...)”

⁷⁷¹ Irányelv 2013/40/EU az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról." *Hivatalos Lap* L 218 (2013) pp.8-14.

⁷⁷² *Ibid.*, (EU) 2013/40/, Preambulum (14)

A jelentős érdeksérelemmel járó személyes adatokkal való visszaélés elkövetője nem korlátozódik kizárólag az adatvédelmi jogszabályok alapján definiált adatkezelőkre, hanem bárki lehet, aki a személyes adatokat jogosulatlanul használja fel.⁷⁷³ Ezzel összhangban a NAIH felhívja a figyelmet arra, hogy különös gyanút keltenek azok az esetek, ahol ismeretlen személyek közösségi oldalakon hamis profilokat hoznak létre, felhasználva valódi felhasználók nevét és fényképeit.⁷⁷⁴ Ezeken a profilokon keresztül az elkövetők gyakran hamis bejegyzéseket és üzeneteket tesznek közzé az érintett nevében, amelyek célja a sértett hírnevének rontása, és ez jelentős érdeksérelemmel járhat. Ezenkívül felmerül a lehetősége annak is, hogy mások személyes adatait felhasználják további bűncselekmények elkövetéséhez. Az IoT-eszközökkel kapcsolatos veszélyek szintén nem elhanyagolandók, mivel az ilyen rendszerek gyakran személyhez köthető adatokat tartalmaznak, amelyek a magánszférát is érinthetik. Ha ezek az adatok összekapcsolhatók az érintett személyekkel, akkor azok személyes adatként kezelhetők. Az IoT-rendszerben résztvevő számos szereplő, például gyártók, alkalmazásfejlesztők, adatfeldolgozók és adatelemzők miatt az adatok útja az adatalany számára gyakran követhetetlen lehet. Minél több eszköz kapcsolódik a hálózatba, annál több adat gyűjthető az egyes személyekről, ami alapján részletes személyiségprofilok is készülhetnek.⁷⁷⁵

Klasszikusnak mondható a személyes adatokat ért támadás tekintetében az identitáslopás jelensége.

3.1. A Bűnügyi Adatvédelmi Irányelv és a GDPR lehetséges hatásai a személyes adatok védelmére a kiberbűnözés vonatkozásában

Az adatvédelmi szabályozások, mint a GDPR, és a LED jelentős preventív hatást gyakorolnak, melyeket zsinórmértékként, azaz mérvadó standardként kezelünk. Az adatvédelmi törvények alapvetően nem a kiberbűnözés elleni küzdelem hatására jöttek létre, kialakulásuk és fejlődésük részben a technológiai forradalomnak köszönhető, azonban az általuk meghatározott „aktuális

⁷⁷³ 1/2012. számú BJE-határozat. Idézi: Mezei Kitti "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre"

⁷⁷⁴ Péterfalvi Attila és Eszteri Dániel.(2017). "A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata." In *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*, szerk. Görög Márta, Menyhárd Attila és Koltay András, Budapest: ELTE-ÁJK p.409.

⁷⁷⁵ Ibid., p. 411.

legjobb gyakorlatok” és szabályozások is hozzájárulnak az adatvédelmi normák megerősítéséhez, ezzel a kiberbűnözés csökkentéséhez, mivel meghatározott keret biztosítanak az adatok kezelésére és védelmére.^{776,777}

A GDPR és LED szabályozásai, melyek a személyes adatok védelmét hivatottak biztosítani, alapvetően hozzájárulnak a kiberbiztonsághoz. Az adatbiztonság és kiberbiztonság összekapcsolódva egy erős védelmi vonalat képeznek a kiberfenyegetésekkel szemben.⁷⁷⁸

Bederna hangsúlyozza, hogy az általános adatvédelmi rendelet elősegíti az információbiztonság iránti elkötelezettséget és a tudatos megvalósítás szükségességét. Az adatkezelési elvek és az érintett személyek jogainak betartása érdekében előírt szervezési és technikai intézkedések konkrétan átültethetők az információbiztonság különböző aspektusaira, mint az adminisztratív, fizikai és logikai kontrollokra, amelyek a bizalmasság, sértetlenség és rendelkezésre állás biztosítását célozzák. Az anonimizálás, titkosítás és hozzáférés-szabályozás kötelező jellegű intézkedéseket jelent, és szigorú követelményeket támaszt az incidenskezelés és a változásmenedzsment tekintetében. A változások kezelésére vonatkozó követelmények közé tartozik a „beépített adatvédelem” elvének alkalmazása és az adatvédelmi hatásvizsgálat elvégzése, amennyiben a meghatározott feltételek teljesülnek.⁷⁷⁹

Az új adatvédelmi reformot jelentő szabályozások kezdetinél, már 2012-ben felmerült a az adatvédelmi elvek szerepe a kiberbűnözés elleni küzdelemben. Porcedda a kiberbűncselekmények szűkebb és tágabb értelmezései alapján (lsd. fogalmi meghatározások) a kiberbiztonság hatáskörébe tartozónak a szűkebb értelemben vett bűncselekményeket tartja (a csak online elkövethető bűncselekmények). Azt állítja, hogy az adatvédelmi elveknek a kiberbiztonsági szabályozásba való beépítése a kiberfenyegetések, és különösen a (szűk értelemben vett) kiberbűnözés csökkentésének eszközeként működhet.⁷⁸⁰

⁷⁷⁶ Moore, T. and Anderson, R. (2019). "Rethinking Information Security to Improve Data Privacy," *European Journal of Information Systems*, 28(5), pp.687-694.

⁷⁷⁷ European Union Agency for Cybersecurity (ENISA). (2020). *Threat Landscape for Cybersecurity in the Context of GDPR*. European Union Agency for Cybersecurity.

⁷⁷⁸ Schreiber, T. (2021). *Data Protection and Cybersecurity Law*. Oxford: Oxford University Press.

⁷⁷⁹ Bederna, Zsolt.(2018) "Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai." *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata* 16, (3) 76-103.p.94

⁷⁸⁰ Porcedda, Maria Grazia. (2012). "Data Protection and the Prevention of Cybercrime - The EU as an Area of Security?" *EUI Working Papers LAW*, No. 2012/25, <https://ssrn.com/abstract=2169340> or <http://dx.doi.org/10.2139/ssrn.2169340>.

Wicki–Birchler a Budapesti Egyezmény II. kiegészítő jegyzőkönyve és a GDPR kapcsán azt vizsgálja, hogy a két szabályozás között fennáll-e összefüggés a kiberbűnözés visszaszorítását célzó törekvések tekintetében.⁷⁸¹

Elemzése szerint a Budapesti Egyezmény és a GDPR közötti a legfontosabb kapcsolódási pont az, hogy a számítógépes bűnözés jellemzően az adatokkal való visszaélés révén történik.

A Budapesti Egyezmény II. Fejezet 2. cikke kimondja, hogy minden szerződő fél köteles jogalkotási és egyéb intézkedéseket megtenni annak érdekében, hogy jogszabályaival összhangban bűncselekménynek minősüljön a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan és szándékos belépés. Ez az elv összhangban áll a GDPR 39. és 40. cikkében foglaltakkal, amelyek a személyes adatok megfelelő biztonságának és bizalmas kezelésének biztosítását írják elő, hogy megakadályozzák a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést.

Az Egyezmény II. Fejezet 3. cikke szerint minden szerződő fél köteles intézkedéseket hozni a számítástechnikai rendszeren belüli, abból származó vagy abba irányuló számítástechnikai adatok nem nyilvános továbbítása során történő jogosulatlan és szándékos kifürkészésének bűncselekménnyé nyilvánításához. Ez a rendelkezés párhuzamba állítható a GDPR 5. cikk (f) pontjával, amely előírja a személyes adatok megfelelő védelmét, beleértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet.

A GDPR 48. cikkében foglaltak, amelyek szerint a harmadik országok bíróságainak vagy közigazgatási hatóságainak döntései, amelyek személyes adatok továbbítását vagy közlését írják elő, csak akkor ismerhetők el vagy hajthatók végre, ha azok egy érvényes nemzetközi megállapodáson alapulnak, szintén összhangban vannak a Budapesti Egyezmény kölcsönös jogsegélyre vonatkozó rendelkezéseivel. A GDPR elveinek alkalmazása ebben a kontextusban kulcsfontosságú szerepet játszott az Európai Adatvédelmi Testület által a második kiegészítő Egyezmény kapcsán végzett véleményezések során.

2020-ban az Egyesült Királyságban készült összefoglaló tanulmány is vizsgálta hogy az általános adatvédelmi rendelet bevezetése milyen hatással volt a szervezetekre kiberbiztonsági

Feltéve, ha előnyben részesítik a technikai számítógépes biztonság fogalmát, (privilege a technical computer security notion), frissítik az adatvédelmi jogszabályokat (különösen a személyes adatok meghatározását) és az emberi jogokat core- periférikus modellben értelmezzük (Alekszij jogelméleti megközelítés)

⁷⁸¹ Wicki-Birchler, David. (2020) "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?" *International Cybersecurity Law Review* 1 63-72. <https://doi.org/10.1365/s43439-020-00012-5>.

eredményeiket illetően.⁷⁸² A felmérés összefüggés keresett a NIS irányelvvel is. Megállapították, hogy a GDPR hatására a szervezetek jelentősen javították kiberbiztonsági rendszereiken, különösen az irányítási struktúrák, a kockázatkezelési folyamatok, az adatvédelem és a rendszerbiztonság területén. A NIS irányelv alapján a legtöbb szervezet kiemelt prioritásként kezelte a kiberbiztonságot, növelte a területre fordított kiadásokat, és bevezetett új, illetve továbbfejlesztett adatvédelmi és kiberbiztonsági folyamatokat és technikai ellenőrzéseket, beleértve a személyes adatok és azokat kezelő rendszerek védelmére irányuló intézkedéseket a kibertámadások ellen.

Hirvonen tanulmánya is ezt kérdést vizsgálta, megállapításai szerint a GDPR a felhasználói profilozás és adatgyűjtés, az üzleti hatások, a menedzsment és megfelelés, a személyes kompetenciák, készségek és karrier, a hitelesítés, a jogosultsági ellenőrzés és az értesítési kötelezettség, valamint az adattárolás területén bár kihívásokkal járt, de növelte az információbiztonsági és adatvédelmi követelményeket.⁷⁸³

Az adatvédelmi szabályozás szerepét a kiberbiztonság területén az alábbiakban összegezzük:

- Proaktív védelem: A GDPR előírja az adatvédelmi intézkedések beépítését az információs rendszerek tervezési fázisában (beépített adatvédelem elve) valamint az adatvédelmi intézkedések folyamatos fenntartását az adatok kezelésének egész folyamata során.⁷⁸⁴ Ez magában foglalja a titkosítást, a hozzáférés-szabályozást, az adatok integritásának és biztonságának fenntartását. Ezek az intézkedések jelentősen csökkenthetik a kiberbűnözők által kihasználható kockázatokat, például jogosulatlan hozzáférést adatainkhoz, vagy az adatlopást.
- Adatkezelési elvek: A GDPR és a LED az adatminimalizálás elvét⁷⁸⁵ is előírja, amely szerint csak a feltétlenül szükséges adatok gyűjthetők és tárolhatók, és csak meghatározott, világos és jogszerű célokra. Ez az elv csökkenti a kiberbűnözők számára elérhető érzékeny információk mennyiségét, ezzel minimalizálva az adatokkal visszaélés kockázatát.

⁷⁸² RSM, „Impact of the GDPR on Cyber Security Outcomes Final Report” ,August 2020, https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf

⁷⁸³ Hirvonen, P. (2022). "A Review of GDPR Impacts on Information Security." In *PACIS 2022: Proceedings of the 26th Pacific Asia Conference on Information Systems*, AI-IS-ASIA: Artificial Intelligence, Information Systems, in Pacific Asia, Article 83.

⁷⁸⁴ (EU) 2016/679, Preambulum (8), 47. cikk d)

⁷⁸⁵ (EU) 2016/679, 5.cikk c)

- **Adatvédelmi hatásvizsgálat:** A GDPR előírja az adatvédelmi hatásvizsgálat elvégzését magas kockázatot jelentő adatkezelési műveletek esetén, mint például nagy mennyiségű személyes adat feldolgozása vagy különösen érzékeny adatok kezelése.⁷⁸⁶ Ez lehetővé teszi az adatkezelési tevékenységek kockázatainak azonosítását és kezelését, így proaktív védelmet nyújthat a kiberfenyegetésekkel szemben.
- **Hozzáférés-vezérlés és felhasználói jogosultságok:** Mind a GDPR, mind a LED szigorú követelményeket állapít meg a személyes adatokhoz való hozzáférés kezelésére.⁷⁸⁷ A szervezeteknek gondosan kell szabályozniuk, hogy ki férhet hozzá az adatokhoz, ezzel csökkentve a jogosulatlan hozzáférés kockázatát.
- **Incidenskezelés és értesítés:** A GDPR kötelezővé teszi az adatvédelmi incidensek, például adatsértések nyilvánosságra hozatalát és jelentését az illetékes hatóságoknak, valamint érintett egyének értesítését, ha az incidens valószínűleg magas kockázatot jelent az érintettek jogaira és szabadságaira.⁷⁸⁸ Ez hatással lehet a kibertámadások okozta károk enyhítésére.

3.2. Az (EU) 2022/2555 Irányelve (NIS 2) és az adatvédelem kapcsolódási pontjai

Az Európai Unió Általános Adatvédelmi Rendelete, amely 2018 óta van érvényben, a személyes adatok védelmére összpontosít, célja a felhasználói adatok védelmének előmozdítása. Ezzel ellentétben a NIS 2 irányelv, és annak nemzeti jogszabályokba való implementálása – mint a 2023. évi XXIII. törvény⁷⁸⁹ és a 10/2023. (V. 15.) SZTFH rendelet –, az egyes kritikus infrastruktúrákhoz tartozó vállalkozások és szervezetek általános információbiztonságát hivatott megreformálni, új standardok bevezetésével az egész digitális infrastruktúrára kiterjedően.

A GDPR és a NIS irányelvet hasonlította össze Cole és Schmitz. Megállapításaik szerint a kettőt kölcsönhatásban kell értelmezni, a NIS Irányelvet a GDPR kiegészítő jogszabályként lehet tekinteni, amely megfelelő biztonsági kötelezettségeket és új bejelentési kötelezettségeket vezet

⁷⁸⁶ (EU) 2016/679, 35.cikk

⁷⁸⁷ (EU) 2016/679, Preambulum (73), 15.cikk

⁷⁸⁸ (EU) 2016/679, Preambulum (49),(85) – (88), 33.cikk

⁷⁸⁹ 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

be bizonyos iparágakban és digitális szolgáltatásnyújtók számára.⁷⁹⁰A tanulmány egyúttal az átfedésekből adódó problémákat is jelzi, ilyen például az incidens bejelentési kötelezettség.

Bár elméletben megkülönböztethetőek azok az incidensek, amelyek a GDPR vagy a NIS-irányelv hatálya alá esnek, a gyakorlatban a legtöbb biztonsági incidens személyes adatokat érint. Ez azt jelenti, hogy a távközlési szolgáltatóknak és a digitális szolgáltatásnyújtóknak (DSP-knek) mindkét illetékes hatóságnak jelentést kell tenniük ezekről az incidensekről. Mivel a DSP-k gyakran adatfeldolgozóként működnek, konfliktusok és zavarok alakulhatnak ki az illetékes hatóságok között, különösen akkor, ha ugyanazt az incidenst különböző szervezetek különböző hatóságoknak jelentik be, például az adatvédelmi hatóságnak és a hálózat- és információbiztonsági hatóságnak.⁷⁹¹

A GDPR alapján kezelt személyes adatok védelme mellett, a NIS 2 irányelv tehát speciális adatvédelmi követelményeket is meghatároz, összhangban a GDPR-ral. A NIS 2 hatálya alá tartozó vállalatoknak és szervezeteknek a GDPR által előírt adatvédelmi elvárásokon túl, a NIS 2-t átültető jogszabályoknak megfelelően is biztosítaniuk kell az adatok biztonságát.

Ez magában foglal néhány olyan előírást is, ahol az adatvédelmi és kiberbiztonsági követelmények átfedik és kapcsolódnak egymáshoz, melyek az alábbiakban foglalhatók össze:

- Biztonsági intézkedések, adatvédelmi szabályzatok: A GDPR elvárja a kockázat mértékének megfelelő szintű adatbiztonságot garantáló technikai és szervezési intézkedések végrehajtását mind az adatkezelőktől, mind pedig az adatfeldolgozóktól. Ilyen például az adatok álnevesítése, titkosítása, a rendszerek bizalmas jellegének, integritásának és rendelkezésre állásának folyamatos biztosítása, incidenskezelés, valamint az intézkedések rendszeres tesztelése és felülvizsgálata. Ezzel szemben a NIS 2, amely a digitális infrastruktúra biztonságára összpontosít, specifikusabb biztonsági intézkedéseket és kontrollokat ír elő az adatkezelők számára. Ezáltal a NIS 2 hatálya alá tartozó szervezeteknek meg kell felelniük mind a GDPR által támasztott elvárásoknak, mind a NIS 2 által előírt specifikus biztonsági követelményeknek,⁷⁹² amelyek együttesen erősítik az adatvédelmi és kiberbiztonsági keretet.

⁷⁹⁰ Cole, Mark D. and Schmitz, Sandra. "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape." *University of Luxembourg Law Working Paper No. 2019-017* (December 31, 2019). Elérhető at SSRN: <https://ssrn.com/abstract=3512093> or <http://dx.doi.org/10.2139/ssrn.3512093>.

⁷⁹¹ Ibid.,17.p

⁷⁹² A NIS 2 előírásai magukban foglalják az információs rendszerek és adatok biztonsági besorolását, információbiztonsági szabályzatok kialakítását, eseménykezelést, ellátási lánc biztonságának garantálását,

- Auditok, ellenőrzések: A GDPR már eddig is szorgalmazta az adatkezelés biztonságának biztosítására vonatkozó technikai és szervezési intézkedések rendszeres ellenőrzését, míg a NIS 2 törvény előírja a felügyeleti hatóság által végzett ellenőrzéseket, valamint a vállalatok és szervezetek számára kétévente kötelező, független auditor általi auditokat. Ez arra ösztönzi a vállalatokat és szervezeteket, hogy felülvizsgálják jelenlegi szabályzataikat és eljárásaikat annak érdekében, hogy megfeleljenek mind a kiberbiztonsági hatóság ellenőrzései, mind az NIS 2 követelményeknek megfelelő auditoknak.⁷⁹³
- Incidensek: A GDPR és a NIS 2 egyaránt fontos szerepet játszik a kiberbiztonsági és adatvédelmi incidensek kezelésében. Míg a GDPR főként a személyes adatok védelmére összpontosít, addig a NIS 2 a kiberbiztonsági intézkedések megerősítését célozza meg. Az incidensek bejelentési kötelezettsége továbbra is érvényben van mindkét szabályozás alapján, de a NIS 2 esetében szigorúbb határidők vonatkoznak a bejelentésekre.⁷⁹⁴
- Adatfeldolgozói szerződések: a GDPR előírja az adatkezelők számára, hogy csak olyan adatfeldolgozókat alkalmazzanak, amelyek megfelelnek a rendelet által megkövetelt biztonsági garanciáknak. E szerződéseknek tartalmazniuk kell a GDPR által előírt tartalmi elemeket. A NIS 2 irányelv e követelményeket kiterjeszti, meghatározva, hogy a releváns szervezeteknek értékelniük kell digitális infrastruktúrájuk beszállítóinak kockázatait. A nemzeti implementációk követelményei szerint az elektronikus információs rendszerek üzemeltetésében részt vevőknek is meg kell felelniük ezeknek az előírásoknak.⁷⁹⁵
- Adatkezelési tájékoztatók: a GDPR átláthatóságot és tájékoztatást követel meg a személyes adatok kezelésében. A NIS 2 implementációja új kiberbiztonsági követelményeket vezet be, amelyek befolyásolják a szervezetek adatkezelési tájékoztatóit.
- A NIS 2 irányelv bevezetése kiterjeszti a kiberbiztonsági szabályok alkalmazási körét, amelyek közvetlenül befolyásolják a szervezetek által kezelt személyes adatokat. Az

kötelező kiberbiztonsági képzést, titkosítási eljárásokat, hozzáférés-ellenőrzési szabályokat, és hitelesítési megoldásokat. Továbbá meghatározza a szervezeti vezetés felelősségét, előírja a biztonságért felelős személy kinevezését, erősítve ezzel az adatvédelmi és információbiztonsági keretet.

⁷⁹³ (EU) 2022/2555 ,32. cikk (2) b)

⁷⁹⁴ EU) 2022/2555 ,Preambulum (102)

⁷⁹⁵ EU) 2022/2555, Preambulum (85)

irányelv előírja, hogy a szervezeteknek bizonyos körülmények között meg kell osztaniuk személyes adatokat a hatóságokkal, például kiberbiztonsági incidenst érintő jelentéstétel során. Emellett az irányelv szigorú követelményeket állít fel a szervezetek adatkezelési gyakorlataira vonatkozóan, különös tekintettel az adatbiztonsági intézkedésekre és az adatkezelés jogaire.⁷⁹⁶

Összefoglalva, a bűnüldözési irányelv és az általános adatvédelmi rendelet az Európai Unió két alapvető adatkezelésekre vonatkozó jogszabálya, amelyek az adatvédelem és az adatbiztonság területén hivatottak szabályozni az adatkezelési gyakorlatokat.

A GDPR az adatkezelés alapelveire összpontosít, úgy, mint az adatminőség, az átláthatóság, az adatkezelés korlátozása, az adatbiztonság, és az elszámoltathatóság.⁷⁹⁷ Ezek az alapelvek különösen fontosak a kiberbűnözés kontextusában, mivel az adatvédelmi intézkedések és az adatbiztonsági protokollok,⁷⁹⁸ a beépített adatvédelem elve közvetlenül befolyásolják a személyes adatokhoz történő jogosulatlan hozzáférés vagy azok illetéktelen felhasználásának kockázatát. A LED meghatározza, hogy a hatóságok miként gyűjthetnek, tárolhatnak és továbbíthatnak adatokat a bűnözés megelőzése, nyomozása, felderítése vagy üldözése érdekében. A NIS 2 irányelvvel összhangban kialakuló új kibervédelmi és adatvédelmi előírások jelentős változásokat hoznak a szervezetek incidenskezelési folyamataiban. Az irányelv alapján a kiberbiztonsáért felelős hatóságok jogosultak arra, hogy kibervédelmi incidens esetén az érintett szervezetek szolgáltatásait igénybe vevő személyeket tájékoztassák az őket érintő potenciális kibervédelmi fenyegetésekről, valamint az ilyen fenyegetések kezeléséhez szükséges intézkedésekről. Ha a kibervédelmi incidens egyben adatvédelmi incidensnek is minősül, az érintett szervezeteknek lehetőségük van saját kezdeményezésükre tájékoztatni az érintett személyeket az incidensről és annak lehetséges következményeiről, valamint a nemzeti felügyelő hatóság (NAIH) is elrendelheti a GDPR előírásainak megfelelő tájékoztatást. Az új szabályozások alkalmazása érdekében a szervezeteknek felül kell vizsgálniuk meglévő adatbiztonsági és incidenskezelési eljárásaikat, szabályzataikat annak érdekében, hogy megfeleljenek az új kibervédelmi és adatvédelmi követelményeknek. Ez magában foglalja az érintett személyek tájékoztatási folyamatának pontosítását, az adatvédelmi

⁷⁹⁶ (EU) 2022/2555, Preambulum (51)

⁷⁹⁷ (EU) 2016/679 5. cikk

⁷⁹⁸ EU) 2016/679 25. cikk (2)

és kiberbiztonsági incidensek kezelésére vonatkozó eljárások integrálását, valamint a kiberbiztonsági és adatvédelmi intézkedések hatékonyságának folyamatos értékelését.

3.3. A személyiséglopás jelensége

Az identitáslopás mint jelenség a kiberbűncselekmények kategóriájába tartozik, különleges azonban abból a szempontból, hogy elkövetési módjai révén egyrészt az információs rendszer elleni bűncselekményekhez kapcsolódik, másrészt megvalósítja elsősorban a személyes adattal való visszaélés büntetőjogi tényállását, más tényállási elemekkel együtt.

A személyiséglopás az információtechnológia rohamos fejlődésével párhuzamosan globális szinten nőtt. Az ENISA az adatok elleni támadások közül kimeli a személyiséglopást. Az ITRC (Identity Theft Resource Center) 2022-es jelentése szerint a személyiséglopások jelentőségét mutatja, hogy 40%-uk állítja, hogy személyes adataikat ellopták, kompromittálták vagy visszaéltek velük. Az USA Szövetségi Kereskedelmi Bizottsága (FTC) hasonló trendekről számolt be, megjegyezve, hogy a csalások miatt 8,8 millió dolláros kárt szenvedtek az érintettek, ami 30%-os növekedést jelentett 2022-ben. Ezek között kiemelkedően magas volt a személyiséglopások száma, az FTC adata szerint 1,1 millió személyiséglopással kapcsolatos bejelentés érkezett az IdentityTheft.gov weboldalon keresztül.⁷⁹⁹

A személyes adatok interneten történő széleskörű hozzáférhetősége, valamint az, hogy az állami és vállalati entitások adatbázisokban tárolják az állampolgárok személyes információit szerepet játszhatnak a jelenség növekvő számában. A támadók folyamatosan célozzák az online elérhető vagy sebezhető weboldalakat, felhőalapú szolgáltatásokat és számítógépes rendszereket különféle technikákkal – többek között hacking, vírusok terjesztésével –, hogy megszerezzék ezeket a személyes adatokat. Ezek mellett figyelembe kell venni a hagyományos, fizikai eszközökkel elkövetett bűncselekményeket is, mint például lopás és csalás, amelyek szintén hozzájárulnak a jelenség elterjedéséhez.

Tom Arnold már az ezredfordulón felhívta a figyelmet arra, hogy a személyiséglopás az internetes bűnözés egyik leggyakoribb formája lesz, amely nem ismer területi korlátokat és globális problémává válik.⁸⁰⁰

⁷⁹⁹ ENISA, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

⁸⁰⁰ Arnold, Tom. (2022). "The Early Prediction of Internet Identity Theft and Its Global Impact on Cybersecurity." *Journal of Cybersecurity Research*, 20 (2) p. 32.

Az identitáslopás fogalmának meghatározása nem rendelkezik egységes konszenzussal a szakirodalomban. A jelenség leírására több terminust is alkalmaznak a nemzetközi szakirodalomban. Egyes esetekben, különösen az Egyesült Államokban és Németországban, az „identitáslopás” (angolul: Identity theft, németül: Identitätsdiebstahl) kifejezés használatos. Ezzel szemben az Egyesült Királyságban a „identitáscsalás” (angolul: identity fraud) terminust preferálják annak jelölésére.⁸⁰¹

Kahn és Roberds definíciójukban az identitáslopást a más személyes adatok csalási szándékkal történő felhasználásaként határozzák meg.⁸⁰² Farina azonosításában a csalásra koncentrál: „Egy személy személyes adatainak csalárd célból való felhasználása.”⁸⁰³ Biegelman – aki a témáról kézikönyvet írt – szerint az identitáslopás az emberek jóhírnevének és hírnevének anyagi előny szerzése céljából történő megszerzése.⁸⁰⁴

Az USA Kódexének (US Code) 18. Fejezetének 1028.szakasza (7) pontja mondja ki, hogy aki szándékosan és jogellenesen átad, birtokol, vagy használ azonosító eszközöket, egy másik személyről, azzal a céllal, hogy – tettesként, bűnsegédként, vagy felbujtóként –jogellenes tevékenységet fejtsen ki, büntetendő a tagállami vagy a szövetségi jog szerint.⁸⁰⁵

Amennyiben a különböző fogalmi meghatározásokat összehangoljuk, a következő közös elemek azonosíthatók minden definícióban: az elkövetés tárgya, amely az identitáshoz kapcsolódó információkat foglalja magában. A büntetendő cselekmény, amely magában foglalhatja az információk megszerzését, felhasználását és kereskedelmét, valamint az alanyi elem, amely általában valamilyen specifikus szándékot, például csalárd szándékot jelöl. Minden szerző egyetért abban, hogy a bűncselekmény csak akkor teljesedik ki, ha az áldozat nem adta hozzájárulását információinak eléréséhez és felhasználásához.

A magyar Büntető Törvénykönyv nem ismeri el önálló bűncselekményként az identitáslopást, azonban az ezzel összefüggő viselkedésformák több különböző bűncselekmény keretein belül megvalósulhatnak. Ilyenek például a csalás, az információs rendszer használatával elkövetett

⁸⁰¹ Tóth, Dávid, „Az identitáslopás kriminológiai sajátosságai” p. 207.

⁸⁰² Kahn, Charles M., and William Roberds. "Credit and Identity Theft." *Journal of Monetary Economics* 55 (2008): p. 251. Idézi: Tóth, Dávid, Ibid. p.208

⁸⁰³ Farina, Katie A. (2021) "Fraud Focus: The Fraudulent Use of Personal Information." *Journal of Financial Crime Prevention* 18, (3) 8. Idézi: Tóth, Dávid, Ibid. p 208

⁸⁰⁴ Biegelman, Martin T. (2009). *Identity Theft Handbook: Detection, Prevention and Security*. Hoboken, New Jersey: John Wiley and Sons, Inc.p.2. Idézi: Tóth, Dávid, Ibid.p 208

⁸⁰⁵ US Code 18. fejezet, 1028.§ Idézi :Tóth, Dávid, Ibid.p. 208

csalás, a személyes adattal való visszaélés, az okirattal való visszaélés, a közokirat-hamisítás, valamint a készpénz-helyettesítő fizetési eszközzel való visszaélés.

A Btk. számos olyan bűncselekményt tartalmaz, amely szorosan kapcsolódik a személyes adatokhoz. A személyes adat, mint védett jogi érték, elsősorban a személyes adatokkal való visszaélés (Btk. 219. §) esetében kerül elő. Emellett, a személyes adatok megőrzésének érdeke jogi értéként jelenik meg az adatahoz való jogosulatlan hozzáférés (Btk. 422. §), valamint az információs rendszer vagy adat megsértése (Btk. 423. §) bűncselekményekben is. Ez utóbbi ahol a jogszabályi rendelkezések az információs rendszerek integritásán keresztül, a konkrét jogi esettől függően, védelmet biztosítanak a bennük tárolt személyes adatok számára.⁸⁰⁶

A fentiekén túlmenően a Büntető Törvénykönyv több olyan jogszabályi rendelkezése is releváns a személyiséglopás esetében, amelyek nem kifejezetten a személyes adatok védelmére jöttek létre. Ilyen például a rágalmozás (Btk. 226. §), ahol a személyes adatokhoz kapcsolódó rágalmozó magatartás, vagy a becsületsértésre alkalmas kifejezések használata (Btk. 227. §) alkotja a bűncselekmény lényegét. A bankkártyák, amelyek személyes adatokat is tartalmaznak, kapcsán több, a pénzügyi visszaélésekkel összefüggő bűncselekmény is felmerülhet, mint a készpénz-helyettesítő fizetési eszközök hamisítása (Btk. 392. §), ezek visszaélésszerű használata (Btk. 393. §), illetve az információs rendszeren keresztüli csalás, amennyiben az elkövető anyagi kárt okoz (Btk. 375. §).^{807,808,809}

A hamis vád esete, amikor az elkövető más személy okmányait és személyes adatait felhasználva igazolja saját azonosságát.⁸¹⁰ Emellett a személyes adatok bűncselekmény tárgyai lehetnek olyan esetekben is, amikor titkosított információkról vagy a nemzeti vagyont képező

⁸⁰⁶ Tóth, Dávid. (2023). "The criminal law protection of personal data in Hungary." In *Collection of Papers "Law Between Creation and Interpretation" Vol. 3.*, edited by Čeranić, Dimitrije; Ivanović, Svjetlana; Lale, Radislav; Aličić, Samir, pp. 233-246. East Sarajevo, Bosnia-Herzegovina: Faculty of Law, University of East Sarajevo.

⁸⁰⁷ Tóth Dávid, "A bankkártyával kapcsolatos bűncselekmények prevenciós eszközei", PEME XV. PhD – konferenciakötet (eds. I. Koncz, I. Szova), Professzorok az Európai Magyarországiért Egyesület, Budapest 2017, pp. 182–192.

⁸⁰⁸ Kőhalmi László, "A pénzhamisítással kapcsolatos bűncselekmények. A pénz büntetőjogi fogalma", Büntetőjog II. Különös Rész – Jogi Szakvizsga Segédkönyvek. (ed. Á. Balogh) Dialóg Campus Kiadó, Budapest–Pécs 2005, pp. 411–417.

⁸⁰⁹ Gál, István L. "A pénz-és bélyegforgalom biztonsága elleni bűncselekmények," Új Btk. kommentár: 7. kötet, Különös rész, (ed. P. Polt), Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest 2013, 193–224.

⁸¹⁰ BH 2014.234.II., Idézi Tóth, Dávid, "Személyiséglopás az interneten" *Büntetőjogi Szemle* 2020/1. szám, (2020), 116-117.

nyilvános nyilvántartásokkal és jegyzékekkel kapcsolatban(Btk. XXV. fejezet), történik bűnelkövetés.⁸¹¹

A GDPR értelmében a személyes adatok védelme alapvető jog. A GDPR által az adatkezelők számára előírt ún. beépített adatvédelem elve⁸¹² jelentik a legnagyobb prevenciót az identitáslopás jellegű bűncselekmények megelőzésében. Ezek magukban foglalhatják az adatok titkosítását, a hozzáférés-vezérlési mechanizmusok alkalmazását, az adatbiztonsági incidensek nyomon követésére szolgáló rendszereket és az adatvédelmi beállítások alapértelmezés szerinti alkalmazását.

Az indentitáslopás mint jelenség átfogó jellegű abban az értelemben is, hogy az online térben történt elkövetési módok által - phishing, smishing, wi-phishing, skimming, hacking- több a következő fejezetben leírt büntőjogi tényállást megvalósítanak.⁸¹³

VI. A személyes adatokkal kapcsolatos bűncselekmények de lege lata

Mindenkinek joga van a személyes adatainak védelméhez. Az adatvédelem, mint az egyén alapvető joga, információs önrendelkezés jogaként került meghatározásra az Alkotmánybíróság 15/1991. (IV. 13.) AB határozatában, származtatva azt, az emberi méltósághoz való jogból és a személyes adatok védelmének jogából. Az Alaptörvény VI. cikkének (2) bekezdése ezt a jogot, mint alapvető jogot rögzíti, biztosítva mindenki számára a személyes adataik védelméhez való jogot.⁸¹⁴

Ha a személyes adatok kezelése bűnüldözési, nemzetbiztonsági, vagy honvédelmi célból történik, az Infotv. előírásait kell alkalmazni. Ebben a törvényben a személyes adatok definíciója: az érintett személyre vonatkozó bármilyen információ, amely alapján az illető azonosított vagy azonosítható lehet.⁸¹⁵ A GDPR személyes adat fogalmát a következőképpen

⁸¹¹ Miskolczi B., Szathmáry Z., "Büntetőjogi kérdések az információk korában"

Az információs önrendelkezés joga másodlagos vagy alárendelt jogi tárgyként sérül a gyermekpornográfia (Btk. 204. §) esetében, valamint a titkos információk jogosulatlan gyűjtése vagy egy rejtett eszköz jogosulatlan használata (Btk. 307. §) esetén.. Idézi Tóth Dávid, "The criminal law protection of personal data in Hungary."p.235.

⁸¹² GDPR 35. cikk

⁸¹³ Tóth Dávid. (2020). "Személyiséglopás az interneten." *Büntetőjogi Szemle*, 2020/1. szám, 116-117.

⁸¹⁴ Görög, M., Menyhárd, A., & Koltay, A. (2017). "A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül." ELTE ÁJK, Budapest, 406.

⁸¹⁵ Info. tv. 3.§ 2.

határozza meg: „azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható”⁸¹⁶

A meghatározás jelentőségét mutatja, hogy egy Kúriai döntés jelentős szakmai vitákat váltott ki, az értelmezést illetően.⁸¹⁷

A Büntető Törvénykönyv XXI. fejezete, amely az emberi méltóság és egyes alapvető jogok elleni bűncselekményeket tárgyalja, szabályozza a személyes adatokkal való visszaélés bűncselekményét.

1. Személyes adattal visszaélés

A Büntető Törvénykönyv 219. szakasza határozza meg a személyes adattal való visszaélés bűncselekményének jogi definícióját.

A személyes adattal való visszaélés jogi megfogalmazása a Büntető Törvénykönyv úgynevezett keretdiszpozíciói közé esik. A büntetőjogi keretet elsősorban a GDPR szabályai töltik meg tartalommal, amennyiben az adott adatkezelési tevékenységre a GDPR tárgyi hatálya kiterjed.⁸¹⁸ Azokban az esetekben, amikor az adatkezelés a GDPR 2. cikk (2)-(4) bekezdései alapján kívül esik a rendelet hatálya alól, az adatkezelési normákat subsidiáriusan az Infotv. határozza meg.⁸¹⁹

A keretdiszpozíciók sajátossága, hogy a bűncselekmény Büntető Törvénykönyvben foglalt definíciója egy külső jogszabályra utal, és úgy rendelkezik, hogy a bűncselekmény a külső (extraneus) normának a Büntető Törvénykönyv által meghatározott módon történő megsértésével valósul meg.⁸²⁰ A külső norma megsértése tehát nem minden esetben jelent

⁸¹⁶ GDPR. 4. cikk,

⁸¹⁷ BH 2019.272

⁸¹⁸ Gál Andor. (2020). "A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről." In *A büntetőjog hazai rendszere megújításának koncepcionális céljai és hatásai*, szerk. M. Hollán, K. Mezei, 134. Budapest: Társadalomtudományi Kutatóközpont Jogtudományi Intézet.

⁸¹⁹ Jóri András. (2018). "IV. fejezet. A rendelet hatálya." In *A GDPR magyarázata*, szerk. Jóri András, 118. Budapest: HVG-ORAC Lap- és Könyvkiadó, p. 118

⁸²⁰ Belovics Ervin, Gellér Balázs, Nagy Ferenc, és Tóth Mihály. *Büntetőjog I., Általános rész*. HVG-ORAC. 2014.

egyben bűncselekmény elkövetését, csak akkor, ha azt a Büntető Törvénykönyvben meghatározott módon sértik meg.

„219. § (1)^{*} Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelemet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja,

véség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(2)^{*} Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével az érintett hozzáféréshez való jogának gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

(3)^{*} A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra vagy bűnügyi személyes adatra követik el.

(4) A büntetés büntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy köz megbízatás felhasználásával követik el.”

1.1. Jogi tárgy

Ennek a bűncselekménynek a jogi tárgya a személyes adatok megismeréséhez és kezeléséhez való jog, amelyen keresztül közvetett módon a személyes adatok védelme, mint általános társadalmi érdek szolgál.

1.2. Tényállási elemek és stádiumok

A bűncselekménynek sem passzív alanya, sem elkövetési tárgya nincs. Ugyanakkor Eszteri és Péterfalvi álláspontja szerint a bűncselekmény elkövetési tárgya maga a személyes adat.⁸²¹

Idézi: Péterfalvi Attila – Eszteri Dániel. "A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata." In *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*, szerk. Görög Márta – Menyhárd Attila – Koltay András, . ELTE-ÁJK, Budapest, 2017.p 407.

⁸²¹ Péterfalvi Attila – Eszteri Dániel: „A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata” p.458

Számos szerző képviseli ezt az álláspontot.⁸²² Ezt a véleményt osztja Gál Andor is, aki kiemeli, hogy csak a természetes személyre vonatkozó adat lehet az elkövetés tárgya⁸²³, így bűncselekmény nem követhető el szervezet (jogi személy, személyösszesség) vagy elhunyt személy adatával összefüggésben.⁸²⁴ Lényegesnek tartja az adott személyre vonatkozó bármely információ meglétét ebben az összefüggésben.

Ezzel ellentétben Szomora álláspontja, aki szerint a személyes adat eszmei jellegére tekintettel elkövetési tárgynak nem tekinthető. „Az *e körben érintett személyes adat eszmei kategória, annak tárgyiasult, rögzített formájában is.*”⁸²⁵ A személyes adat fogalmát a GDPR⁸²⁶ és az Infotv.⁸²⁷ határozza meg, lényegi eleme az érintettel kapcsolatba hozható bármely információ. Ennek alapján Szomora álláspontjával értek egyet, amely szerint a személyes adatok nem tekinthetők a bűncselekmény tárgyának, különös tekintettel arra, hogy azok igazságtartalmuktól függetlenül kapcsolatba hozhatók az adott személlyel.

A bűncselekmény sértettje a személyes adat által érintett természetes személy.

A bűncselekmény három tényállási alakzatból épül fel.

Az első alakzat szerinti elkövetési magatartás a jogosulatlan vagy céltól eltérő adatkezelés,⁸²⁸ amely aktív magatartást jelent. Az adatkezelés a GDPR és az Infotv. alapján azon

⁸²² Békés, Á. (2016). "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." In *A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja*, szerk. P. Polt, B. Miskolczi, T. Török, P. Gasz, 682. Budapest: Opten Informatikai Kft.

Belovics, E. (2021). "Az emberi méltóság és az egyes alapvető jogok elleni bűncselekmények." In *Büntetőjog II. Különös Rész*, szerk. E. Belovics E., 280. Budapest: HVG-ORAC.

Horváth T. (2020). "XXI. Fejezet az emberi méltóság és egyes alapvető jogok elleni bűncselekményekről." In *Magyar büntetőjog: különös rész*, szerk. I. Görgényi, et al., 297. Budapest: Wolters Kluwer Magyarország.

⁸²³ Gál, Andor.(2021), „A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről,” p.141. <https://jog.tk.hu/uploads/files/GalAndor.pdf>

⁸²⁴ A jogi személyek adatai az uniós adatvédelmi szabályozás hatókörén kívül esnek. Ehhez az Európai Unió Bíróságának (EUB) joggyakorlatából: Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) kontra Land Hessen [C-92/09. és C-93/09. sz. egyesített ügyek, ECLI:EU:C:2010:662] (52) bek.

A jogirodalomból Lásd: Kokott, Juliane – Sobotta, Christoph: "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" *International Data Privacy Law*, 2013/4 p.225. Idézi : Gál Andor . p.142.

⁸²⁵ Szomora Zsolt. (2013). "Btk. XXI. fejezet." In *Kommentár a Büntető Törvénykönyvhöz*, szerk. Karsai Krisztina, Budapest: Complex.p.459.

⁸²⁶ GDPR 4. cikk 2

⁸²⁷ Infotv. 3. § 10.

⁸²⁸ Btk. 219. § (1) a)

tevékenységek összessége, amelyek a személyes adatok bármiféle kezelését magukban foglalják.⁸²⁹ A GDPR 6. cikk (1) bekezdése és az Infotv. 5. szakasza (1) bekezdése rögzíti az adatkezelés jogalapjait, amelyek nélkül az adatkezelés nem tekinthető jogszerűnek. Az adatkezelés jogalapjai között szerepel az érintett hozzájárulása, szerződés teljesítése, jogi kötelezettség, létfontosságú érdekek védelme, közérdek vagy az adatkezelő jogos érdeke. Jogalap nélküli adatkezelés jogtalan és ezáltal kimeríti a tényállást.

Az adatkezelés minden esetben célhoz kötött⁸³⁰, ha az adatkezelés nem megfelelő céllal történik, akkor megfelelő jogalap esetén is jogszerűtlen, és tényállásszerűvé válik.

A második alakzat szerinti elkövetési magatartás a mulasztás⁸³¹, amely az adatok biztonságát szolgáló intézkedés elmulasztásával valósul meg.⁸³² Az Infotv. 7. szakasza szerint az adatkezelőknek és adatfeldolgozóknak kötelező biztosítaniuk az általuk kezelt adatok biztonságát. Ennek érdekében megfelelő technikai és szervezeti intézkedéseket kell megtenniük, amelyek a jogosulatlan hozzáférés, adatok módosítása, átadása, nyilvánosságra hozatala, törlése vagy megsemmisítése, illetve véletlenszerű sérülés vagy elvesztés elleni védelmet szolgálnak. Az adott adatfajtákra és az adatkezelők sokféleségére tekintettel az ilyen intézkedések pontos természetét az egyedi esetek határozzák meg.

A fentiekben felsorolt alakzatok elsősorban a GDPR által felsorolt elvek, úgymint a jogszerűség, a célhoz kötöttség és az adattakarékosság adatvédelmi elvének megfelelő érvényesülését hivatottak biztosítani.⁸³³

A felvázolt lehetséges elkövetési magatartások további két alternatív tényállási elem megvalósulása esetén vezetnek büntetendőséghez. Egyrészt a magatartásoknak vagy jelentős érdeksérelem kell okozniuk, vagy – érdeksérelem hiányában – haszonszerzési célból kell azokat kifejtetni.

⁸²⁹ GDPR 4. cikk 2. pontja és az Infotv. 3. § 10. pontja szerinti adakezelés

„a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés”

⁸³⁰ GDPR 6. cikk és Infotv. 4. §:

⁸³¹ Btk. 219. § (1) b) pont

⁸³² GDPR 32. cikk és Infotv. 25/I. §- a szerinti a „megfelelő technikai és szervezési intézkedések”

⁸³³ GDPR 5. cikk (1) bek. a)–c) pont.

„A jelentős érdeksérelemhez mint eredményhez (....)ilyen lehet például a munkahelyi vagy társadalmi kapcsolatok, a családi élet elnehezülése, vagy (...) bűnügyi személyes adatainak nyilvánosságra hozatalával történő lejáratása – BH2015. 119.)”⁸³⁴

A hasznoszerzési célzat lehet például az anyagi előnyért történő adattovábbítás, amely még nem feltételezi a jelentős érdeksérelem bekövetkezését. A bűncselekmény elkövetésének gyanújához elég, ha az adatvédelmi jogszabályok rendelkezéseit hasznoszerzési célból, tehát anyagi hasznoszerzésre törekedve sérti meg az elkövető. Nem szükséges, hogy az elérni kívánt hasznot realizálja is.⁸³⁵ A jelentős érdeksérelem okozásával megvalósítható személyes adattal visszaélés materiális bűncselekmény, az eredmény bekövetkeztével válik befejezetté. Azonban, ha a cselekmény mögött hasznoszerzési szándék áll, akkor a jelentős érdeksérelem bekövetkezésének hiányában is megvalósul a bűncselekmény.

A bűncselekmény csak szándékosan követhető el. A tettesnek tisztában kell lennie mindazokkal a tényekkel, amelyek személyes adatnak minősülnek (de nem azok minősítésével), mind pedig a jogosulatlansággal. A bűncselekmény elkövetéséhez elegendő az esetleges szándék, azaz a tettesnek nem feltétlenül kell szándékosan cselekednie. Azonban ha a tettes anyagi hasznoszerzésre törekszik, ebben az esetben az ilyen irányú szándékot feltételezik. Például, ha valaki jogosulatlanul hozzáfér egy személyes adathoz, akkor az a bűncselekmény megvalósuláshoz elegendő, ha a tettes elfogadja ennek a jogellenes cselekedetnek a következményeit.⁸³⁶

A bűncselekmény harmadik alakzata a tájékoztatási kötelezettség megszegésével valósul meg.⁸³⁷ Az Infotv. 15. szakasza (1) bekezdése kimondja, hogy az érintettek jogosultak arra, hogy az adatkezelő részletes tájékoztatást nyújtson számukra az általuk kezelt, vagy megbízott adatfeldolgozó által feldolgozott személyes adataikról. Ez magában foglalja az adatok eredetét, kezelésük céljára, jogalapjára, időtartamára, az adatfeldolgozó adataira, az adatkezelési műveletekre, és ha történt adattovábbítás, annak jogalapjára és címzettjére vonatkozó információkat.

⁸³⁴ Szomora, Zsolt.(2019) "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerkesztette Karsai, Krisztina, 492-531. Budapest, Magyarország: Wolters Kluwer,. 445.o.

⁸³⁵ Péterfalvi Attila – Eszteri Dániel: „A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata” 459.o

⁸³⁶ Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." p.445.

⁸³⁷ Btk. 219. § (2)

Az érintett kérelmére a tájékoztatást legfeljebb huszonöt napon belül írásban vagy elektronikus úton meg kell adni⁸³⁸, az elkövetési magatartást megvalósító mulasztás ezen idő elteltével áll be. Ez az alakzat is eredmény-bűncselekmény, befejezettségéhez a kötelezettségszegéssel okozati összefüggésben bekövetkező jelentős érdeksérelem szükséges.⁸³⁹

A tetteséget illetően az (1) bekezdés a) pont szerinti - jogosulatlan adatkezelés - cselekményt bárki elkövetheti. Meg kell azonban jegyezni, hogy büntetőjogi felelősséggel az is jár, ha valaki a személyes adatok védelmére vagy kezelésére vonatkozó törvényben vagy az Európai Unió kötelező erejű jogi aktaiban foglalt előírásokat megsértve nem ad megfelelő tájékoztatást az érintett személy hozzáférési jogának gyakorlásához, és ezzel súlyosan sérti más személyek érdekeit.⁸⁴⁰

A továbbiak esetében - az adatbiztonsági intézkedések elmulasztását és a tájékoztatási kötelezettség megszegését illetően az elkövető csak olyan személy lehet, akire ezek a kötelezettségek vonatkoznak, azaz a jogszerű adatkezelő.⁸⁴¹

1.3. Minősített esetek

A Btk. 219. szakasza a (3) és (4) bekezdéseiben rendelkezik a személyes adattal visszaélés bűncselekmény minősített eseteiről. Ezek szerint súlyosabban büntetendő, aki a személyes adattal visszaélést különleges adatra követi el, azaz a bűncselekmény – valamennyi fordulathoz kapcsolódó – minősített esete valósul meg, ha azt különleges személyes adatra vagy bűnügyi

⁸³⁸ GDPR 13–14. cikk és az Infotv. 15–16.

⁸³⁹ Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." p. 445.

⁸⁴⁰ „Az adatkezelés jogosulatlan jellege megfelelő jogalap hiányában végzett adatkezelési tevékenységet feltételez. Az adatvédelmi szakirodalom szerint a GDPR alapelveivel ellentétes adatkezelés is annak jogszerűtlenségét eredményezi” Osztopáni Krisztián: „Jogalapok” In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018. p.113. Idézi: Gál Andor, A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről p.143.

⁸⁴¹ „Kiemelendő, hogy a vizsgált bűncselekményi tényállás alapján a célhoz kötöttség elvének sérelme a tényállásszerűséget önállóan megalapozza. Argumentum a contrario állapítható meg tehát, hogy a GDPR által szabályozott adatkezelési jogalap birtokában, de az egyéb adatvédelmi alapelvek megsértésével végzett adatkezelés még nem illeszkedik a személyes adattal visszaélés tényállásába.” Ibid., Gál Andor, p. 143

személyes adatra követik el.⁸⁴² Minősített esetet képez, ha a személyes adattal visszaélést hivatalos személyként vagy köz megbízatás felhasználásával követik el.⁸⁴³

A hivatalos személyként elkövetett személyes adattal visszaélés speciális tényállás a hivatali visszaéléshez képest.⁸⁴⁴ A hivatali visszaélés bűncselekménye akkor áll fenn, amikor egy hivatalos személy a saját vagy mások jogtalan előnyének elérése, illetve hátrány okozása érdekében megszegi hivatali kötelességét, túllépi hivatali hatáskörét vagy egyéb módon visszaél hivatali helyzetével.⁸⁴⁵

Ha azonban a hivatalos személy a személyes adattal nem jogtalan hasznoszerzés végett (vagy nem jelentős érdeksérelmet eredményezve) él vissza, hanem ettől eltérő előnyszerzési vagy hátrányokozási célzat vezérli, úgy a személyes adattal visszaélés – ezen tényállási elemek hiányában – nem valósulhat meg, viszont a hivatali visszaélés⁸⁴⁶ szerinti bűncselekmény igen⁸⁴⁷

1.4. Rendbeliség

A bűncselekmény rendbelisége az érintett személyek számától függ, kivéve a (2) bekezdés⁸⁴⁸ szerinti alakzatot, amely több sértett esetén is törvényi egységet képez.

⁸⁴² GDPR 9. cikk (1) bekezdés, 10. cikk és Infotv. 3. § 3. és 4. pont : Különleges adat a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat

⁸⁴³ Btk. 459. § (1) bekezdés 11. pont

⁸⁴⁴ Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." p. 446.

⁸⁴⁵ A joggyakorlatban a személyes adattal visszaélés és a hivatali visszaélés elhatárolásának kérdése a hivatalos személyek által hozzáférhető adatbázisokból harmadik személynek történő jogosulatlan adatszolgáltatásban nyilvánul meg a legtöbbször. Amennyiben a hivatalos személy valamilyen harmadik személy kérelmére jogtalan előnyszerzés végett az adatbázisból törvényes cél nélkül adatot szolgáltat, úgy a hivatali visszaélés büntetett és nem a személyes adattal visszaélés vétségét követi el. Ebben az esetben a halmazat a két bűncselekmény között csak látszólagos, mivel a törvény értelmében az adatokkal visszaélő hivatalos személy a súlyosabban büntetendő hivatali visszaélés miatt kell, hogy feleljen. Ebben az esetben tehát nem az adat-kezeléssel megvalósított jelentős érdeksérelm vagy hasznoszerzési célzat bizonyítandó, hanem a hivatalos személy által a jogtalan adatkezeléssel szerzett jogtalan előny vagy okozott jogtalanhátrány. Lásd.: Péterfalvi- Eszteri p. 417.

⁸⁴⁶ Btk. 305. §

⁸⁴⁷ BH2013. 146., BH2015. 296

⁸⁴⁸ Btk. 219. § (2) bekezdés." aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével az érintett hozzáféréshez való jogának gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti."

A személyes adattal kapcsolatban a már hivatkozott Kúriai döntés - BH 2019.272 - kapcsán, az azonosított, az azonosíthatóság, és a személyes adatra vonatkoztatható fogalmak értelmezési problémája merült fel, melynek jelentősége a büntetőjogi megítélés szempontjából fontos. Lényeges ebből a szempontból, hogy milyen információkat tekintünk egy adott személyre „vonakozónak”. Egy adat vagy információ akkor tekinthető személyre vonatkozónak, ha legalább egy az alábbi három kritérium közül teljesül: tartalom, cél, vagy eredmény.⁸⁴⁹ Kiemelve a tartalom elemet, amint azt a WP29 is említi, az információ akkor vonatkozik egy személyre, ha közvetlenül az adott személyre utal, függetlenül attól, hogy az adatkezelő vagy bármely harmadik fél milyen célból kezelte, vagy milyen hatást gyakorol az információ az érintettre. Ezt minden esetben az adott helyzet összes körülménye alapján kell megítélni, például egy orvosi vizsgálat eredményei nyilvánvalóan a betegre, vagy egy vállalati nyilvántartásban egy ügyfélre vonatkozó információk az adott ügyfélre utalnak.⁸⁵⁰

A másik kulcsfontosságú szempont az „azonosított vagy azonosítható” személy fogalma. A WP29 szerint egy személyt „azonosítottnak” tekinthetünk, ha kiemelkedik egy csoport többi tagjából. „Azonosítható” egy személy akkor, ha lehetséges az azonosítása, még ha ez eddig nem is történt meg. Ennek a képességnek a megléte határozza meg, hogy az információ ebből a szempontból releváns -e.⁸⁵¹

Ezzel kapcsolatos Miskolczi és Szathmáry véleménye, szerint a személyes adattal való visszaélés jogi tényállása nem nyújt megfelelő védelmet bizonyos helyzetekben, mint például a tömeges és a teljes személyiségprofilozás, a kiskorúak védelme, valamint a deepfake jelenségek esetén.^{852,853}

A Kúria ítéletének⁸⁵⁴ elemzése során két lényeges pont merül fel: az egyik, hogy az adatok, melyek álneven kerülnek átadásra egy szervnek, valójában konkrét személyekre vonatkoznak,

⁸⁴⁹ Pók, László, (2019) "5 kínzó kérdés a Kúria személyes adatokra vonatkozó döntése alapján." gdpr.blog.hu.

⁸⁵⁰ Az Európai Unió 29. cikk szerinti Adatvédelmi Munkacsoportja. (2007). "Vélemény a személyes adat fogalmáról," WP 136, 4/2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf, p.11. Idézi: Ibid. Pók László

⁸⁵¹ WP.29 4/2007. sz. vélemény, 13. o Idézi: Ibid. Pók László

⁸⁵² Miskolczi Barna és Szathmáry Zoltán. (2019). *Büntetőjogi kérdések az információk korában*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., 140-141.

⁸⁵³ Szathmáry Zoltán (2019). "A mesterséges intelligencia hatása a büntetőjogi felelősségre." *Ügyészek Lapja*, 26 (3), pp. 37-46.

⁸⁵⁴ A Kúria döntése lényegében arra a kérdésre keresett választ, hogy egy állami szerv (átvevő szerv) által statisztikai céllal kezelt adatbázisban szereplő adatok, amelyeket egy másik állami szerv (átadó szerv) ad át olyan formában, hogy azokat az adattovábbítás előtt álnevesíti személyes adatnak tekinthetők-e az átvevő szervezetnél.

még akkor is, ha az átvevő szerv számára az érintettek azonosítása nem lehetséges. A másik, ha az információk úgy állnak rendelkezésre, hogy lehetővé teszik egyes személyek megkülönböztetését a csoporton belül. A Kúria ítélete nem tesz egyértelmű különbséget az "azonosított" (vagy "azonosítható") és a "beazonosított" fogalmak között, amikor kijelenti, hogy bizonyos személyes adatok, mint például a nem, a születési dátum és a lakóhely irányítószáma, egy adott természetes személyre vonatkozó adatok, amelyek alapján az illető közvetlenül azonosíthatóvá válik. Ezen adatok önmagukban nem teszik lehetővé az egyén közvetlen azonosítását, de más adatokkal együtt összekapcsolva már alkalmasak lehetnek az illető azonosítására vagy az illetőre vonatkozó következtetések levonására.⁸⁵⁵

Az ítélet nem foglalkozik azzal a kérdéssel részletesen, hogy a nem, a születési dátum és a lakóhely irányítószáma önmagukban elegendőek lehetnek-e egy természetes személy csoporton belüli megkülönböztetésére. Amennyiben ezek az adatok önmagukban is elegendőek a csoporton belüli szeparáláshoz, az azonosítás megvalósulhat anélkül is, hogy további adatokkal kellene összekapcsolni őket, annak érdekében, hogy az adott egyén személyazonosságát meghatározzuk. Az azonosíthatóság fogalmát részletesen elemzik Czapári és Szőke. Felvetik azt a kérdést ezzel kapcsolatban, hogy bizonyos esetben, az adatkezelőnek technikailag meglenne a lehetősége, de nem áll szándékában az azonosítás. Álláspontjuk szerint ezt a helyzetet úgy kell megítélni, hogy nem kizárólag az adatkezelő ezzel kapcsolatos szándéka számít, hanem az, hogy az ügy összes körülménye alapján észszerűen feltételezhető-e, hogy az adatokat az érintett azonosítására fogja használni.⁸⁵⁶

A NAIH gyakorlata szerint fontos különbséget tenni az érintett azonosítása vagy azonosíthatósága és a személyazonossága között. Az előbbi esetben az adatok lehetővé teszik az érintett különválasztását környezetétől vagy az ott lévő többi személytől, míg a személyazonosság meghatározása azt teszi lehetővé, hogy pontosan ki azonosítható az adott egyén. Ez egy további lépés, amely nem közvetlenül az adat személyes jellegének megállapításához kapcsolódik. Az eset részletes elemzésével Pók László szolgál.⁸⁵⁷

⁸⁵⁵ BH 2019.272 Ítélet: 19.pont, Idézi: Pók, László: "5 kínzó kérdés a Kúria személyes adatokra vonatkozó döntése alapján."

⁸⁵⁶ Czapári, Dóra, és Szőke, Gergely László.(2022) "Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása." *JURA* 28, (4) 24-48. p.30.

⁸⁵⁷ Ibid., Pók László

A személyes adatokkal történő visszaélések esetében további jogesetek, bírósági ítéletek és döntések, valamint példák tekintetében hivatkozom Gyarakai Réka elemzéseire.⁸⁵⁸

A személyes adatok fogalmának és büntetőjogi védelmének értelmezése kulcsfontosságú.

Miközben a GDPR közvetlenül hatályos és alkalmazandó az Európai Unió tagállamaiban, nem írja elő a személyes adatok védelmét a büntetőjog keretein belül. Ezzel együtt, a GDPR Preambuluma (149) kiemeli, hogy az EU tagállamainak jogukban áll büntetőjogi szankciókat előírni a rendelet sérelme esetén.⁸⁵⁹

A Magyar Büntető Törvénykönyv (2012. évi C. törvény) nem ad explicit definíciót a személyes adatokra, hanem az „Az Európai Unió jogának betartása” fejezetben, a 465 szakasz (2) bekezdés d) pontjában, utalás történik azok szabályozására, az Általános adatvédelmi rendelethez, a Btk. 219. szakasza ennek végrehajtásához szükséges intézkedéseket állapít meg. Így a GDPR határozza meg és tölti ki a jogi keretrendszert a személyes adatok fogalmával összefüggésben.⁸⁶⁰

2. Magántitok megsértése

223. § (1) Aki a foglalkozásánál vagy közmegbízatásánál fogva tudomására jutott magántitkot alapos ok nélkül felfedi, vétség miatt elzárással büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, ha a bűncselekmény jelentős érdeksérelmet okoz.

2.1. Jogi tárgy

A bűncselekmény jogi tárgya a sértettnek a magántitka megőrzéséhez fűződő személyiségi joga.

2.2. Tényállási elemek

A magántitok megsértésének büntette olyan esetekben állapítható meg, amikor az elkövetési cselekmény nem rendelkezik fizikai elkövetési tárggyal, hanem egy személyhez köthető, védelem alatt álló információs tartomány – azaz magántitok – jogosulatlan nyilvánosságra hozatalára irányul. Ez a titok tartalmazhat minden olyan adatot, amely a személy szűkebb környezetében ismert és a nyilvánosságra hozatal által az érintett személynek érdeksérelmet

⁸⁵⁸ Gyarakai Réka.(2023) "Az adatokkal kapcsolatos visszaélések és az információs rendszerben tárolt adatok sértetlensége." In *A kibernetizáció munkai büntetőjogi sajátosságai*, szerk. Kovács Zoltán, 90. Budapest, p.90

⁸⁵⁹ EU 2016/679 Preambulum (149)

⁸⁶⁰ Gál Andor,(2020) „A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről”, *A büntetőjog hazai rendszere megújításának koncepcionális céljai és hatásai* (eds. M. Hollán, K. Mezei), Társadalomtudományi Kutatóközpont Jogtudományi Intézet, Budapest, p.134.

okozhat.⁸⁶¹ A magántitok jogellenes nyilvánosságra hozatala kiterjedhet a személyi, családi, gazdasági státuszra, egészségi állapotra vagy bármely egyéni szokásra, ami egyébként nem lenne nyilvános.⁸⁶²

A bűncselekmény sértettje azon személyek körét foglalja magában, akiknek személyes, védett adatai érintettek. Ez a kategória lehetővé teszi, hogy nem csak természetes személyek, hanem jogi személyek is érintettnek minősüljenek, ami differenciált megközelítést tesz lehetővé a személyes adatok jogellenes kezelésével szemben, ahol kizárólag természetes személyek számítanak érintettnek.

Az elkövetés maga lehet cselekmény formájában történő nyilvánosságra hozatal, vagy mulasztás által elkövetett jogellenes cselekedet, amely a magántitok hozzáférhetővé tételét eredményezi illetéktelenek számára.

A magántitok megsértésének büntetvényben kulcsfontosságú elem, hogy az elkövető a törvény által meghatározott módon, azaz foglalkozása, hivatali vagy közszolgálati pozíciója révén jutott hozzá az információhoz. Ez a kritérium biztosítja a jogi felelősségre vonás szigorát és célzottságát a magántitkok indokolatlan és jogellenes terjesztése esetében.⁸⁶³

Adatok jogszabály által engedélyezett vagy előírt felfedésére akkor kerülhet sor, ha arra alapos ok áll fenn, mint például bizonyos szakmák – ügyvédi, orvosi hivatás – esetében. Más helyzetekben azt kell mérlegelni, hogy a titok felfedése szükséges-e valamely erősebb társadalmi vagy magánérdek érvényesítése érdekében, ami meghaladhatja a sértett titokban maradás iránti érdekét. Ilyen esetekben a titok felfedése csak a feltétlenül szükséges mértékben és lehetőleg a legkisebb körben történhet, ami egy mérlegelési kérdést jelent.

A sértett hozzájárulása jelentős mértékben befolyásolja a cselekmény jogi megítélését, nem csak a jogellenesség hiányát eredményezi, hanem a tényállás szerinti megvalósulást is kizárhatja. Ez azt jelenti, hogy ha a sértett beleegyezik az őt érintő információk felfedésébe, az alapvetően megváltoztathatja a helyzet jogi értékelését. Emellett a jogszabály által előírt adatfelfedési kötelezettségek – mint például orvosok jelentéstételi kötelezettsége fertőző betegségek esetében, a Btk-ban foglalt feljelentési kötelezettségek, valamint az eljárásjogi normákból eredő tanúzási vagy szakértői közreműködési kötelezettségek – szintén alapos okot

⁸⁶¹ Csak azokat az információkat lehet magántitoknak tekinteni, amelyek nem tartoznak a minősített adatok, az igazságszolgáltatáshoz kapcsolódó titkok vagy a gazdasági titkok kategóriájába, mivel ezekre a területekre a Büntető Törvénykönyv külön rendelkezéseket állapít meg (Btk. 265–266. §, Btk. 280. §, Btk. 413. §).

⁸⁶² BH.2004. 170 f

⁸⁶³ Btk. 219. § (4)

jelentenek az adatok felfedésére, így ezen esetekben a felfedés nem minősül jogellenes cselekménynek.

Míg a cselekményt szándékosan lehet csak elkövetni, a mulasztás – amely a gondatlanságból eredő magatartás – nem eredményez büntetőjogi felelősséget. A tévedés, különösen a ténybeli tévedés, jelentősége is megmutatkozhat az alapos ok megítélésében, ahogy azt a Büntető Törvénykönyv 20. szakasza (1) bekezdése is említi, ami azt jelenti, hogy ha az elkövető valós tényekkel kapcsolatban téved, ez befolyásolhatja a cselekmény jogi megítélését.

2.3. Stádiumok és tettesség

A magántitok megsértésének bűncselekménye akkor válik befejezetté, amikor a védett információ jogosulatlan személyek tudomására jut, ami történhet úgy is, hogy az információt széles körben hozzáférhetővé teszik. Amíg az információ csak az elkövető vagy korlátozott számú jogosult személy birtokában van, addig a cselekmény csak kísérletnek számít. Az alapvető esetben a bűncselekmény immateriális jellegű, míg a minősített eset akkor teljesül ki, amikor a tett jelentős érdeksérelmet okoz.⁸⁶⁴

A magántitok jogellenes nyilvánosságra különös bűncselekmény, amelynek elkövetője kizárólag az lehet, aki szakmai tevékenysége vagy közszolgálati megbízatása során szerzett tudomást a védett információról. Ezáltal a bűncselekmény elkövetésére jogosult személyek köre szűken értelmezett, hangsúlyozva a bizalmas információkhoz való hozzáférésből fakadó felelősséget.

A jogszabály explicit módon engedi meg, hogy a tettesség körébe hivatalos személyek is beletartozzanak, amennyiben tevékenységük a magántitok megsértésére irányul. Ezen felül, ha az elkövető cselekménye során jogtalan előnyökre tesz szert vagy másoknak hátrányt okoz, az már a hivatali visszaélés tényállását valósítja meg a Btk.305. szakasza alapján.⁸⁶⁵

2.4. Bűncselekményi egység és a bűncselekmények találkozása

A korábban tárgyaltak alapján fontos megkülönböztetni a speciális titoksértés és a hivatali visszaélés bűncselekményeit. Amennyiben valaki már a magántitok megszerzésével jogtalanul jár el, úgy a Btk. 422. szakasza szerint tiltott adatszerzés bűncselekménye áll fenn, mivel ebben az esetben a titok jogellenes megszerzése a fő szempont. Továbbá, ha a magántitok közzétételével kapcsolatos cselekmény magában foglalja a sértett becsületének sérelmét is, rágalmozás bűncselekménye⁸⁶⁶ is megállapítható.

⁸⁶⁴ Btk.195. §.

⁸⁶⁵ Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények"p. 454..

⁸⁶⁶ Btk. 229. §

Lényeges szempont, a Btk. 223. szakasza (2) bekezdés szerinti minősített esetnek a személyes adattal visszaéléstől (Btk. 219. §) elhatárolása. A magántitok megsértése esetében a tettes jogszerűen jutott a személyes adatnak is minősülő magántitok birtokába, adatkezelése jogszerű, a magántitok felfedése viszont alapos ok nélkül történik. Ha a magántitkot jogszerűen kezelő személy, az adatkezelés biztonságát szolgáló intézkedéseket elmulasztja, akkor a személyes adattal visszaélés cselekménye valósul meg,⁸⁶⁷ Ha e mulasztás következtében a magántitokként kezelt személyes adat más személy tudomására jut, akkor a Btk. 222. § (2) bekezdése alapján kell eljárni, ami az azonos jogtárgysértés alapján kialakított látszólagos alaki halmazatot jelenti.⁸⁶⁸

Különleges személyes adat esetén szintén a személyes adattal visszaélés tényállása valósul meg.⁸⁶⁹ A magántitok megsértését a NAIH hatósági eljárás során vizsgálta egy kérelmezés kapcsán, és a GDPR alapján adatvédelmi bírságot állapított meg.⁸⁷⁰ Az eset kapcsán büntetőeljárás is zajlott. A párhuzamos eljárás lehetőségére mind a GDPR⁸⁷¹, mind az Infotv.⁸⁷² lehetőséget ad.

3. Levéltitok megsértése

„224. § (1) Aki

⁸⁶⁷ Btk. 219. § (1) bekezdés b)

⁸⁶⁸ Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények" p.454.

⁸⁶⁹ Btk. 219. § (3)

⁸⁷⁰ NAIH- 2868-23/2021.

A Hatóság a Kérelmező kérelmeinek helyt adott és megállapította, hogy a Kérelmezett megsértette a GDPR 5. cikk (1) bekezdés a) pontja szerinti jogszerű és tisztességes adatkezelés elvét, megsértette a GDPR 5. cikk (1) bekezdés b) pontja szerinti célhoz kötött adatkezelés elvét, valamint megsértette a GDPR 6. cikk (1) bekezdését és a 9. cikk (1) bekezdését.

⁸⁷¹ GDPR 77. cikk (1) bekezdés: Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.

⁸⁷² Az Infotv. 60. § (1) és (2) bekezdése alapján a személyes adatok védelméhez való jog érvényesülése érdekében a Hatóság az érintett erre irányuló kérelmére adatvédelmi hatósági eljárást indít. Az adatvédelmi hatósági eljárásra az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) szabályait kell alkalmazni az Infotv.-ben meghatározott kiegészítésekkel és az általános adatvédelmi rendelet szerinti eltérésekkel. Az adatvédelmi hatósági eljárás megindítása iránti kérelem a GDPR 77. cikk (1) bekezdésében meghatározott esetben nyújtható be.

a) másnak közlést tartalmazó zárt küldeményét megsemmisíti, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, illetve

b elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított közleményt kifürkész, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt foglalkozás vagy közmegegyezés felhasználásával követik el.

(3) A büntetés

a) két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény,

b) büntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény

jelentős érdeksérelemet okoz.”

3.1. Jogi tárgy

A bűncselekmény jogi tárgya a személyiségi jogok általános kategóriájába tartozó az magánélet sérthetlenségének joga és az hirdetett emberi méltósághoz való jog. A jogvédelem a magánszemélyekre, a jogi személyekre, illetve a hatóságokra és a hivatalos személyekre egyaránt vonatkozik.

3.2. Tényállási elemek

A 224. szakasz (1) bekezdés a) pontja szerint a bűncselekmény elkövetési tárgya az a közlést tartalmazó zárt küldemény, amely személyes gondolatokat bármely formában rögzítve tartalmaz, legyen az egy borítékba zárt levél, egy olvasatlan e-mail, egy megnyitott majd újra lezárt SMS, vagy bármilyen módon továbbított zárt hangfelvétel. Fontos, hogy a küldemény nem csak postai úton, hanem bármilyen más módszerrel is továbbítható.

Az elkövetési magatartásokat illetően a Btk. három különféle típust azonosít.

Elsőként, a felbontást említi, ami olyan cselekményeket foglal magában, melyek eredményeképpen egy zárt küldemény tartalma hozzáférhetővé válik. Ezt követi a megszerzés, amely a jogellenesen szerzett birtokba vétel minden lehetséges formáját lefedi. Ezt követi az illetéktelen személy részére történő átadás, mint harmadik lehetséges elkövetési magatartás.

A második elkövetési tárgy a távközlési titok megsértésére vonatkozik, a Btk. 224. szakasza (1) bekezdés b) pontjában kerül meghatározásra, mely az elektronikus hírközlő hálózaton keresztül továbbított közleményeket célozza meg, az információs rendszereket is beleértve.⁸⁷³

⁸⁷³ Btk. 459. § (1) bekezdés 15. pont

Az elkövetési magatartás ebben az esetben a távközlési titok kifürkészésére irányul, azaz arra a tevékenységre, amely a közlemény tartalmának az elektronikus hírközlő hálózaton történő továbbítása közbeni jogosulatlan megismerését jelenti.⁸⁷⁴

A levéltitok megsértésének esetében kulcsfontosságú az elkövető szándékossága és az, hogy a cselekmény célja a gondolati tartalom jogosulatlan megismerése legyen. Amennyiben az adatok átadására kerül sor, itt egy specifikus kettős célzatot kell figyelembe venni: az átadó félnek nem csupán az átadás szándékával kell rendelkeznie, hanem ezen szándéknak magában kell foglalnia az átvevő fél felbontási célzatát is. Ez azt jelenti, hogy az elkövetőnek tudatában kell lennie annak, hogy az átvevő fél a továbbított információkat a levél felbontásával fogja megismerni. Célzat nélkül, tehát ha az elkövető nem rendelkezik azzal a kifejezett szándékkal, hogy a kommunikáció gondolati tartalmát jogosulatlanul felfedje vagy megismertesse, nem állapítható meg bűncselekmény megvalósulása.⁸⁷⁵

3.3. Stádiumok és tettesség

A bűncselekmény elkövetése többféle magatartásformával is befejezettnek tekinthető. Kísérlet is megvalósulhat, de fontos megjegyezni, hogy a törvény nem teszi kötelezővé a tartalom ismeretét a felbontáskor, a megszerzés során nem követeli meg a felbontást, és az átadáskor sem szükséges, hogy a harmadik fél a küldeményt felbontsa. Ezáltal a felbontás kísérlete lehet befejezett megszerzés is. A kifürkészés akkor minősül befejezettnek, ha a tettes a közlemény lényegi tartalmát megismeri. Kísérletnek számít a lehallgató készülék távközlési berendezésre történő rácsatlakozása, valamint a technikai okok miatt kudarcot vallott lehallgatási kísérletek is.

Tettese bárki lehet, az is, akire a küldeményt jogszerűen rábízták, vagy a távközlési berendezést jogszerűen kezeli.

3.4. Minősített esetek

Amennyiben a cselekményt a tettes a foglalkozásával vagy köz megbízatásának felhasználásával követi el, az minősített esetnek számít. Ebben az esetben a foglalkozás nem korlátozódik kizárólag az elkövető saját foglalkozására, például egy szomszéd, aki a postást arra készíti, hogy egy levelet átadjon a tartalmának megismerése céljából, szintén ide tartozik. További minősítő körülmény, ha a cselekmény jelentős érdeksérelemmet okoz. Ebben az összefüggésben a Btk. 9. szakasza alapján a tettes gondatlansága is elegendő ahhoz, hogy a jelentős érdeksérelem kritériuma teljesüljön.

⁸⁷⁴ Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények" p.456.

⁸⁷⁵ Btk. 459. § (1) bekezdés 15. pont

3.5. Jogellenesség hiánya

A levéltitok megsértésével kapcsolatban figyelembe kell venni bizonyos, a jogellenességet kizáró körülményeket is. Ilyen esetekben - ha a sértett kifejezetten beleegyezett az őt érintő információk megismerésébe vagy azok továbbításába - a levéltitok megsértése nem minősül bűncselekménynek. Emellett a jogellenesség kizárására lehetőséget ad, ha a jogszabályok kifejezetten engedélyezik vagy előírják az adott információk megosztását vagy nyilvánosságra hozatalát.⁸⁷⁶

3.6. Bűncselekményi egység és a bűncselekmények találkozása

A levéltitok megsértése egy alárendelt jogi tényállás, amely csak abban az esetben alkalmazható, ha az adott cselekménnyel nem következik be súlyosabb bűncselekmény, mint például tiltott adatszerzés, minősített adatokkal való visszaélés, jogosulatlan titkos információgyűjtés vagy gazdasági titok megsértése. Egy levéltitok megsértése eszközcselekményként is megvalósulhat, például okirattal visszaélés esetén, ha az okirat megszerzése zárt küldeményből történt. Amennyiben a levéltitok megsértéséből származó információk felhasználásával később más bűncselekmények következnek be, mint magántitok megsértése, rágalmozás vagy becsületsértés, ekkor a bűncselekmények között valóságos anyagi halmazat jön létre. Azonban egy jelentős érdeksérelem esetén a minősítő körülmény csak egyszer vehető figyelembe. A levéltitok megsértése csak magánindítványra büntethető a Btk. 231.szakasa (2) bekezdés alapján.

4. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

Az informatikai bűncselekmények saját fejezetet kaptak a Büntető Törvénykönyvben, az Európai Unió 2013/40 irányelvének⁸⁷⁷ megfelelően, amely az információs rendszerek elleni támadásokkal foglalkozik. Az irányelv átültetése révén a jogszabályok megújultak, a korábbi „számítástechnikai rendszer” fogalom helyett az „információs rendszer” terminológiát használja a Kódex. Háttérként érvényesül még az Európai Tanács 2004. évi LXXIX. törvénnyel kihirdetett ún. Budapesti Egyezménye. Szathmáry véleménye szerint szükséges az adat- és információbiztonsági jogforrások, mint mögöttes normaanyagok alkalmazása is. Ilyen jogforrás

⁸⁷⁶ Be. 43. § (2), 200–206/A. §

⁸⁷⁷ Európai Parlament és a Tanács.(2013.) " 2013/40/EU Irányelve(2013. augusztus 12.): Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról." *Hivatalos Lap L 218* (2013. augusztus 14.):pp. 8-14.

például a hálózati és információs rendszerek biztonságának egységesen magas uniós szintjét előíró (EU) 2016/1148 irányelv, továbbá az ezt kiegészítő, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) és annak végrehajtási rendeletei.⁸⁷⁸

A Btk. külön fejezetben, a Tiltott adatszerzés és információs rendszer elleni bűncselekmények (XLIII. fejezet) címszó alatt foglalkozik az információs rendszerek elleni támadásokkal, többek között a tiltott adatszerzés (422. §), az információs rendszer vagy adat megsértése (423. §), valamint az információs rendszer védelmét biztosító technikai intézkedések kijátszása (424. §) bűncselekményeivel. Emellett a vagyon elleni bűncselekmények között önálló tényállásként kezeli az információs rendszer felhasználásával elkövetett csalást (375. §).

Az alábbiakban ezeket a tényállásokat ismertetem.

4.1. Tiltott adatszerzés

422. § (1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,*

b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történeteket technikai eszköz alkalmazásával titokban megfigyeli vagy rögzíti,*

c) más postai küldeményét vagy egyéb zárt küldeményét titokban felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,*

d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti,*

e) információs rendszerben kezelt adatokat titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti, (...)*

422/A. § (1) Aki pilóta nélküli légi jármű jogosulatlan használatával más lakását, egyéb helyiségét, vagy ezekhez tartozó bekerített helyet megfigyeli és az ott történeteket rögzíti, ha más bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.

A Büntető Törvénykönyv 422. szakasza alapján a tiltott adatszerzés bűncselekménye magában foglalja a személyes adatok, magántitkok, gazdasági vagy üzleti titkok jogellenes megismerését célzó jogosulatlan tevékenységeket. E bűncselekmény elkövetője az a személy, aki titokban

⁸⁷⁸ Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I., *Infokommunikáció és Jog*, 2022/2. (79.), pp. 6-10

átkutatja mások lakását, helyiségét vagy azokhoz tartozó területet, technikai eszköz segítségével megfigyeli, rögzíti az ott történeteket, felbontja vagy megszerzi más zárt küldeményét, rögzítve annak tartalmát, vagy elektronikus hírközlő hálózaton keresztül továbbított vagy tárolt adatokat kifürkész, majd ezeket rögzíti. A bűncselekmény során tehát személyes adatok, magán-és levéltitok és gazdasági titkok jogellenes átkutatása, megfigyelése vagy levél felbontása révén történő jogosulatlan megismerése áll a középpontban. Az elkövetési módszerek között szerepel az otthoni magánéletbe való beavatkozás, zárt küldemények jogellenes felbontása, valamint az információs technológiák alkalmazásával történő adatgyűjtés.

4.1.1. A bűncselekmény jogi tárgya: a személyes adat, magántitok, gazdasági titok, üzleti titok védelme.

4.1.2. Elkövetési tárgy és magatartás

Elkövetési tárgyai másnak a lakása (Btk. 221. §), a közlést tartalmazó zárt küldeménye (Btk. 224. §), illetőleg az elektronikus hírközlő hálózat (Btk. 459. § (1) bekezdés 21. pont c).⁸⁷⁹ A Btk. az elkövetési magatartások között olyan titkos módszereket és eszközöket sorol fel, amelyeket a bűnüldöző hatóságok jogszerű eljárásuk során csak bírói vagy az igazságügyért felelős miniszter által kiadott engedéllyel használhatnak fel, mint például a titkos adatszerzés vagy titkos információgyűjtés.⁸⁸⁰

Az első alapeset közül elkövetési magatartásai, a titkos helyiségek átkutatása, technikai eszközökkel történő megfigyelés, zárt küldemények jogosulatlan felbontása, elektronikus hírközlő hálózatokon és információs rendszereken továbbított adatok jogosulatlan kifürkészése és rögzítése.

A második alapesetnél a célzat kiemelt jelentőségű. A bűncselekmény második alapesete a fedett nyomozók, illetve bűnüldöző hatóságokkal vagy titkosszolgálattal titkosan együttműködő személyek kilétüknek vagy tevékenységüknek felderítése céljából történő információgyűjtésre irányul.⁸⁸¹ Ebben az esetben a törvény célja ezeknek a személyeknek a

⁸⁷⁹ Karsai, Krisztina. "Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerkesztette Karsai, Krisztina, 989-996. Budapest, Magyarország: Wolters Kluwer, 2019. p.911

⁸⁸⁰ Ibid., p. 911.

⁸⁸¹ E munkakörbe tartozó személyek kiválasztása és foglalkoztatása a Be. 222. §, valamint a Rendőrségi törvény (Rtv.) 68/F. § alapján történik, amelyek meghatározzák a fedett nyomozók jogállását, feladatait és a velük szemben támasztott követelményeket.

védelme, akik különleges, rejtett módszerekkel vesznek részt a nyomozásban. A bűncselekmény immateriális jellegű, ami azt jelenti, hogy maga a cselekmény anyagi kárt nem okoz közvetlenül, de a bűnüldözési tevékenység sikerességét veszélyezteti. A bűncselekmény már akkor megvalósul, amikor az elkövető megkezdte a fedett nyomozók vagy együttműködő személyek kilétének vagy tevékenységének felderítésére irányuló tevékenységét, még akkor is, ha ez a felderítés nem vezet konkrét eredményre.

A bűncselekmény harmadik alapesete azonosított személyes adatok, magántitkok, üzleti vagy gazdasági titkok jogosulatlan továbbítására vagy felhasználására összpontosít. Itt a hangsúly azokon az információkon van, amelyeket az elkövető birtokol vagy amelyekhez valamilyen módon hozzájutott, és ezeket az információkat illetéktelenül használja fel vagy osztja meg harmadik felekkel. A cselekmény magában foglalhatja az adatok digitális vagy fizikai formában történő továbbítását, valamint az információk különböző célokra történő felhasználását, például gazdasági előnyök elérését vagy mások kárára történő felhasználást.

4.1.3. Tettesség

A bűncselekmény elkövethető bárki által, aki nem hivatalos személy. Ez azt jelenti, hogy az átlagemberek, vállalati alkalmazottak vagy bármely más, nem hivatalos funkcióban tevékenykedő személyek beletartoznak ebbe a kategóriába, amennyiben jogosulatlanul továbbítják vagy használják fel a megismert személyes, magán, üzleti vagy gazdasági titkokat. Hivatalos személyek, például állami alkalmazottak vagy köztisztviselők esetében, ha hasonló magatartást követnek el, az a jogosulatlan titkos információgyűjtés vagy adatszerzés külön bűncselekményeként szabályozott, szigorúbb szankciókkal. (Btk.307) A bűncselekmény kizárólag szándékosan követhető el.

4.1.4 Minősített esetek

A bűncselekmény minősített esetei azokat a helyzeteket jelölik, ahol az alapbűncselekményt bizonyos körülmények között, vagy különleges módszerekkel követik el. Ezek a hivatalos eljárás színlelésével, üzletszerűen, bünszövetségben jelentős érdeksérelem okozva történt elkövetés.

A cselekmény súlyosabb büntetést von maga után, ha az okozott kár vagy érdeksérelem jelentős. Ez a kategória magában foglalhatja a jelentős anyagi károkat, a célszemélyek vagy szervezetek üzleti tevékenységének komoly zavarását, vagy olyan személyes adatok jogosulatlan felhasználását, amelyek súlyosan befolyásolják az érintettek életét.

422/A. § (1) bekezdése szerint a pilóta nélküli járművek által történő kifürkészés is tiltott adatszerzés. A jogalkotó, a drónok által nyújtott új technológiai lehetőségekre és a magánélet

védelmének kihívásaira válaszul, ezt a tevékenységet tiltott adatszerzésnek minősítette, ennek nem tényállási eleme azonban a titkosság.

A tiltott adatszerzés bűncselekményének elkövetési magatartásai súlyosan sértik az érintettek személyes adatokhoz és magánélethez való jogait, valamint fenyegetést jelentenek az adatbiztonságra és az információs rendszerek integritására.⁸⁸²

4.2. Információs rendszer vagy adat megsértése

„423. §* (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

büntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3)* A büntetés büntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint, vagy jelentős érdeksérelmet okoz.

(4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”

4.2.1. A bűncselekmény jogi és elkövetési tárgya

Jogi Tárgy: az információs rendszerek zavartalan működése, valamint az abban tárolt adatok hitelessége és bizalmas jellegének megőrzése. Az "adat" fogalmát a tényállás, Szathmáry szerint a Btk. „megszorító” értelmezésének tartja, - különösen a „hacking” viszonylatában, a Btk. 375. szakaszában meghatározott tényállás miatt, amely részben magában foglalja a

⁸⁸² Molnár Gábor. (2016) "XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In *Magyar Büntetőjog - Kommentár a gyakorlat számára (Harmadik kiadás)*, szerk. Kónya Sándor. Budapest: HVG-ORAC.

„hackinget” mint eszközcselekményt.⁸⁸³ Tipikusan a DDoS- és a malware-támadások az információs rendszer vagy adat megsértése körébe tartozó cselekmények.

Elkövetési tárgy: az információs rendszer maga, beleértve annak minden részét és a benne tárolt adatokat. A cselekmény elkövetési tárgyát illetően Nagy elkülöníti egymástól az egyes számítógépet, illetve az informatikai rendszert, valamint a számítógépes programokat és elektronikus adatokat.⁸⁸⁴ Az elektronikus adatok fogalma a digitális bizonyítékok fogalmának megfeleltethető, annak megfelelően határozza meg azt a büntetőeljárásról szóló törvény is.⁸⁸⁵

4.2.2. Elkövetési magatartások

Jogosulatlan belépés, az információs rendszerbe történő jogosulatlan belepéssel, vagy keretet túllépve a rendszerben maradással történhet. Jogosulatlan akadályozás, az információs rendszer működésének akadályozása, amely nem kötődik konkrét elkövetési cselekményhez, hanem az eredményre - a működés zavarására összpontosít. Tipikusan a hacking, DDoS- és a malware-támadások az információs rendszer vagy adat megsértése körébe tartozó cselekmények.⁸⁸⁶

Adatintegritás sértése, az információs rendszerben tárolt adatok jogosulatlan megváltoztatásával történhet. Ennek jogi tárgya, kiegészül, az az adatok tartalmától függően azok által képviselt értékkel.⁸⁸⁷

A jogosulatlan belépés esetével kapcsolatban 2017-ben a Kúria egy bűnügyi technikus esetét vizsgálta, aki a rendőrség "Robotzsaru Neo" adatfeldolgozó rendszerében hivatalos jogosultsággal lépett be, de jogosultságain túllépve kétszer keresett különböző bűncselekményekkel kapcsolatos személyekre, ezzel megsértve az adatkezelési szabályokat.⁸⁸⁸

A másodfokú bíróság megállapította, hogy a vádlott túllépte jogosultságait, de a Kúria és az elsőfokú bíróság felmentette, mert az információs rendszer megsértése csak védelmi intézkedések megsértésével vagy kijátszásával minősült volna bűncselekménynek. Grund szerint a bírói döntések közötti eltérés abból adódott, hogy a jogalkotó nem választotta külön a jogosulatlan belépés, illetve a belépési jogosultság kereteit túllépő vagy megsértő bennmaradás

⁸⁸³ Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.

⁸⁸⁴ Nagy Zoltán. "A kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor. Budapest: Dialóg Campus, 2020.p.51.

⁸⁸⁵ Máté István Zsolt. (2018). "Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe." *Belügyi Szemle*, 2018, 66, (7-8), pp. 36-54.

⁸⁸⁶ Nagy Zoltán. "A kiberbűncselekmények szabályozása."p.51.

⁸⁸⁷ Nagy, Zoltán András. "A számítógépes környezetben elkövetett bűncselekmények új szabályozásáról. Háttér és elemzés." *Ügyészek Lapja*, 2014/3-4. sz., p.32.

⁸⁸⁸ Kúria BHAR.I.537/2017/5. sz. határozata és BH2017. 392.

elkövetési magatartásokat. ehelyett e két elkövetési magatartást egyetlen mondatban, technikai intézkedések megsértését vagy kijátszását követően vesszővel elválasztva fogalmazta meg. A másodfokú bíróság arra alapította döntését, miszerint a vádlott túllépte jogosultságainak kereteit, így a rendszerben maradt, de nem tartotta lényegesnek annak vizsgálatát, hogy a vádlott sértett-e vagy kijátszott-e valamilyen védelmi intézkedést, hivatkozva egy 2014-es, hasonló ügyben hozott kúriai döntésre. Amennyiben e cselekmények két külön pont alá kerülnének, egyértelművé válna, hogy mindkét elkövetési magatartás megállapíthatóságához szükséges-e a tényállás első tagmondatában szereplő elkövetési mód, vagy az csupán az első fordulatra vonatkozik.⁸⁸⁹

Az elkövető bárki lehet, aki szándékosan hajtja végre a fent említett magatartások valamelyikét. A bűncselekmény nem követel meg speciális státuszt vagy hivatalos pozíciót.

A jogosulatlan belépés akkor tényállásszerű, ha a rendszer biztonsági megoldásokkal védett, és a védelem aktív, azaz szükséges legyen a belépéshez jelszavak, kódok, más azonosítók használata a hálózat eléréséhez.⁸⁹⁰ Ezek konjunktív feltételek.

Az információs rendszer akadályoztatása kapcsán a törvény az elkövetési módokat nyitva hagyja, így a tényállás nem korlátozódik csak az informatikai műveletekre, úgy, mint adatbevitel vagy törlés, hanem magában foglalhatja a rendszer működését akadályozó bármilyen behatást is, például egy szerverszoba hűtőrendszerének megrongálását. A törvényi szöveg nyitottsága azt is felveti, hogy milyen esetek minősülnek akadályozásként: csak azok, ahol a rendszer működésképtelensége a rendszeren belüli hiba miatt következik be, vagy bármely helyzet, amikor az információs rendszer nem képes az elvárt funkció ellátására, függetlenül attól, hogy üzemzavar vagy hiba áll-e fenn.⁸⁹¹

A megkülönböztetés jelentősége akkor válik érzékelhetővé, ha az információs rendszeren kívüli eseményeket vizsgáljuk, mint például egy szenzor által mért környezeti adatok manipulálása. Amennyiben a szenzor feladata az információk elektronikus adattá konvertálása és azoknak az információs rendszerbe történő bevitelére szolgál, a cselekmény nem feltétlenül valósít meg bűncselekményt a jogszabály b) pontja szerint, mivel az adatbevitel nem része a tényállásnak, tehát a valóságtól eltérő adat bevitelének ténye irreleváns. Azonban az a) pont szerint az adatbevitel tényállásszerű lehet, különösen, ha a szenzor nem képes a környezet érzékelésére

⁸⁸⁹ Grund, Borbála.(2021) "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról." p.15.

⁸⁹⁰ Nagy Zoltán. "A kiberbűncselekmények szabályozása." p. 51.

⁸⁹¹ Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.

és ennek következtében az adatbevitelre, ebben az esetben a rendszer működésének akadályozása kérdéses lehet.⁸⁹²

Szűk értelmezésben a rendszer működése akkor tekinthető akadályozottnak, ha az információs rendszer funkciói vagy a benne kezelt adatok a jogosultak számára hozzáférhetetlenek, vagy csak korlátozottan érhetőek el. Az akadályoztatás csak akkor állapítható meg, ha az számottevő hatással bír a rendszer működésére, beleértve azokat az eseteket is, amikor a rendszer üzemeltetője a további adatfeldolgozási feladatait nem, vagy csak jelentős többletráfordítással tudja ellátni.⁸⁹³

A b) pont szerint az elkövetési magatartások közé tartozik az adatok megváltoztatása, törlése vagy hozzáférhetetlenné tétele. Az adatok megváltoztatása azt jelenti, hogy az adat tartalmát technikai eszközökkel módosítják, így az eredeti információ tartalma változik meg.

Az adatok törlése esetén az adat eltávolításra kerül a rendszerből, gyakorlatilag megsemmisül, ami azt jelenti, hogy visszaállítása lehetetlen. A törölt adatnak azonban nem csak a fizikailag törlődött állapotát kell érteni alatta, hanem azt is, amikor az adatot csak különleges szakértelemmel és eljárásokkal lehet helyreállítani. Az ilyen típusú elkövetési magatartás jogosulatlan programmanipulációkat foglal magában, amelyek az adatok megváltoztatását vagy a program lefutásának módosítását eredményezhetik. A törvény értelmében már egyetlen adat törlésével is megvalósulhat a bűncselekmény.

Ha az adat módosítása vagy törlése a számítástechnikai rendszer működésének akadályozását eredményezi, akkor a (2) bekezdés a) pontja alapján is megvalósulhat a cselekmény. Azonban az alaki halmazat feloldása érdekében fontos az adat jellegének megvizsgálása. Ha az adat a rendszer szabályos működését szolgálja, mint például egy programrész, akkor az a) pont szerinti magatartás valósul meg. Ha viszont az adat tartalmának van jelentősége, mint például egy dokumentum törlése, és ez nem befolyásolja a rendszer működését, akkor a b) pont szerinti eset áll fenn.⁸⁹⁴

A Btk. 423. § (2) bekezdés a) pontja - az információs rendszer működésének jogosulatlan vagy jogosultság kereteit megsértő akadályozása az Irányelv 4. cikkének, mint „rendszert érintő jogellenes beavatkozás”, a bekezdés b) pontja - az adat jogosulatlan, vagy jogosultság kereteit

⁸⁹² Ibid.,

⁸⁹³ Szabó I. 2008. "Informatikai bűncselekmények."p.612.

⁸⁹⁴ Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.

megsértő törlése, vagy hozzáférhetetlenné tétele az Irányelv 5. cikkének mint „adatot érintő jogellenes beavatkozás” a magyar szabályozásba történő átültetésének feleltethető meg.⁸⁹⁵

Az adatok hozzáférhetetlenné tétele akkor következik be, amikor a jogosult személy nem tud hozzáférni az adatokhoz, nem képes azokon műveletet végezni, vagy az általuk hordozott információkat használni. Ez történhet az adatok titkosításával, áthelyezésével vagy a hozzáférés technológiai úton történő megtagadásával, például ransomware által. Ebben az esetben az adatok megmaradnak, de a jogosult nem fér hozzá az adatokhoz.

Egyetértve Szathmáry felvetéseivel, a „fizikai külső” tényezők biztosítását, és az informatikai rendszer működőképességének biztosítását is szükségesnek tartom. Az Infotv. az adatbiztonsági intézkedések között a 25/I §. (1) pontja alapján az adatkezelő vagy az adatfeldolgozó megfelelő „műszaki és szervezési intézkedéseket tesz.” Biztosítja „*az adathordozók (...) eltávolításának megakadályozását,*[Infotv. 25/I.L.(3)b)] valamint hogy „*üzemzavar esetén az adatkezelő rendszer helyreállítható legyen*”[Infotv. 25/I.L.(3)i)] „*valamint azt, hogy az adatkezelő rendszer működőképes legyen*”[Infotv. 25/I.L.(3)j)]. Mindezek alapján a fizikai tényezők által, és a rendszer működésének egyéb módon történő akadályoztatásait is a tényállás részeinek kellene tekinteni.

Jelenleg a számítógépes rendszerek mechanikus - technikai védelmét ez tényállás nem tartalmazza, azt a rongálás törvényi tényállása adja.⁸⁹⁶

4.2.3 Minősített esetek

Ha a cselekmény jelentős számú információs rendszert érint, és jelentő érdeksérelem következik be, vagy ha bűncselekmény egy közérdekű üzem információs rendszerét érinti.⁸⁹⁷

4.2.4 Rendbeliség

A bűncselekmény rendbelisége, vagyis a büntetési tételek súlyossága, az érintett információs rendszerek számától függően változhat, ami azt jelenti, hogy minél több rendszert érint a cselekmény, annál súlyosabb lehet a büntetési tétel.

⁸⁹⁵ Grund, Borbála. "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról." p.15.

⁸⁹⁶ Molnár Gábor (2016). "XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In Kónya Sándor (szerk.), *Magyar büntetőjog – Kommentár a gyakorlat számára*. Budapest: HVG-ORAC, 971–972. p.946

⁸⁹⁷ Btk. 459. § (1) bekezdés 21. Közérdekű üzem a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek, a hadianyagot, haditechnikai eszközt termelő üzemet, energiát vagy üzemi felhasználásra szánt alapanyagot termelő üzem

4.3. Információs rendszer védelmét biztosító technikai intézkedés kijátszása

424. § (1) Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerz, vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja,

véség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

(3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.

4.3.1. A bűncselekmény tárgya

Jogi tárgy: Az információs rendszerek zavartalan működéséhez, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint titokban maradásához fűződő érdek.

Elkövetési tárgy: A 375.§ vagy a 423.§ szerinti - a károkozó adatvisszaélés, a tiltott adathalászat egy formája - bűncselekmények elkövetését elősegítő vagy lehetővé tevő eszközök és ismeretek, mint például jelszavak, kódok, számítástechnikai programok, valamint az ezek készítéséhez szükséges szakmai tudás, és nem maguk a felsorolt eszközök.

4.3.2 Elkövetési magatartás

Jelszavak vagy számítástechnikai programok készítése, átadása, hozzáférhetővé tétele, megszerzése, vagy forgalomba hozatala, jelszó vagy számítástechnikai program készítéséhez szükséges gazdasági, műszaki, szervezési ismeretek más személyek rendelkezésére bocsátása. A bűncselekmény alanya bárki lehet, aki szándékosan vesz részt a fenti tevékenységekben. Ez magában foglalja azokat is, akik közvetlenül nem követnek el információs rendszer elleni bűncselekményt, de tevékenységükkel hozzájárulnak annak előkészítéséhez. Azonban csak azokat a személyeket lehet a b) pont szerinti büntetni, akik rendelkeznek az adott szakmai ismeretekkel, úgy mint jelszó vagy számítástechnikai program készítésére vonatkozó

gazdasági, műszaki, szervezési ismeretek. A bűncselekmény elkövetője bárki lehet függetlenül attól, hogy rendelkezik-e szakmai ismeretekkel vagy milyen szintű tudása van. Büntetésmegállapítás során azonban jelentőséget kaphat, és súlyosbító tényezőként értékelhető, ha a vádlott rendelkezik számítástechnikai képesítéssel, vagy ha ilyen területen, például számítástechnikai cég vagy szerviz alkalmazottjaként dolgozik.⁸⁹⁸

Az (1) bekezdés szerinti bűncselekmény olyan elkövetési magatartással teljesedik ki, amely magában foglalja a programok írását, belépési kódok és jelszavak generálását, ezek megszerzését, forgalomba hozatalát, kereskedelmét és hozzáférhetővé tételét. A bűncselekmény ezen formája befejezettnek minősül anélkül, hogy a 375. § vagy a 423. § szerinti cselekmények kísérleti szakaszba jutnának. A (2) bekezdés szerint a gazdasági, műszaki, szervezési ismeretek más személy számára történő rendelkezésre bocsátásával a bűncselekmény szintén befejezetté válik. Nem követelmény, hogy ezeket az ismereteket az illető személy programok írására, belépési kódok vagy jelszavak generálására használja fel.⁸⁹⁹

Minősített esetek: (3) bekezdése szerint az információs rendszer megsértése akkor minősül súlyosabb bűncselekménynek, ha a cselekmény jelentős számú rendszert érint. A "jelentős szám" nem csak kvantitatív értékelést jelent, hanem magában foglalja azokat a tevékenységeket is, mint a botnet-ek létrehozása vagy zsarolóvírusok terjesztése, amelyek miatt ez a minősítés szükséges. Kísérletnek számít, ha a tevékenység célja például botnet létrehozása, de jelentős számú rendszer fertőzése nem következik be.⁹⁰⁰ Befejezett a bűncselekmény az elkövetési magatartások bármelyikének tanúsításával. A bűncselekmény elkövetője tettesként bárki lehet.⁹⁰¹

.4.3.3.Rendbeliség

A bűncselekmény súlyosságát és a kapcsolódó büntetési tételeket az érintett információs rendszerek száma befolyásolja.

A törvényi tényállás megköveteli a cselekmény célzatos voltát, azaz hogy az elkövető szándéka az legyen, hogy ő maga vagy egy másik személy elkövesse a 375.§ vagy a 423. §-ban meghatározott bűncselekményt, ami hangsúlyozza a szándékos és célzott előkészítő tevékenységek büntethetőségét. Ugyanakkor nem büntethető az, aki program, jelszó, adat

⁸⁹⁸ Nagy Zoltán. "A kiberbűncselekmények szabályozása." p.56.

⁸⁹⁹ Ibid.,p. 56

⁹⁰⁰ Szathmáry Zoltán: (2023) "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése II.", *Infokommunikáció és Jog*, 2023/1. (80.), pp. 11-13.

⁹⁰¹ Karsai, Krisztina. "Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." p. 918.

készítő tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

4.4. Az információs rendszer felhasználásával elkövetett csalás

A vagyon elleni bűncselekményekről szóló XXXVI. fejezetben a 375. § alatt szerepel az információs rendszer felhasználásával elkövetett csalás ún. károkozó adatvisszaélés, és a készpénz-helyettesítési fizetési eszközzel visszaélés egyes alakzatainak összevonásával jött létre.⁹⁰²

375. § (1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, büntetett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

- a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy*
- b) a nagyobb kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.*

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

- a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy*
- b) a jelentős kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.*

(4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha

- a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy*
- b) a különösen nagy kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.*

(5) Az (1)–(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.

⁹⁰² Szomora, Zsolt.(2019) "A vagyon elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerkesztette Karsai, Krisztina, Budapest, Magyarország: Wolters Kluwer, p.810.

(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.”

4.4.1. Jogi tárgy és a tényállás szerkezete

A 375. § által védett jogi érdek az információs rendszerekkel és az elektronikus készpénz-helyettesítő fizetési eszközökkel történő fizetési műveletek során érintett vagyoni jogok biztonsága. A jogi tárgy ebben az esetben egyaránt magában foglalja a csalás és a lopás jogi elemeit, mivel az információs rendszerek zavartalan működéséhez kapcsolódó társadalmi érdekeket, valamint a vagyoni és tulajdoni jogokat is védi. Ennek fényében, figyelemmel a jogi tárgy kettős jellegére, e bűncselekmény nem minősül sem szabálysértésnek, sem vétségnek, hanem értékhatártól függetlenül bűncselekménynek tekinthető.⁹⁰³

A tényállás szerkezete szerint a bűncselekmény két fő alakzatot különböztet meg.

Az egyik a károkozó adatvisszaélés,⁹⁰⁴ ami az információs rendszerbe jogtalanul bevitelt, a rendszerben kezelt adatok jogosulatlan módosítását, törlését, vagy hozzáférhetetlenné tételét, valamint az információs rendszer működésének egyéb módon való befolyásolását foglalja magában, amennyiben ezek a cselekmények jogtalan haszonszerzés céljából kárt okoznak.

A másik, az elektronikus készpénz-helyettesítő fizetési eszközzel visszaélés.⁹⁰⁵ Ez magában foglalja a hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszközök használatát vagy az ilyen eszközökkel történő fizetés elfogadását, amennyiben ez kárt okoz.⁹⁰⁶

4.4.2 Elkövetési tárgy

Az információs rendszer vagy annak bármely eleme, valamint az információs rendszer szempontjából releváns adat.⁹⁰⁷

4.4.3 A bűncselekményi alakzat elkövetési magatartásai

Magukban foglalják az adatok jogosulatlan bevitelét a rendszerbe, az információs rendszerben tárolt adatok módosítását, törlését vagy hozzáférhetetlenné tételét, illetve bármely más olyan

⁹⁰³ Ambrus István.(2021) "Vagyon elleni kriminális cselekmények a modernizálódó kiskereskedelemben." *Ügyészek Lapja* 27, no. 1-2 ISSN 1217-7059.

⁹⁰⁴ Btk. 375. § (1)–(4) bekezdés

⁹⁰⁵ Btk. 375. § (5)–(6)

⁹⁰⁶ Tóth Dávid. (2019). "A virtuális pénzekkel kapcsolatos visszaélések." In: Baráth Emőke Noémi – Mezei József (szerk.): *Rendészet-Tudomány-Aktualitások. A rendészettudomány a fiatal kutatók szemével.* Budapest: Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, pp. 242-250.

⁹⁰⁷ Btk. 459. § (1) bekezdés 15.

tevékenységet, amely az információs rendszer működését befolyásolja. Az adatbevitel azt jelenti, hogy az információs rendszerbe új adatot visznek be, míg az adat megváltoztatása a meglévő adatok tartalmának vagy formátumának módosítását foglalja magában. A törlés az adatok megsemmisítésére, míg a hozzáférhetetlenné tétel az adatok ideiglenes vagy végleges elrejtésére utal, megakadályozva, hogy a jogosult felhasználók hozzáférjenek hozzájuk. Ezek a tevékenységek minden esetben befolyásolják az információs rendszer működését, amit a jogalkotó szándékosan széles körűen értelmez, beleértve minden olyan cselekedetet, amely befolyásolhatja a rendszer működését.

A bűncselekmény megvalósításához kár bekövetkezése szükséges, ami az említett tevékenységek következtében az információs rendszerben vagy a rendszer által kezelt vagyontárgyakban keletkezhet. A károkozó adatvisszaélés bűncselekménye szándékosan, jogtalan haszonszerzési szándékkal követhető el, ahol a károkozás szándéka kiterjedhet a közvetlenül előidézett kárra, illetve annak mértékére is.⁹⁰⁸

Ez a tényállás kiegészíti a hagyományos csalás bűncselekményét, lehetővé téve, hogy az információs rendszerek útján elkövetett vagyoni károkozást, amely nem jár természetes személyek megtévesztésével, büntetőjogilag szankcionálják.

4.4.4. Stádiumok

A bűncselekmény akkor tekinthető befejezettnek, amikor a kár bekövetkezik. A kísérleti szakasz a cselekmény megkezdésével veszi kezdetét, még ha a kártékony hatás elmarad is. Mivel a károkozó adatvisszaélés egyes elkövetési magatartásai átfedésben lehetnek az információs rendszer vagy adat megsértésével (Btk. 423. §), így a károkozó adatvisszaélés kísérleti szakasza magában foglalhatja a 423. szakasz szerinti bűncselekmény befejezett alakzatát is, legalábbis az objektív tényállás szempontjából. A két bűncselekmény közötti különbségtétel a tettes jogtalan haszonszerzésre irányuló szándékában rejlik: ha ez a szándék fennáll, akkor a 423. szakasza helyett az információs rendszer felhasználásával elkövetett csalás kísérletét kell megállapítani.⁹⁰⁹

4.4.5 Tettesség

A bűncselekmény elkövetője bárki lehet, legyen szó a rendszer külső támadójáról vagy a rendszer kezeléséért felelős belső személyről. A modern távközlési technológiák és az internet térhódításával a bűncselekmény elkövetésének helye is változóvá vált, amely lehet a

⁹⁰⁸ Szomora, Zsolt. "A vagyon elleni bűncselekmények." p 811.

⁹⁰⁹ Ibid., 811.o

cselekmény megvalósulásának helye (pl. a terminál vagy szerver fizikai helye) vagy a bekövetkezett kár helye, mindkettő megalapozhatja a magyar Btk. területi hatályát.⁹¹⁰

4.4.6 Minősített esetek

A bűncselekmény súlyosságát a kár nagysága és az elkövetés módja (bűnszövetségben vagy üzletszerűen történő elkövetés) határozza meg. A jelentős kárt okozó esetektől kezdődően a bűncselekmény súlyosabban minősül, ami a Btk. 375. § (2)–(4) bekezdéseiben kerül meghatározásra. A bűncselekménynek nincs enyhébb, szabálysértési formája: már csekély kár esetén is bűncselekménynek minősül.

4.4.7. Bűncselekményi egység és a bűncselekmények találkozása

A károkozó adatvisszaélés bűncselekményének rendbelisége, azaz a büntetési tétel meghatározása, az érintett sértettek számától függ. Ez azt jelenti, hogy a bűncselekmény súlyosságát a károsított vagyoni jogok jogosultjainak száma alapján kell értékelni. Fontos kiemelni, hogy a nem védett hálózatokon keresztül történő illetéktelen internet-hozzáférés, gyakran „wifi-lopásnak” nevezett tevékenység, nem esik bele a Btk. 375. szakasza(1) bekezdése által meghatározott bűncselekmény kategóriájába, tehát nem minősül bűncselekménynek.⁹¹¹

4.4.8. Elektronikus készpénz-helyettesítő fizetőeszközzel való visszaéléssel megvalósuló alakzat

A Btk. 375. § (5) bekezdése szerint a tényállás elemei megvalósulnak akkor is, ha hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt. Ez a bűncselekmény különösen az elektronikus készpénz-helyettesítő fizetési eszközöket érinti⁹¹². A külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszközök ugyanolyan védelmet élveznek, mint a belföldön kibocsátottak, tehát a bűncselekmény megállapításában a kártya kibocsátásának helye nem játszik szerepet.⁹¹³

Az elkövetési tárgy magában foglalhatja a hamisított, hamis, vagy jogosulatlanul megszerzett valódi elektronikus készpénz-helyettesítő fizetési eszközöket. A "jogosulatlanul megszerzett valódi" kifejezés olyan eszközökre utal, amelyek a tettes birtokába jogellenes módon kerültek, például lopás, csalás vagy jogtalan megtalálás révén.

⁹¹⁰ Btk. 3.§

⁹¹¹ Szomora, Zsolt. "A vagyon elleni bűncselekmények." p. 812.

⁹¹² Btk. 459. § (1) bekezdés 20.

⁹¹³ Btk. 375. § (6)

Ez a bűncselekményi alakzat tehát kifejezetten azokat a helyzeteket célozza meg, ahol az elektronikus fizetési eszközök jogellenes felhasználása által közvetlen vagyoni kárt okoznak, kihasználva az információs rendszerek adta lehetőségeket.

A bűncselekmény passzív alanya, vagyis a sértett általában az az (elektronikus) bankszámlatulajdonos, aki a számláján lévő összeg felett a készpénz-helyettesítő fizetési eszköz használatával rendelkezik. A károkozás jellege és a bekövetkezett kár függvényében a sértett lehet az érintett számlavezető pénzügyi intézmény vagy maga a fizetési eszközt kibocsátó szervezet is.

Az elkövetési magatartások közé tartozik a fizetési eszköz felhasználása és annak elfogadása. A felhasználás során a készpénz-helyettesítő fizetési eszközt a kibocsátás eredeti céljának megfelelően használják fel, például készpénzfelvételre vagy áruk, szolgáltatások fizetésére. Ez akkor is megvalósulhat, ha a tettes a fizetési eszközt a hozzá tartozó PIN-kóddal együtt szerezte meg, vagy érintéses fizetéskor, ahol bizonyos összeghatár alatt nem szükséges PIN-kód bevitel.⁹¹⁴

Az elektronikus készpénz-helyettesítő fizetési eszközzel való visszaélés bűncselekményének alapja a kár bekövetkezése. Ezen bűncselekmény befejeztként értékelhető, amikor a kár ténylegesen bekövetkezik. Azonban, ha a kísérleti cselekmény (pl. hamis bankkártya használata) eredménytelen marad, például az ATM azonnal visszautasítja a tranzakciót, akkor is szóba jöhet az alkalmatlan kísérlet fogalma.

A bűncselekmény elkövetője bárki lehet, beleértve azt is, aki tudatosan elfogadja a hamis fizetési eszközzel történő fizetést, különösen, ha a haszon megosztásáról előzetes megállapodás születik a felhasználóval. Amennyiben a fizetés elfogadója tudatában van a fizetési eszköz hamisságának, de mégis elfogadja azt, önálló tettesként azonosítható.

Fontos megjegyezni, hogy a bűncselekmény nem követel meg többszörös közreműködést; egyedüli elkövető esetén is megállapítható, még ha a fizetés elfogadója nem ismeri fel a fizetési

⁹¹⁴ A Btk. szerint ez a helyzet nem feltétlenül jelent bűncselekményt, ha a fizetési eszköz használata a jogosult által történik. Azonban, ha a tettes a fizetési eszközt jogosulatlanul használja fel, például jogosulatlanul megszerzett, hamis vagy hamisított eszközzel, akkor a Btk. 375. § (5) bekezdés szerinti bűncselekmény áll fenn. A fizetés elfogadása magában foglalhat hamis, hamisított vagy jogosulatlanul használt valódi fizetési eszközök elfogadását. Itt fontos megkülönböztetni, hogy ha a tettes jogszerűen birtokolja a fizetési eszközt (pl. a sértett megbízásából), de jogtalanul használja azt, a helyzet sikkasztásként (Btk. 372. §) értékelhető, nem pedig mint a Btk. 375. § (5) bekezdés szerinti bűncselekmény.

eszköz hamisságát. A bűncselekmény általában jogtalan haszonszerzési szándékkal követik el, de ez nem kötelező elem, így eshetőlegesen szándékkal is megvalósulhat.

A bűncselekmény minősített eseteinek rendszere a károkozó adatvisszaélésével azonos minősítési rendszerhez igazodik, ami a Btk. 375. szakasza (1)–(4) bekezdéseit követi. E bűncselekmény sajátossága, hogy nincs szabálysértési formája, és már egy forinttól is bűncselekménynek minősülhet, ami aránytalannak tűnhet.

A bűncselekmény rendbelisége az érintett sértettek, azaz a károsult bankszámla-tulajdonosok számától függ. Amennyiben konkrét bankszámla-tulajdonos nem állapítható meg, a pénzintézetek tekinthetők a tényleges károsultaknak, így a bűncselekmény súlyossága a sértettek számával arányos.

Az elektronikus készpénz-helyettesítő fizetési eszközzel való visszaélés bűncselekménye magában foglalhatja a készpénz-helyettesítő fizetési eszköz hamisítását is, ha az elkövető és a hamisító ugyanaz a személy. Ezenkívül, ha a fizetési eszköz használatával egyidejűleg több bűncselekmény is megvalósul, azok anyagi halmazatot alkothatnak, de a bűncselekmény megvalósulása magánindítványra is büntethető lehet bizonyos esetekben a Btk. rendelkezése alapján.

Az információbiztonság fogalma az információs rendszer definícióját szélesebb értelemben alkalmazza, mint azt a Büntető Törvénykönyv értelmező rendelkezése teszi. Az információbiztonság elleni cselekmények nem csak a közvetlenül védett információs rendszert érintik, hanem annak szélesebb környezetében, a rendszerelemeken keresztül is megvalósulhatnak. Az információs rendszer biztonságát közvetlenül érintő támadások tipikusan a Büntető Törvénykönyv 423. §-ában definiált tényállás alá esnek, míg a közvetett vagy előkészítő jellegű tevékenységek, mint például a social engineering vagy a jelszavak és egyéb azonosítók megszerzésére irányuló adathalászat, amelyek az információs rendszert kezelő személyeket célozzák, a Büntető Törvénykönyv 424. §-a szerint minősülhetnek.⁹¹⁵

A jelenleg hatályos Büntető Törvénykönyv szabályozása a személyes adatok védelme és az információs rendszerekkel kapcsolatos tényállások tekintetében összhangban áll az uniós jogi előírásokkal. Ezeket a kereteket az Általános Adatvédelmi Rendelet és a Bűnügyi Adatvédelmi Irányelv alapján az Infotv. határozza meg. A Btk. rendelkezik is az uniós jogszabályoknak való megfelelésről. Az egyes szabályozási kérdésekkel kapcsolatban ismertetem a szakirodalmi álláspontokat, különös tekintettel a személyes adatokkal való visszaélésre vonatkozó tényállásra. A bírói ítélezési gyakorlat döntő szerepet fog játszani az

⁹¹⁵ Szathmáry Zoltán: "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése II.

információs rendszer elleni bűncselekményekkel kapcsolatos pontos jogértelmezés kialakításában.

VII. Összefoglalás - Az eredmények bemutatása

A disszertáció bevezető részében az adatvédelem fogalmával kapcsolatos elméleti megfontolások, az adatvédelmi jog fejlődésének főbb állomásai, és a személyes adatok védelmének aktuális jogi szabályozása kerültek bemutatásra. Az értekezés további részeiben a 2016/680/EU irányelv - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv és jogharmonizációja bemutatása után, a bűnügyi célú adatkezelésekkel kapcsolatos probléma felvetés kapcsán bemutattam a nyomozás-, a vádeljárás-, a büntetés-végrehajtás jogszabályi hátterét, továbbá a személyes adatok védelméhez kapcsolódó büntetési szankciókat meghatározó kódexünk szabályozását is. A digitális térben elkövetett bűncselekmények és az adatvédelem közötti összefüggéseket részletesen elemeztem, különös hangsúlyt fektetve a személyes adatok védelmének jelentőségére.

1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése

A II. fejezetben az adatvédelem fogalmának és történetének rövid áttekintése után bemutattam a vonatkozó aktuális uniós szabályozást és annak intézményrendszerét. Az adatvédelem fogalmát illetően, annak gyakorlati szempontú megközelítését tartottam fontosnak, figyelembe véve az értekezés során vizsgált szempontokat.

Ennek megfelelően a személyes adatok védelme – véleményem szerint gyakorlati szempontból - nem más, mint, a természetes személyek jogainak és szabadságainak védelme a természetes személyek személyes adataihoz fűződő önrendelkezési jog gyakorlási körülményeinek meghatározása által, - valamint a természetes személyek személyes adatait kezelő adatkezelőkre vonatkozó adatkezelési feltételek szabályozása által.

Ennek értelmében mind az adatkezelő, mind az adatkezeléssel érintett természetes személy (továbbiakban: érintett) rendelkezési joggal bírnak az érintett személyes adatai felett. Míg az adatkezelő által történő rendelkezési jog jogszerűségét, másnéven jogalapját a vonatkozó szabályozásban, úgy, mint a GDPR-ban, valamint a LED-ben foglalt jogalapok valamelyike biztosítja, addig az érintett személyes adataival információs önrendelkezési joga keretében saját

maga rendelkezik. Azaz az adatkezelés feltételeit, a személyes adatok feletti rendelkezési jog gyakorlásának feltételeit az érintetten kívüli személyek, vagyis az adatkezelők vonatkozásában valamely „adatvédelmi” jogszabály vonatkozó rendelkezése határozza meg.

A rendelkezési jognak vannak korlátai mindkét irányból. Az adatkezelés mint fogalom maga is jogszabály által szabályozott rendelkezési jogosultság az érintett személyes adatai felett. [GDPR 4.cikk. 2.)] Az adatkezelő által végzett adatkezeléseknek, vagyis a személyes adatokon végrehajtott valamely műveleteknek vannak bizonyos korlátai. Ha elméleti síkon egy mérleg két serpenyőjébe helyeznénk az érintett személyes adatait érintő rendelkezési jogosultságokat adatkezelői, valamint érintett oldalról egyaránt, akkor általános következtetésként elmondható lenne, hogy a személyes adatokkal kapcsolatos rendelkezési jogosultságoknak több jogszabályi korlátja van adatkezelői oldalon, mint érintetti oldalon.

Ugyanakkor ettől függetlenül az érintett saját személyes adatai feletti önrendelkezési jogának is vannak egyéb korlátai, amelyek klasszikus értelemben nem az úgynevezett „adatvédelmi szabályozás” részét képezik, hanem egyéb jogi normák által és etikai elvek által meghatározottak. (pl. nem küldhetünk intim képet kiskorú személy részére saját magunkról).

Az adatkezelés mindig egy bizonyos mértékű korlátozás. A jogszabályi követelmény, hogy az adatkezelés annak céljától függően nem korlátozhatja aránytalan mértékben az érintettek jogait és szabadságait.

A hatósági típusú adatkezelések - ideértve a bünyügyi típusú adatkezeléseket is - során jellemzően az előbbi mérleges példával ellentétben az adatkezelők rendelkezési jogosultsága van túlsúlyban. Ezen belül a bünyügyi célú adatkezelések a büntetőjog ultima ratio elvet megtestesítő jellege okán jellemzően magukon hordozzák a hatósági jogosultságok többletét a hatósági eljáráson belül megvalósuló adatkezelések tekintetében.

2. Első hipotézisemmel kapcsolatos eredmények áttekintése - A Bünyügyi Adatvédelmi Irányelv (LED) és jogharmonizációja

A III. fejezetben a bünyügyi adatvédelmi irányelvet ennek tagállami jogharmonizációját, és a szabályozással kapcsolatos szakirodalmi álláspontokat és az egyes értelmezési kérdéseket illetően EUB ítélezési gyakorlatát ismertettem. A jogirodalomban az irányelv számos értelmezése és bemutatása lelhető fel. (Sajfert, Quintel 2017, Oswald 2018, Nagy, Mezei 2018, Eszteri 2018, Leiser, Custers 2019, Quezada-Tavárez, et al. 2019, Lynskey 2019, Winter 2020, Bolognini 2020, Drechsler 2020, Naudts, 2020, Eszteri 2021)

Áttekintettem az Európai Bizottságnak a bűnüldözésben érvényesítendő adatvédelemről szóló irányelve alkalmazásáról és működéséről szóló jelentéseit, valamint az Állampolgári Jogi, Bel- és Igazságügyi Bizottság (LIBE) megbízásából készült tanulmányt, amely a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásának kritikai értékelését tartalmazta (Vogiatzoglou 2022). A jogharmonizációs értékeléséről szóló átfogó jelentések áttekintése mellett, a magyar, a német, a francia és a svéd jogba történő átültetés példáin keresztül ismertettem az egyes nemzeti jogszabályokba történő gyakorlatot, beleértve az adott nemzeti jogrendszerek adatvédelmi történetéhez kapcsolódó összefüggéseket.

Az egyes tagállami átültetések sajátosságai a magyar, a német, a francia és a svéd joggyakorlatban

Általánosságban elmondható, hogy a jogharmonizáció kereteit az adott tagállam jogrendszerének szabályai adják, azok történeti kialakulásának és hierarchiájának megfelelően. (Palánkai 2019)

A magyar szabályozás ezen elvek mentén, az információs szabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról szóló 2018. évi XXXVIII. törvény által fogalmazta meg jogszabályok módosítását. Az Infotv. a harmonizált szabályok mellett megtartotta a korábbi rendelkezéseket, és a változások kiemelésével implementálta a 2018-s adatvédelmi reformcsomagot. Az Infotv. teljes egységben az általános adatvédelmi rendelettel ültette át a bűnügyi irányelv rendelkezéseit, háttérszabályokat is biztosítva.

Németországban, hat évvel a hesseni (a világ első adatvédelmi törvénye) törvény után a „Die erste Fassung des deutschen Bundesdatenschutzgesetzes megalkotásával, a szövetségi kormány a német szövetségi adatvédelmi törvény első változatát hozta létre. A BDSG az adatvédelmi reformot követő szabályozásig több módosításon esett át, melyek a tartományi módosításokkal kezdődtek, és ezek után jött létre az egységes adatvédelmi törvény, amely magában foglalja a tartományi szabályozást is. Az új német szövetségi adatvédelmi törvény (Bundesdatenschutzgesetz – "BDSG") elfogadásával hozzáigazították a korábbi német jogi keretet a GDPR-hoz. A BGSZ együttesen implementálta az EU 2016/680 rendeletét a GDPR-ral.

Franciaország a jogharmonizáció során fenntartotta az 1978-as törvény architektúráját, (Loi n° 78-17) megőrizve a 40 évvel korábban jogalkotó által meghatározott elveket, és csak az

egymásnak ellentmondó rendelkezéseket helyezte hatályon kívül. A Módosító törvénnyel - Loi n° 2018-493 – együttesen ültette át a francia jogba a bűnügyi adatvédelmi irányelvet és az általános adatvédelmi rendeletet. A törvény 2018. május 25-én, visszamenőlegesen lépett hatályba. Ismételt módosítást követően (2018-687. számú rendelet) hatályba lépett az egységes adatvédelmi törvény, az „Informatique et Libertés” biztosítva az összhangot a többi hatályos szabályozással és az uniós joggal.

Svédország az elsők között, 1973-ban alkotta meg a nemzeti adatvédelemmel kapcsolatos jogszabályait. A következő, az SFS 1998:204 számú törvény az Európai Parlament és Tanács 95/46/EK irányelvének átültetésével jött létre. Ezt vonták vissza, helyette a GDPR kiegészítő rendelkezéseit tartalmazó törvény, valamint rendeleti szabályozással meghatározott, úgynevezett nyilvántartási jogszabályok - amelyek elsősorban a személyes adatok hatóságok általi feldolgozását szabályozzák, léptek életbe. Az (EU) 2016/680/EU irányelvet külön törvénnyel, (SFS 2018:1177) ültették át a svéd jogrendszerbe. A svéd adatvédelmi rendszer hármas pilléren alapul, melynek első két eleme – a létrehozás sorrendjét tekintve – az általános adatvédelmi rendelethez kapcsolódó SFS 2018:218 számú törvény és SFS 2018:219 számú rendelet együttese. A harmadik elem a személyes adatok bűnügyi célból történő kezelésére szolgáló 2018:1177 számú törvény.

A bűnügyi adatvédelmi irányelv tagállami átültetése a magyar, a német, a francia- és a svéd nemzeti jogrendszerekbe az általános adatvédelmi rendelettel csaknem egyidőben történt. A magyar, a német és a francia jogalkotó mindkét uniós jogszabályt egységesen, a nemzeti adatvédelmi szabályozás szerinti korábbi törvény keretében, módosító törvényjavaslattal ültette át, megtartva azok uniós szabályozással nem ellentétes rendelkezéseit. A svéd jogalkotás annyiban különbözik, hogy a korábbi adatvédelmi rendeleteket hatályon kívül helyezve új jogszabály megalkotásával alkalmazta az általános adatvédelmi rendeletet, és ugyanígy implementálta a bűnügyi irányelvet is, megfelelően a korábbi jogi szabályozásnak, külön törvényi szabályozás keretei között.

Az egyes nemzeti szabályozások összehasonlítása az Irányelv egyes szempontjai szerint

A már hivatkozott tanulmányok szerint a tagállamok közül többen nem tartották be az átültetésre vonatkozó 2018. májusi határidőt, kötelezettségi eljárások után 2019-ig azonban ez a legtöbb esetben megtörtént. A megfeleléségi értékelés szerint a tagállamok az irányelv bevezetésekor vagy módosították meglévő adatvédelmi törvényeiket, vagy azokat hatályon

kívül helyezve, új, horizontális adatvédelmi jogszabályokkal helyettesítették. A nemzeti jogszabályok gyakran hivatkoznak a GDPR megfelelő vagy hasonló rendelkezéseire az irányelv átültetésekor, számos rendelkezést azonban új jogszabályi elemek bevezetésével ültettek át, például az általános közigazgatási jog, a közigazgatási eljárásjog és a büntetőeljárás területén. Egyes tagállamok az irányelv illetékes hatóságok működését-, és hatásköreit szabályozó rendelkezéseit beépítették ágazati jogszabályaikba is. Az általam vizsgált – magyar, német, francia, és svéd átültetési gyakorlatok esetében is ez volt a jellemző.

Az irányelv hatályát illetően alapvetően két szempont az irányadó, a személyi (illetékes hatóság) és a tárgyi hatály (bűncselekmény fogalma), melyek együttesen határozzák meg az egységes megközelítést. [(EU)2016/680, 2. cikk (1) és (12)–(14) preambulumbekzdés)]

A magyar joggyakorlatban az Infotv. kiterjesztette a törvény hatályát a nemzetbiztonsági-és honvédelmi célú adatkezelésekre is, „az Infotv. előírásainak teljességét rendelte el alkalmazni” (Infotv. 2. § (3) bekezdés) A német adatvédelmi törvény az (EU) 2016/680 irányelv hatályával kapcsolatban egyértelműen megjelöli az irányelv szerinti bűnügyi adatkezelési célt, és a törvény hatályát a „ (...) büntetőjogi vagy közigazgatási szankciók végrehajtására illetékes állami szervek által végzett adatkezelésre” rendeli alkalmazni. (BDSG 45.§) Arról is rendelkezik, hogy ez a hatály a szövetségi adatvédelmi biztosra és hivatalára is vonatkozik. Alkalmazható azokra a közigazgatási szabálysértésekre is, amely nem minősülnek büntetőjogi szabálysértésnek és csak pénzbírság formájában kiszabott közigazgatási szankciókkal sújthatók [BDSG 11. § (1). 8.] A német törvény hatálya így eltér a bűncselekmény szűkebb értelmezését alkalmazó országokban megfigyelhető joggyakorlattól, amelyek a hasonló közigazgatási szankciókat esetleg nem tekintik a LED végrehajtása alá tartozónak. A francia 78-17- s számú törvény a 87. cikkben határozza meg az irányelv szerinti hatályt. A 87. cikk külön kitér a hatóságok GDPR szerinti célú adatkezeléseire is. A 2018. júniusi törvényben még szerepelt a nemzetbiztonság védelme az adatkezelés céljai között, a jelenleg hatályos törvényben már nem szerepel. A svéd bűnügyi adatokról szóló törvény meghatározza a törvény célját, és az illetékes hatóságokat a hatályt illetően. (SFS 2018:1177 1.ch.2.§) A törvény nem vonatkozik a nemzetbiztonsági vonatkozású személyes adatok biztonsági rendőrség általi kezelésére, illetve arra az esetre, ha a rendőrség nemzetbiztonsági feladatot vett át a biztonsági rendőrségtől. A törvény nem vonatkozik továbbá a személyes adatok fegyveres erők általi kezeléséről szóló törvényre, illetve fegyveres műveletekkel kapcsolatos törvény által meghatározott adatkezelésekre sem.

A hatályt illetően a közrend és a közbiztonság azok a fogalmak, melyekhez a tagállamok egy része a nemzetbiztonságot is köti, áttételesen a közrend megzavarására alkalmas

bűncselekmények által. Ez láthatóan a magyar, a német és a korábbi francia joggyakorlatban is megjelent. A hatály tekintetében a GDPR-tól való elhatárolás - a Bizottság jelentése szerint - nem minden tagállamban egyértelmű, elsősorban egyes közigazgatási egységek nem bűnüldözési célú, például pénzügyi információs adatkezelését is az irányelv hatálya alá sorolják. Az általam vizsgált országok gyakorlatában ez nem lehetséges fel.

Az adatvédelmi felügyelő hatóságok irányítása és jogköreit tekintve, az általam vizsgált tagállamok a GDPR végrehajtásáért is felelős felügyeleti hatóságot bízták meg a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásával. Jogkörükben a vizsgálati hatásköröket, a korrekciós hatásköröket biztosították, tényleges hatáskörrel rendelkeznek, közigazgatási bírságot kiszabhatnak. Magyarország és Svédország nemzeti felügyeleti hatóságai az irányelv hatáskörén túl további jogokat biztosított a hatóságoknak, úgy, mint az adatkezelő és az adatfeldolgozó bármely helyiségébe való belépésének, valamint a bármely adatfeldolgozó berendezéshez és eszközhöz való hozzáférés jogát.

Svédország esetében az egyes illetékes hatóságok – köztük a rendőrség – felügyeletét a GDPR tekintetében illetékes felügyeleti hatóság (Integritetsskyddsmyndigheten, IMY) és a Svéd Biztonsági és Integritésvédelmi Bizottság felügyeleti hatóság közösen látja el. A távközlési szolgáltatóknak csak a Svéd Posta és Távközlési Hatóság felé kell bejelenteniük a biztonsági eseményeket, azaz nem az IMY-nek, még akkor sem, ha az incidens személyes adatok megsértését is magában foglalja.

A nemzeti felügyelő hatóságok az igazságszolgáltatás függetlensége miatt nem jogosultak az ezzel összefüggő adatkezeléseket felügyelni, ez a szabályozás jelenik meg a magyar [(Infotv. 38.§ (2b)], a német [BDSG 9.§ (2)], a francia (Informatique Lib. n°78-17 19.cikk), és a svéd (SFS 2018:1177 5.ch, 2.§)szabályozásban is.

Fontos szempont a hatáskör tekintetében, hogy az irányelvvel kapcsolatos nemzeti adatvédelmi jogszabályok megsértését a nemzeti adatvédelmi hatóságok, az igazságügyi hatóságok tudomására hozhatják-e, vagy indíthatnak-e bírósági eljárást, vagy abban részt vesznek-e. n

A jogorvoslati lehetőségekkel kapcsolatban valamennyi tagállam biztosította a jogot arra, hogy az érintett panaszt nyújtson be az illetékes felügyeleti hatóságához. A bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel összhangban, az általam vizsgált tagállamok – [Infotv. 55.§ (3)] (BDSG 20.§) , (Informatique Lib.108. cikk),(SFS 2018:1177 5.ch. 2.§ és 3.§) – biztosítják ezeket a jogokat az érintettek számára, beleértve a bírósági jogorvoslatot is. Svédország kivételével bírósági jogorvoslat áll rendelkezésre abban az esetben is, ha a felügyeleti hatóság három hónapon belül nem foglalkozik a panasszal, vagy nem tájékoztatja az érintettet a panasz állásáról vagy eredményéről.

Az Irányelv szerint a nemzeti adatvédelmi jogszabályoknak az adatkezelés jogalapját meg kell határozniuk, rendelkezniük kell legalább az adatkezelés célkitűzéseiről, a kezelendő személyes adatokról és az adatkezelés céljairól. A magyar [Infotv. 5.§ (1) –(4)], a német (BDSG 22.§ és 48.§), a francia (Informatiq Lib. 78-17 5.6 és 87.cikk), valamint a svéd (SFS 2018:1177, 2.ch 1-3. §, és 11-14.§) adatvédelmi törvények biztosítják ezt. Jogalapok tekintetében a hozzájárulást, mint jogalapot, a német, francia, svéd és a magyar harmonizált joggyakorlat nem használta, összhangban a LED-del.

Az érintettek kategóriái közötti irányelv által meghatározott különbségtétel mindegyik általam vizsgálat tagállam esetén jelen van. [Infotv.7.§.1.a),(BDSG 72.§), (Informatique lib. 78-17 98.§) , (SFS 2018:1177 2.ch.9.§).

Minden tagállam tiltja az automatizált döntéshozatalt, amikor különleges kategóriájú személyes adatok kezeléséről van szó, kivéve ha a megfelelő garanciák biztosítottak.[Infotv. 6.§ ba), és bb)] (BDSG 37.§), (Loi.No.78-17 95.§) (SFS 2018:1177 2. ch.19.§)

A naplózással kapcsolatban a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv meghatározza azokat a minimális információ típusokat, amelyeket a naplónak tartalmazniuk kell. A magyar, a német, a francia és svéd szabályozás is rögzíti ezeket. [Infotv.25/E.§ és 25/F.§], (BDSG 76.§), (Informatique Lib.78-17 101. cikk),(SFS 2018:1177 3.ch. 5.§)

Az érintettek jogaival kapcsolatban az irányelv szerinti korlátozás lehetőségével valamennyi tagállam élt. Az érintetti jogok gyakorlása a nemzeti adatvédelmi hatóságokon keresztül történik a nemzeti joggal összhangban. Az érintettek kategóriái közötti, bűnügyi irányelv szerinti különbségtétel, különösen a gyanúsított tekintetében mindegyik általam vizsgálat tagállam esetén jelen van.

A tájékoztatással kapcsolatban – LED 13.cikk- a német átültetés értelmében az adatkezelő elhalaszthatja, korlátozhatja vagy mellőzheti a tájékoztatási kötelezettséget 13. cikk (3) bekezdésében felsorolt feltételek teljesülése esetén, azonban kiegészíti azt: ha úgy ítéli meg, hogy a veszély elhárítása meghaladja az érintett tájékoztatásához fűződő érdekeket.

A hozzáféréssel kapcsolatban – LED 14. cikk - csak néhány nemzeti jogszabály fogadott el eltérő megfogalmazást vagy további követelményeket. A német jogalkotó emellett a hozzáférés megtagadását kibővítette. Franciaország az érintett azonosítására vonatkozóan külön eljárást ír elő, amelynek során az érintettnek bármilyen, az adatkezelő által a hitelesítéshez elegendőnek ítélt eszközzel (beleértve a digitális személyazonosság használatát is) igazolnia kell személyazonosságát. A hozzáférési jog akkor is megtagadható, ha az érintett nem ad elegendő információt ahhoz, hogy az adatkezelő aránytalan erőfeszítés nélkül megtalálja a személyes

adatait. Kérdéses, hogy ezek az indokok összhangban vannak-e a LED-del (Dimitrova, De Hert, 2018). Eltérés még a LED- től, hogy a német adatvédelmi törvény nem tesz kifejezett említést a közös adatkezelésre vonatkozó kapcsolattartási pont kijelölésének kötelezettségéről, így a LED 21.cikk szerinti követelménye látszólag teljesen hiányzik a nemzeti jogi keretből.

Megállapítottam, hogy a tagállamok között eltérések vannak a bűnügyi irányelv átültetésében, a bűnüldözési célú adatkezelések uniós szabályozása nem rendeleti formában, hanem irányelvi megfogalmazás keretei között jött létre, ami tág mérlegelési jogkört biztosított a tagállamok részére. A "bűncselekmény", "közbiztonság" és "illetékes hatóság" fogalmak értelmezési különbségei jelentek meg, ami befolyásolja a hatály fogalmának értelmezését. Az eltérések abból is adódnak, hogy a LED nem ad egységes meghatározást ezekre a fogalmakra. Véleményem szerint az irányelv végrehajtásának további pontosítása érdekében fontos a tagállamok közötti együttműködés erősítése, a legjobb gyakorlatok cseréje, az Európai Bizottság, az Adatvédelmi Testület iránymutatásai, a folyamatban lévő EUB döntések által nyújtott iránymutatások és támogatások hatékony alkalmazása. Emellett szükség lehet az irányelv felülvizsgálatára a fogalmak pontosítása szempontjából, valamint, hogy egyértelműbbé tegyék a személyes adatok különleges kategóriáinak feldolgozásával, valamint az automatizált döntéshozatallal kapcsolatos szabályozást.

Álláspontom szerint azonban jelenleg az Irányelv megfelelő keretrendszert biztosít a tagállamok számára, a fogalmak értelmezése tekintetében az EUB gyakorlata megfelelő útmutatást ad, úgy, mint a személyes adatok különleges kategóriái, valamint az automatizált döntéshozatal kérdésköre. Az EDPB által kialakított gyakorlat és a kötelező érvényű döntések képesek a technikai fejlődés által megkívánt kiegészítéseket a szabályozási folyamatba „kívülről” beépíteni.

3. Második hipotézissel kapcsolatos eredmények áttekintése - Bűncselekményekhez kapcsolódó személyes adatok védelme a büntetőeljárás és a büntetésvégrehajtás során

A büntetőeljárás és a személyes adatok védelme

A büntetőeljárások alapvető célja a bűncselekmények felderítése, az elkövetők felelősségre vonása és a jogellenes cselekményekből eredő károk orvoslása, miközben az alapvető jogokat, a magánélet védelmét is tiszteletben kell tartani (Kőhalmi 2013).

A IV. fejezetben elemeztem a bűncselekményekhez kapcsolódó személyes adatok védelmét a büntetőeljárás során, különös tekintettel az érintettek kategóriáinak megkülönböztetésére.

Az adatvédelmi szabályoknak való megfelelést az eljárás különböző szakaszaiban, a Büntetőeljárásról szóló törvény szabályozását figyelembe véve vizsgáltam. (Király 2000, Fenyvesi, Herke, Tremmel 2004, Nyíri 2018, Herke 2018, Fantoly, Budaházi 2019).

Részletesen áttekintettem, hogyan határozzák meg a jogszabályok a gyanúsítottak tanúk, vádlottak és sértettek személyes adatainak kezelését, valamint milyen potenciális problémákat vetnek fel az eljárás során. (Hesz, Kőhalmi 2009, Pálvölgyi 2014, Németh 2019, Róth 2021, Mándi 2023)

Kiemelt figyelmet fordítottam a tárgyalás nyilvánosságának és a zárt tárgyalásnak az adatvédelemmel kapcsolatos kihívásaira, valamint az ügyiratok zárt kezelésének problémáira. Bemutattam a tárgyalás nyilvánosságának elvéből és a természetes személyek adatainak védelméről szóló jogszabályokból eredő lehetséges konfliktusokat. (Cséka 2007, Petrik 2009, Erdei 2011, Navratil 2011, Varga 2018, Németh 2019, Kőhalmi 2023, Márki 2023).

Adatvédelmi aggályok a tárgyalási jegyzék kifüggesztése, a tárgyalás nyilvánossága vagy zárt tárgyalás elrendelése, valamint az ítélelhirdetés nyilvánossága, és a bírósági tárgyalásokról szóló tudósítás kapcsán merültek fel. Az aggályokra adott válaszokat a bűnügyi adatkezelést szabályozó keretrendszer, azaz a bűnügyi irányelv nyomán, az Infotv. által előírt rendelkezések alapján vizsgáltam meg. Az adatkezelésnek egyrészt meg kell felelnie a jogszerűség, a törvényesség [Infotv. 4.§. (1)] és célhoz kötöttség alapelveinek. [Infotv. 5.§. (2)]. Ez utóbbi, melyet a Be. is megfogalmaz [Be. 98.§. (3)] kimondja, hogy személyes adatok kezelése kizárólag abban az esetben történhet, ha az adott cél megvalósításához szükséges, a cél elérését lehetővé teszi, és az adott cél eléréshez elengedhetetlenül szüksége időszakra korlátozódik. Másrészt a bűnügyi adatkezelés során figyelembe kell venni az érintettek kategóriáit, mivel ez meghatározza az alkalmazandó adatvédelmi szabályozásból adódó jogokat és korlátokat.

Az Infotv. rendelkezései alapján a bíróság az adatkezelő szerepét tölti be a vádeljárás során, tehát az érintetti jogok és korlátozások tekintetében rendelkezhet. [Infotv. 7.§ (1) a) –d)], és [Infotv. 7.§ (4)]

Egyetértve Mándi felvetésével, véleményem szerint a bíróság mérlegelési jogkörét figyelembe véve, amennyiben az eljáró bíró úgy ítéli meg, hogy valamely - az eljárásban felsorolt egyéni kategóriák szerinti megkülönböztetés alapján - személyes adat védelméhez az elengedhetetlenül szükséges, a Be. szerinti „erkölcsi okból” [Be. 436.§. (4) a)] elrendelheti a zárt tárgyalást. (Mándi 2023)

De lege ferenda javaslatom ezzel kapcsolatban a Be. taxatív felsorolásainak ilyen irányú módosítása. [Be. 436.§. (4) c)]. A 436. szakasz (4) bekezdése c) pontjának „,minősített adat és egyéb védett adat védelme érdekében” kiegészítését javasolnám az alábbiak szerint: - „, minősített adat és egyéb védett adat védelme érdekében, valamint olyan személyes adat esetében melynek védelméhez az elengedhetetlenül szükséges különös tekintettel az érintettek kategóriái közötti különbségtételre.”

Felmerül a kérdés az „az elengedhetetlenül szükséges” meghatározás értelmezését illetően.

A Be. használja ezt a kifejezést, a személyes adatok zárt kezelése esetében a személyes adatot az áldozat segítség és pártfogói felügyelet ellátásához „elengedhetetlenül szükséges” mértékben lehet továbbítani.[Be. 99. § (5) b)] Használja továbbá a minősített adat felhasználása esetén, azaz a bíró és az ügyész „elengedhetetlenül szükséges” mértékben kezelhet minősített adatot feladatai végrehajtásához, [Be.104.§.(2)] Használja a különleges bánásmódot igénylő személy személyes adatainak védelméhez, ha az „elengedhetetlenül szükséges”. [Be.109.§.(1) b), c), d)] Az adatkérési szolgáltatással kapcsolatban „csak annyi és olyan személyes adat szolgáltatása kérhető, amely az adatkérés céljának megvalósításához elengedhetetlenül szükséges.”[Be. 264.§. (4)]

A tárgyalási jegyzék nyilvánosságával kapcsolatban egyetértek Mándi és Németh álláspontjával, amennyiben az eljárás ügyszámának önmagában történő kifüggesztése biztosíthatja az érintettek személyes adatainak védelmét. Az ügyszám csak akkor válik személyes adattá, ha az a természetes személlyel kapcsolatba hozható, és megismerhető, egyébként közérdekű adatnak minősül, ahogy ezt a NAIH is rögzíti állásfoglalásában. (NAIH/2020/294/4)

A tárgyalás nyilvánossága mellett a zártan történő eljárás esetében az ítélet nyilvános kihirdetésének problémája merült fel még adatvédelmi szempontból. Ezzel és az ehhez kapcsolódó sajtónyilvánosságával kapcsolatban a NAIH állásfoglalását tekintem irányadónak. (NAIH-4418-5/2012/V).

A bírósági eljárások során kialakított ítéletek nyilvános kihirdetése egyrészt a társadalmi normák érvényesítését szolgálja az elkövetőkkel szemben, másrészt pedig prevenciós célt is hordoz, mivel célja a hasonló jogsértések megelőzése. A büntetőeljárás nem csupán a megtorlást célozza, hanem arra is törekszik, hogy elrettentse a terhelteket a további bűncselekmények elkövetésétől. Alapvető fontosságú, hogy a büntetőjogi rendszer lehetőséget biztosítson az elítéltek számára, hogy a büntetésük letöltése után sikeresen reintegrálódjanak a társadalomba, a büntetett előéletből adódó hátrányok nélkül. Ezzel összefüggésben az online térben közzétett bírósági tárgyalásokról szóló tudósítások esetében megjelenő személyes

adatok, mint az elítéltek neve, a bűncselekmények és a kiszabott büntetések, hosszú távon is hozzáférhetővé válnak, (Németh 2019, Köhalmi 2023, Márki 2023) ami figyelmen kívül hagyja az elítéltek jogát a büntetett előlethez fűződő hátrányok idővel történő eltörlésére. *Ennek érdekében az Infotv. alapján, a személyes adatok kezelése során - ahogy a tárgyalás nyilvánosságával kapcsolatosan is, az ítélethirdetés kapcsán is, csak a célnak megfelelő - jelen esetben a bírósági tárgyalásról történő tájékoztatás megvalósulásához elengedhetetlenül szükséges személyes adat kezelhető, a cél megvalósulásáig szükséges mértékben és ideig.*

A nyilvánosság a közvetlenség és szóbeliség mellett egy alapvető tárgyalási elv, amely a bírói önkény ellen szolgál biztosítékként. A modern kor tárgyalásnyilvánossága különösen sebezhetővé válik az elektronikus média jelenléte és a tudósítások kihívásai által .Ez a gyakorlat jelentős hatással van az érintettek magánéletére és társadalmi reintegrációjukra. Ezért felmerül a kérdés, hogy a nyilvános bírósági tárgyalásokról szóló tudósítások milyen mélységben és mely személyes adatokat tartalmazhatnak jogosan (Havasiné 2017, Márki 2023, Köhalmi 2023).

Véleményem szerint a sajtónyilvánossággal kapcsolatban egyensúlyt kell biztosítani a közvélemény tájékoztatásának jogos igénye és az egyének magánszférája, személyes adatokhoz való jogának védelme között. A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény, hangsúlyozza, hogy a sajtószabadság gyakorlása nem eredményezheti bűncselekmény elkövetését vagy annak felhívását, nem sértheti a közízlést, továbbá nem sértheti harmadik fél személyhez fűződő jogait.(2010. évi CIV. törvény)

A médiatartalom-szolgáltatóknak meg kell őriznie az emberi méltóságot a közvetített tartalmakban.[2010.éviCIV.tv.14.§.(1)]. A jogszabályi előírások alapján adatvédelmi szempontokból csak kivételes esetekben indokolt, hogy a bírósági tárgyalásokról szóló sajtóbeszámolók személyes adatokat tartalmazzanak. Fontos figyelembe venni azokat az eseteket is, ahol az információközlés hozzájárulhat a jövőbeli bűncselekmények megelőzéséhez, különösen, ha az érintett nem közszereplő vagy nem lát el közfeladatot. A sajtótermék kiadójának vagy szerkesztőségének meg kell vizsgálni, hogy a célt anonimizált adatok, vagy csak a kezdőbetűk használatával is el lehet-e érni, miközben a személyiségvédelem maximálisan biztosított marad, összhangban a sajtószabadságról és médiatartalmak alapvető szabályairól szóló törvény általános elveivel. Képi-és hangszközök használata esetére is vonatkoztatható ez megállapítás.

A bűncselekményekhez kapcsolódó személyes adatok védelme a büntetésvégrehajtás során

A büntetésvégrehajtás adatvédelmi vonatkozásaival kapcsolatban részletesen bemutattam a vonatkozó jogszabályok adatkezeléssel kapcsolatos rendelkezéseit.

Adatkezelés a 2013. évi CCXL. törvény (Bvtv.) alapján

A Bvtv. részletezi a kezelhető adatokat, beleértve a személyes adatokat, bűnügyi személyes adatokat és különleges adatokat. Ezen adatkategóriák széles körűek, tartalmazva az elítéltek és fogvatartottak nevét, lakcímét, értesítési címét, elektronikus elérhetőségeit, egészségügyi adatait, bűnügyi előéletre vonatkozó információkat és más személyes jellemzőket. Új elemként a törvény kiterjesztette az adatkezelést az elektronikus kapcsolattartási adatokra is. [Bvtv.76 § (2)] A büntetésvégrehajtás során szükséges az elektronikus megfigyelési eszközök és az arcképfelismerő rendszerek használata. Az elektronikus megfigyelési eszközök alkalmazása kiterjedhet az elítélt vagy fogvatartott személyek mozgásának nyomon követésére, míg az arcképfelismerő rendszerek az azonosításukat és tevékenységeik ellenőrzését szolgálják. [Bvtv.76 § (3b)]

A büntetés-végrehajtás során kezelt adatok biztonságos működtetését a biztonsági kockázatelemzési kötelezettség biztosítja. [Bvtv.27/A. § (1)]

A büntetésvégrehajtás során a rendőrség is jogosult az érintettek adatainak kezelésére, tekintettel arra, hogy az általuk fogatosított kényszerintézkedések beleszámítanak a kiszabott büntetés időtartamába. Jogosultságuk vonatkozik az őrizetbe vett személyek, letartóztatottak, szabálysértési elzárás alatt állók, pártfogó felügyelet alatt állók, valamint az előállított vagy szállított személyek adatainak kezelésére. [Bvtv.78 § (1)]

Amennyiben törvény eltérően nem rendelkezik, az adatokat a büntetés, az intézkedés, a kényszerintézkedés vagy a szabálysértési elzárás végrehajtásának befejezésekor, vagy végrehajthatóságának megszűnésekor törölni kell.[Bvtv.79 § (1)] Ezzel szemben a büntetés-végrehajtási szervezetről szóló törvény alapján [1995.évi CVII.tv. (Bvsztv.) 32. §.(1)] a fogvatartottról szóló adatokat 25 évig kell megőrizni, a fogvatartott szabadulásakor törölni kell a nyilvántartásból a kapcsolattartó és a sértettel kapcsolatos adatokat.[Bvsztv.) 32. §.(1)] Az egészségügyi dokumentációk esetében külön törvény még hosszabb, akár 30 vagy 50 éves megőrzési időt ír elő.[1997. évi XLVII. (Eüak.)tv.] Ellentmondás állhat fenn, főként, ha sor került egészségügyi adatok kezelésre.

A büntetés-végrehajtás kapcsán megemlítendő a pártfogó felügyelet intézménye. [(Bvtv. 68.§) Ez a rendelkezés biztosítja a pártfogó felügyelet hatékony ellátásához szükséges adatok hozzáférhetőségét, ugyanakkor szigorú keretek között tartja az adattovábbítást. [Bvtv. 80 § (1)] A törvény lehetővé teszi az elítéltek, fogvatartottak, pártfogó felügyelet alatt állók és utógondozottak adatainak statisztikai és tudományos célú felhasználását, amennyiben ez az azonosításra alkalmatlan módon történik.(Bvtv. 81.§)

A fogvatartottak személyes adatainak védelme a 1995. évi CVII. (Bvszttv.) törvény alapján

A büntetés-végrehajtási rendszer magában foglalja a Büntetés-végrehajtás Országos Parancsnokságát (a továbbiakban: BVOP), a büntetés-végrehajtási intézményeket, a büntetés-végrehajtási intézeteket, és a gazdasági társaságokat [Kondás 2018].

A BVOP feladatai közé tartozik a fogvatartás körülményeinek, biztonságának biztosítása, a fogvatartottak társadalmi reintegrációjának elősegítése, munkaerő-piaci reintegrációjuk, egészségügyi ellátásuk, logisztikai menedzselésük, valamint az adatkezelésük szabályozása és felügyelete.[Bvszttv.4.§.g)] A Bvszttv. rendelkezik a fogvatartottak és kapcsolattartóik nyilvántartásáról, a sértett és kapcsolattartóik nyilvántartásáról.(Bvszttv. 28. § - 29.§)

A büntetés-végrehajtási rendszeren belül a személyes adatok integritásának megőrzése kiemelt fontosságú, melyen belül hangsúlyt kapott a nemzetközi adattovábbítás kérdése.[Bvszttv. 29/A. §.(1)-(5)]. Az Európai Unió tagállamai és az EU által létrehozott nemzetközi bűnüldöző szervezetek részére a büntetés-végrehajtási szervezet által kezelt személyes adatokat az EU jogszabályainak végrehajtását szolgáló törvény vagy két- vagy többoldalú nemzetközi szerződés alapján az előírt célból lehet átadni. [Bvszttv.29/A.(1)].

A szabályozás különös figyelmet fordít arra, hogy az adattovábbítás csak meghatározott célokra, mint a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából történhessen. Az adattovábbítás csak akkor lehetséges, ha a harmadik országok vagy a nemzetközi szervezetek illetékes hatóságai megfelelnek „az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározott feltételeknek” [Bvszttv.29/A.(4)]. Az adattovábbítás nem érintheti a sértettel kapcsolatos adatokat.[Bvszttv. 28/B. § (2)]

Az adatkezelő szervek kötelesek gondoskodni az adatok biztonságáról, az adatokhoz való illetéktelen hozzáférés megakadályozásáról, valamint az adatok pontosságának, teljességének és naprakészségének ellenőrzéséről. Az adatszolgáltatásra irányuló kérelemnek tartalmaznia kell az adatkérés indokát és jogszabályi alapját, így biztosítva az adatkezelés átláthatóságát és

célhoz kötöttségét, lehetővé téve az adatok hatékony felhasználását a bűnüldözés és az igazságszolgáltatás területén. (Bvsztv. 31.§).

Mesterséges intelligencia alapú rendszerek a büntésvégrehajtásban

Ismertettem a büntésvégrehajtásban hazánkban használatos mesterséges intelligencia alapú rendszereket (Hinkel, 2020). Ezzel kapcsolatban felhívtam a figyelmet arra, hogy az MI alapú rendszerek, mint a SAFE, Navigator és KIOSZK, adatvédelmi kihívásokat vetnek fel, különösen a személyes adatok nagy mennyiségű kezelése és azok biztonsága kapcsán. Az MI alapú rendszerek adatvédelmi problémái közé tartozik a személyes adatok bizalmas kezelése, az adatok szükségtelen gyűjtése és tárolása, valamint a diszkrimináció lehetősége (Schmehl 2020, Mezei 2022, Eszteri, Péterfalvi 2022, Herke 2023). Az MI alkalmazása adatokra támaszkodik, melyek kezelésének az uniós adatvédelmi normáknak kell megfelelnie. A rendszereknek tiszteletben kell tartaniuk az érintettek jogait, mint az adathoz való hozzáférés, helyesbítés, törlés, és az adatkezelés korlátozásának jogát. Az adatvédelmi szempontból kockázatos tevékenységek esetén előzetes adatvédelmi hatásvizsgálat elvégzése szükséges. Adatkezeléskor csak hiteles, megbízható forrásból származó adatok használata lehetséges, készen állva a nemzetközi bűnügyi vonatkozásokkal kapcsolatos MI-adatigénylések támogatására. (Nagy, 2021).

A büntésvégrehajtás területén a személyes adatok kezelésével kapcsolatos jogi keretek véleményem szerint szigorúak, a GDPR és az Infotv. szabályainak megfelelnek. Az adatkezelők felelőssége nagy, károkozás esetén kártérítésre és sérelemdíj fizetésére kötelezhetőek. A bizonyítási teher az adatkezelőre hárul, aki köteles igazolni, hogy az adatkezelés jogszabályoknak megfelelt.

4. Harmadik hipotézisemmel kapcsolatos eredmények áttekintése - Az adatvédelem és a kiberbűnözés kapcsolata

Megállapítható, hogy a GDPR és a LED szabályozásai, melyek a személyes adatok védelmét hivatottak biztosítani, alapvetően hozzájárulnak a kiberbiztonsághoz is. (Porcedda

2012, Bederna,2018, Moore, Anderson 2019, Wicki-Birchler 2020, Schreiber 2021, Hirvonen 2022)

Ezzel kapcsolatban az alábbi pontokban foglaltam össze a legfontosabb tényezőket:

Proaktív védelem: A GDPR előírja az adatvédelmi intézkedések beépítését az információs rendszerek tervezési fázisában (beépített adatvédelem elve), valamint az adatvédelmi intézkedések folyamatos fenntartását az adatok kezelésének egész folyamata során. Ez magában foglalja a titkosítást, a hozzáférés-szabályozást, az adatok integritásának és biztonságának fenntartását. Ezek az intézkedések jelentősen csökkenthetik a kiberbűnözők által kihasználható kockázatokat, például jogosulatlan hozzáférést adatainkhoz, vagy az adatlopást. (GDPR, Preambulum (8), 47. cikk d))

Adatkezelési elvek: A GDPR és a LED az adatminimalizálás elvét is előírja, amely szerint csak a feltétlenül szükséges adatok gyűjthetők és tárolhatók, és csak meghatározott, világos és jogszerű célokra. Ez az elv csökkenti a kiberbűnözők számára elérhető érzékeny információk mennyiségét, ezzel minimalizálva az adatokkal visszaélés kockázatát. [GDPR, 5.cikk c)]

Adatvédelmi hatásvizsgálat: A GDPR előírja az adatvédelmi hatásvizsgálat elvégzését magas kockázatot jelentő adatkezelési műveletek esetén, mint például nagy mennyiségű személyes adat feldolgozása vagy különösen érzékeny adatok kezelése. Ez lehetővé teszi az adatkezelési tevékenységek kockázatainak azonosítását és kezelését, így proaktív védelmet nyújthat a kiberfenyegetésekkel szemben. (GDPR, 35.cikk)

Hozzáférés-vezérlés és felhasználói jogosultságok Mind a GDPR, mind a LED szigorú követelményeket állapít meg a személyes adatokhoz való hozzáférés kezelésére. A szervezeteknek gondosan kell szabályozniuk, hogy ki férhet hozzá az adatokhoz, ezzel csökkentve a jogosulatlan hozzáférés kockázatát.(GDPR, Preambulum (73), 15.cikk)

Incidenskezelés és értesítés: A GDPR kötelezővé teszi az adatvédelmi incidensek, például adatsértések nyilvánosságra hozatalát és jelentését az illetékes hatóságoknak, valamint érintett egyének értesítését, ha az incidens valószínűleg magas kockázatot jelent az érintettek jogaira és szabadságaira. Ez hatással lehet a kibertámadások okozta károk enyhítésére.[GDPR, Preambulum (49), (85) – (88), 33.cikk]

A NIS2 irányelv számos kötelezettséget ró a tagállamokra a kiberbiztonság területén, ezek egy része speciális adatvédelmi követelményeket is meghatároz, összhangban a GDPR-ral.

A NIS Irányelvet a GDPR kiegészítő jogszabályként lehet tekinteni, amely megfelelő biztonsági kötelezettségeket és új bejelentési kötelezettségeket vezet be bizonyos iparágakban és digitális szolgáltatásnyújtók számára.(Cole, Schmitz 2019)

A NIS 2 irányelv bevezetése kiterjeszti a kiberbiztonsági szabályok alkalmazási körét. Szigorú követelményeket állít fel a szervezetek adatkezelési gyakorlataira vonatkozóan, különös tekintettel az adatbiztonsági intézkedésekre és az adatkezelés jogalapjára.

A NIS 2 hatálya alá tartozó vállalatoknak és szervezeteknek a GDPR által előírt adatvédelmi elvárásokon túl, a NIS 2-t átültető jogszabályoknak megfelelően is biztosítaniuk kell az adatok biztonságát. Ez magában foglal néhány olyan előírást is, ahol az adatvédelmi és kiberbiztonsági követelmények átfedik és kapcsolódnak egymáshoz, úgy, mint a biztonsági intézkedések, adatvédelmi szabályzatok, az auditok, ellenőrzések, az incidensek, az adatfeldolgozói szerződések, és az adatkezelési tájékoztatók területén.

Összefoglalva, a bűnüldözési irányelv és az általános adatvédelmi rendelet az Európai Unió két alapvető adatkezelésekre vonatkozó jogszabálya, amelyek az adatvédelem és az adatbiztonság területén hivatottak szabályozni az adatkezelési gyakorlatokat.

A GDPR az adatkezelés alapelveire összpontosít, úgy, mint az adatminőség, az átláthatóság, az adatkezelés korlátozása, az adatbiztonság, és az elszámoltathatóság. Ezek az alapelvek különösen fontosak a kiberbűnözés kontextusában, mivel az adatvédelmi intézkedések és az adatbiztonsági protokollok közvetlenül befolyásolják a személyes adatokhoz történő jogosulatlan hozzáférés vagy azok illetéktelen felhasználásának kockázatát. A NIS 2 irányelvvel összhangban kialakuló új kibervédelmi és adatvédelmi előírások jelentős változásokat hoznak a szervezetek incidenskezelési folyamataiban. A NIS 2 Irányelv ebben az értelemben kiegészíti az adatvédelmi szabályokat.

5.Negyedik hipotézisemmel kapcsolatos eredmények áttekintése - A személyes adatokkal kapcsolatos és az információs rendszerrel kapcsolatos bűncselekmények

Személyes adatokkal kapcsolatos tényállások

Az adatvédelem, mint az egyén alapvető joga, információs önrendelkezés jogaként került meghatározásra az Alkotmánybíróság 15/1991. (IV. 13.) AB határozatában, származtatva azt, az emberi méltósághoz való jogból és a személyes adatok védelmének jogából. Az Alaptörvény VI. cikkének (2) bekezdése ezt a jogot, mint alapvető jogot rögzíti, biztosítva mindenki számára a személyes adataik védelméhez való jogot. (Eszteri, Péterfalvi 2017)

A Büntető Törvénykönyv XXI. fejezete, amely az emberi méltóság és egyes alapvető jogok elleni bűncselekményeket tárgyalja, szabályozza a személyes adatokkal kapcsolatos visszaélés bűncselekményét. A személyes adattal való visszaélés jogi megfogalmazása a Büntető Törvénykönyv úgynevezett keretdiszpozíciói közé esik. A keretdiszpozíciók sajátossága hogy a bűncselekmény Büntető Törvénykönyvben foglalt definíciója egy külső jogszabályra utal, és úgy rendelkezik, hogy a bűncselekmény a külső (extraneus) normának a Büntető Törvénykönyv által meghatározott módon történő megsértésével valósul meg (Belovics és mts.2014, Péterfalvi, Eszteri, 2017) A külső norma megsértése tehát nem minden esetben jelent egyben bűncselekmény elkövetését, csak akkor, ha azt a Büntető Törvénykönyvben meghatározott módon sértik meg.

A büntetőjogi keretet elsősorban a GDPR szabályai töltik meg tartalommal, amennyiben az adott adatkezelési tevékenységre a GDPR tárgyi hatálya kiterjed. Azokban az esetekben, amikor az adatkezelés a GDPR 2. cikk (2)-(4) bekezdései alapján kívül esik a rendelet hatálya alól, az adatkezelési normákat subszidiáriusan az Infotv. határozza meg. (Jóri 2018) Abban az esetben, ha a személyes adatok kezelése bűnüldözési, nemzetbiztonsági, vagy honvédelmi célból történik, az Infotv. előírásait kell alkalmazni.

A Büntető Törvénykönyv 219.§-a határozza meg a személyes adattal való visszaélés bűncselekményének jogi definícióját.

A bűncselekménynek sem passzív alanya, sem elkövetési tárgya nincs, tekintettel arra, hogy a személyes adat eszmei kategória. (Szomora 2014, 2019) Ugyanakkor számos szerző szerint a bűncselekmény elkövetési tárgya maga a személyes adat.(Békés 2016, Péterfalvi, Eszteri 2017, Horváth 2020, Gál A. 2020, Belovics 2021)

A személyes adat fogalmát a GDPR és az Infotv. határozza meg, lényegi eleme az érintettel kapcsolatba hozható bármely információ. Ennek alapján Szomora álláspontjával értek egyet, amely szerint a személyes adatok nem tekinthetők a bűncselekmény tárgyának, különös tekintettel arra, hogy azok igazságtartalmuktól függetlenül kapcsolatba hozhatók az adott személlyel.

Az elkövetési alakzatok elsősorban a GDPR által felsorolt elvek, úgymint a jogszerűség, a célhoz kötöttség és az adattakarékosság adatvédelmi elvének megfelelő érvényesülését hivatottak biztosítani.[GDPR 5. cikk (1) a)–c)]

Az első alakzat szerinti elkövetési magatartás a jogosulatlan vagy céltól eltérő adatkezelés, amely aktív magatartást jelent, elkövetője bárki lehet. [Btk. 219. § (1) a)] Az adatkezelés a GDPR és Infotv. által meghatározott tevékenység, [GDPR 4. cikk 2. és Infotv. 3. § (10).] amelynek megfelelő joggal kell történnie.[GDPR 6. cikk (1) ,és Infotv. 5.§.(1)]

A mulasztással elkövetett második alakzat az, amely az adatok biztonságát szolgáló intézkedés elmulasztásával valósul meg.[GDPR 32. cikk és Infotv. 25/I.§] A bűncselekmény harmadik alakzata, a tájékoztatási kötelezettség megszegésével valósul meg.[GDPR 13–14. cikk és Infotv. 15–16.§] Ez utóbbi két alakzatot csak a jogszerű adatkezelő követheti el. Meg kell azonban jegyezni, hogy büntetőjogi felelősséggel az is jár, ha valaki a személyes adatok védelmére vagy kezelésére vonatkozó törvényben vagy az Európai Unió kötelező erejű jogi aktaiban foglalt előírásokat megsértve nem ad megfelelő tájékoztatást az érintett személy hozzáférési jogának gyakorlásához,[Btk.219 (2)] és ezzel súlyosan sérti más személyek érdekeit.(Gál A. 2020)

Kulcsfontosságú szempont az „azonosított vagy azonosítható” személy fogalma a tényállást illetően, mivel meghatározza a személyes adat fogalmának értelmezését. A meghatározás jelentőségét mutatja, hogy egy Kúriai döntés jelentős szakmai vitákat váltott ki, az értelmezést illetően, amelynek kapcsán az azonosított, az azonosíthatóság, és a személyes adatra vonatkoztatható fogalmak értelemezési problémája merült fel. (BH 2019.272) Egy adat vagy információ akkor tekinthető személyre vonatkozóknak, ha legalább egy az alábbi három kritérium közül teljesül: tartalom, cél, vagy eredmény.(Pók,2019) Az információ akkor vonatkozik egy személyre, ha közvetlenül az adott személyre utal, függetlenül attól, hogy az adatkezelő vagy bármely harmadik fél milyen célból kezelte, vagy milyen hatást gyakorol az információ az érintettre. (WP 136, 4/2007) Felvetődik a kérdés ezzel kapcsolatban, hogy bizonyos esetben „az adatkezelőnek technikailag meglenne a lehetősége, de nem áll szándékában az azonosítás. Ezt a helyzetet úgy kell megítélni, hogy nem kizárólag az adatkezelő ezzel kapcsolatos szándéka számít, hanem az, hogy az ügy összes körülménye alapján észszerűen feltételezhető-e, hogy az adatokat az érintett azonosítására fogja használni. (Czapáry, Szőke 2022)

Egy személyt „azonosítottnak” tekinthetünk, ha kiemelkedik egy csoport többi tagjából.(WP 136, 4/2007) Azonosítható” egy személy akkor, ha lehetséges az azonosítása, még ha ez eddig nem is történt meg. Ennek a képességnek a megléte határozza meg, hogy az információ ebből a szempontból releváns –e.(Pók 2019) Ezzel kapcsolatban felmerül, hogy a személyes adattal való visszaélés jogi tényállása nem nyújt megfelelő védelmet bizonyos helyzetekben, mint például a tömeges és a teljes személyiségprofilozás, a kiskorúak védelme, valamint a deepfake jelenségek esetén.(Miskolczi, Szathmáry 2019).

Fontos különbséget tenni az érintett azonosítása vagy azonosíthatósága és a személyazonossága között. Az előbbi esetben az adatok lehetővé teszik az érintett különválasztását környezetétől

vagy az ott lévő többi személytől, míg a személyazonosság meghatározása azt teszi lehetővé, hogy pontosan ki azonosítható az adott egyén.(Pók 2019)

A személyes adatok fogalmának és büntetőjogi védelmének értelmezése kulcsfontosságú.

Miközben a GDPR közvetlenül hatályos és alkalmazandó az Európai Unió tagállamaiban, nem írja elő a személyes adatok védelmét a büntetőjog keretein belül. Ezzel együtt, a GDPR kiemeli, hogy az EU tagállamainak jogukban áll büntetőjogi szankciókat előírni a rendelet sérelme esetén.[EU 2016/679 Preambulum (149)] A Magyar Büntető Törvénykönyv (2012. évi C. törvény) nem ad explicit definíciót a személyes adatokra, hanem az „Az Európai Unió jogának betartása” fejezetben, utalás történik azok szabályozására,[465.§ (2) d)], az ennek végrehajtásához szükséges intézkedéseket megállapítására.(Btk.219.§)

A személyes adatokkal kapcsolatos tényállások közül ritkábban valósul meg a magántitok megsértése (Btk.223.§) és a levéltitok megsértése (Btk. 224.§)

A magántitok megsértésének büntette olyan esetekben állapítható meg, amikor az elkövetési cselekmény nem rendelkezik fizikai elkövetési tárggyal, hanem egy személyhez köthető, védelem alatt álló információs tartomány – azaz magántitok – jogosulatlan nyilvánosságra hozatalára irányul. Ez a titok tartalmazhat minden olyan adatot, amely a személy szűkebb környezetében ismert és a nyilvánosságra hozatal által az érintett személynek érdeksérelmet okozhat. A magántitok jogellenes nyilvánosságra hozatala kiterjedhet a személyi, családi, gazdasági státuszra, egészségi állapotra vagy bármely egyéni szokásra, ami egyébként nem lenne nyilvános.(BH.2004. 170 f). A bűncselekmény sértettje azon személyek körét foglalja magában, akiknek személyes, védett adatai érintettek. Ez a kategória lehetővé teszi, hogy nem csak természetes személyek, hanem jogi személyek is érintettnek minősüljenek, ami differenciált megközelítést tesz lehetővé a személyes adatok jogellenes kezelésével szemben, ahol kizárólag természetes személyek számítanak érintettnek.(Szomora 2019)

A levéltitok megsértése egy alárendelt jogi tényállás, amely csak abban az esetben alkalmazható, ha az adott cselekménnyel nem következik be súlyosabb bűncselekmény, mint például tiltott adatszerzés, minősített adatokkal való visszaélés, jogosulatlan titkos információgyűjtés vagy gazdasági titok megsértése.

Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

Az informatikai bűncselekmények saját fejezetet kaptak a Büntető Törvénykönyvben, az Európai Unió 2013/40 irányelvének megfelelően, amely az információs rendszerek elleni támadásokkal foglalkozik. Az irányelv átültetése révén a jogszabályok megújultak, a korábbi

„számítástechnikai rendszer” fogalom helyett az „információs rendszer” terminológiát használja a Kódex. Háttérként érvényesül még az Európai Tanács 2004. évi LXXIX. törvénnyel kihirdetett ún. Budapesti Egyezménye. Szükséges azonban az adat- és információbiztonsági jogforrások, mint mögöttes normaanyagok alkalmazása is. Ilyen jogforrás például a hálózati és információs rendszerek biztonságának egységesen magas uniós szintjét előíró (EU) 2016/1148 irányelv, továbbá az ezt kiegészítő, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) és annak végrehajtási rendeletei. (Szathmáry 2022)

A Btk. külön fejezetben, a Tiltott adatszerzés és információs rendszer elleni bűncselekmények (XLIII. fejezet) címszó alatt foglalkozik az információs rendszerek elleni támadásokkal, többek között a tiltott adatszerzés (Btk.422. §), az információs rendszer vagy adat megsértése (Btk.423. §), valamint az információs rendszer védelmét biztosító technikai intézkedések kijátszása (Btk.424. §) bűncselekményeivel. Emellett a vagyon elleni bűncselekmények között önálló tényállásként kezeli az információs rendszer felhasználásával elkövetett csalást (Btk.375. §).

A tiltott adatszerzés bűncselekményének jogi tárgya, a személyes adat, magántitok, gazdasági titok, üzleti titok védelme. Elkövetési tárgyai másnak a lakása (Btk. 221. §), a közlést tartalmazó zárt küldeménye (Btk. 224. §), illetőleg az elektronikus hírközlő hálózat. [Btk. 459. § (1) 21. c)] A Btk. az elkövetési magatartások között olyan titkos módszereket és eszközöket sorol fel, amelyeket a bűnüldöző hatóságok jogszerű eljárásuk során csak bírói vagy az igazságügyért felelős miniszter által kiadott engedéllyel használhatnak fel, mint például a titkos adatszerzés vagy titkos információgyűjtés. (Karsai, 2019) Az első alapeset közül elkövetési magatartásai, a titkos helyiségek átkutatása, technikai eszközökkel történő megfigyelés, zárt küldemények jogosulatlan felbontása, elektronikus hírközlő hálózatokon és információs rendszereken továbbított adatok jogosulatlan kifürkészése és rögzítése. A második alapesetnél a célzat kiemelt jelentőségű. A bűncselekmény második alapesete a fedett nyomozók, illetve bűnüldöző hatóságokkal vagy titkosszolgálattal titkosan együttműködő személyek kilétüknek vagy tevékenységüknek felderítése céljából történő információgyűjtésre irányul. A bűncselekmény harmadik alapesete azonosított személyes adatok, magántitkok, üzleti vagy gazdasági titkok jogosulatlan továbbítására vagy felhasználására összpontosít. Itt a hangsúly azokon az információkon van, amelyeket az elkövető birtokol vagy amelyekhez valamilyen módon hozzájutott, és ezeket az információkat illetéktelenül használja fel vagy osztja meg harmadik felekkel. A cselekmény magában foglalhatja az adatok digitális vagy fizikai formában történő továbbítását, valamint az információk különböző célokra történő felhasználását, például gazdasági előnyök elérését vagy mások kárára történő felhasználást. Elkövetési magatartásai

súlyosan sértik az érintettek személyes adatokhoz és magánélethez való jogait, valamint fenyegetést jelentenek az adatbiztonságra és az információs rendszerek integritására (Molnár 2016).

A pilóta nélküli járművek által történő kifürkészés is tiltott adatszerzés.[422/A. § (1)] A jogalkotó, a drónok által nyújtott új technológiai lehetőségekre és a magánélet védelmének kihívásaira válaszul, ezt a tevékenységet tiltott adatszerzésnek minősítette, ennek nem tényállási eleme azonban a titkosság.

Az információs rendszer vagy adat megsértése (Btk.423§) jogi tárgya, az információs rendszerek zavartalan működése, valamint az abban tárolt adatok hitelessége és bizalmas jellegének megőrzése. Tipikusan a DDoS- és a malware-támadások az információs rendszer vagy adat megsértése körébe tartozó cselekmények .Elkövetési tárgyuk, az információs rendszer maga, beleértve annak minden részét és a benne tárolt adatokat. Adott esetben egymástól elkülönítve az egyes számítógépet, az informatikai rendszert, valamint a számítógépes programokat és elektronikus adatokat. (Nagy 2020).

Az információs rendszer akadályoztatása kapcsán a törvény az elkövetési módokat nyitva hagyja, így a tényállás nem korlátozódik csak az informatikai műveletekre, úgy, mint adatbevitel vagy törlés, hanem magában foglalhatja a rendszer működését akadályozó bármilyen behatást is, például egy szerverszoba hűtőrendszerének megrongálását. A törvényi szöveg nyitottsága azt is felveti, hogy milyen esetek minősülnek akadályozásként: csak azok, ahol a rendszer működésképtelensége a rendszeren belüli hiba miatt következik be, vagy bármely helyzet, amikor az információs rendszer nem képes az elvárt funkció ellátására, függetlenül attól, hogy üzemzavar vagy hiba áll-e fenn (Szathmáry 2022)

Az elkövetési magatartások közül a második fordulat - az információs rendszer működésének jogosulatlan vagy jogosultság kereteit megsértő akadályozása [423. § (2) bekezdés a)] - az Irányelv 4. cikkének, mint „rendszer érintő jogellenes beavatkozás”, az adat jogosulatlan, vagy jogosultság kereteit megsértő törlése, vagy hozzáférhetlenné tétele [423. § (2) bekezdés b)] az Irányelv 5. cikkének mint „adatot érintő jogellenes beavatkozás” a magyar szabályozásba történő átültetésének feleltethető meg (Grund 2021)

Az információs rendszer vagy adat megsértése kapcsán adatok hozzáférhetlenné tétele akkor következik be, amikor a jogosult személy nem tud hozzáférni az adatokhoz, nem képes azokon műveletet végezni, vagy az általuk hordozott információkat használni. Ez történhet az adatok titkosításával, áthelyezésével vagy a hozzáférés technológiai úton történő megtagadásával, például ransomware által. Ebben az esetben az adatok megmaradnak, de a jogosult nem fér hozzá az adatokhoz.

Egyetértve Szathmáry felvetéseivel, a „fizikai külső” tényezők biztosítását, és az informatikai rendszer működőképességének biztosítását is szükségesnek tartom. Az adatbiztonsági intézkedések alapján az adatkezelő vagy az adatfeldolgozó megfelelő műszaki és szervezési intézkedéseket tesz. [Infotv a 25/I §. (1).] Biztosítja „az adathordozók (...) eltávolításának megakadályozását,[Infotv. 25/I.L.(3)b)] valamint hogy „üzemzavar esetén az adatkezelő rendszer helyreállítható legyen”[Infotv. 25/I.L.(3)i)] „valamint azt, hogy az adatkezelő rendszer működőképes legyen”[Infotv. 25/I.L.(3)j)]. Mindezek alapján a fizikai tényezők által, és a rendszer működésének egyéb módon történő akadályoztatásait is a tényállás részeinek kellene tekinteni. Jelenleg a számítógépes rendszerek mechanikus - technikai védelmét ez tényállás nem tartalmazza, azt a rongálás törvényi tényállása adja (Molnár 2016).

Információs rendszer védelmét biztosító technikai intézkedés kijátszásának (Btk.424.§) jogi tárgya az információs rendszerek zavartalan működéséhez, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint titokban maradásához fűződő érdek.

Elkövetési tárgya a károkozói adatvisszaélés, (Btk. 375.§ /Btk 423.§) a tiltott adathalászat egy formája, a bűncselekmények elkövetését elősegítő vagy lehetővé tevő eszközök és ismeretek, mint például jelszavak, kódok, számítástechnikai programok, valamint az ezek készítéséhez szükséges szakmai tudás, és nem maguk a felsorolt eszközök.

Elkövetési magatartása, jelszavak vagy számítástechnikai programok készítése, átadása, hozzáférhetővé tétele, megszerzése, vagy forgalomba hozatala, jelszó vagy számítástechnikai program készítéséhez szükséges gazdasági, műszaki, szervezési ismeretek más személyek rendelkezésére bocsátása, akár ha ezeket az ismereteket a Darkneten szerezték meg.

A bűncselekmény alanya bárki lehet, aki szándékosan vesz részt a fenti tevékenységekben.

Az információs rendszer felhasználásával elkövetett csalás a vagyon elleni bűncselekményekről szóló XXXVI. fejezetben a 375. § alatt szerepel. Az információs rendszer felhasználásával elkövetett csalás ún. károkozó adatvisszaélés, és a készpénz-helyettesítési fizetési eszközzel visszaélés egyes alakzatainak összevonásával jött létre. (Szomora 2012).Jogi tárgya az információs rendszer vagy annak bármely eleme, valamint az információs rendszer szempontjából releváns adat.

A tényállás szerkezete szerint a bűncselekmény két fő alakzatot különböztet meg.

Az egyik a károkozó adatvisszaélés ,ami az információs rendszerbe jogtalanul bevitelt, a rendszerben kezelt adatok jogosulatlan módosítását, törlését, vagy hozzáférhetetlenné tételét, valamint az információs rendszer működésének egyéb módon való befolyásolását foglalja magában, amennyiben ezek a cselekmények jogtalan haszonszerzés céljából kárt okoznak.

A másik, az elektronikus készpénz-helyettesítő fizetési eszközzel visszaélés. Ez magában foglalja a hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszközök használatát vagy az ilyen eszközökkel történő fizetés elfogadását, amennyiben ez kárt okoz (Tóth D. 2019).

Ez a tényállás kiegészíti a hagyományos csalás bűncselekményét, lehetővé téve, hogy az információs rendszerek útján elkövetett vagyoni károkozást, amely nem jár természetes személyek megtevesztésével, büntetőjogilag szankcionálják.

Az információbiztonság elleni cselekmények nemcsak a közvetlenül védett információs rendszert érintik, hanem annak szélesebb környezetében, a rendszerelemeken keresztül is megvalósulhatnak. Az információs rendszer biztonságát közvetlenül érintő támadások tipikusan az információs rendszer vagy adat megsértése (Btk.423. §.) tényállás alá esnek, míg a közvetett vagy előkészítő jellegű tevékenységek, mint például a social engineering vagy a jelszavak és egyéb azonosítók megszerzésére irányuló adathalászat, amelyek az információs rendszert kezelő személyeket célozzák, az információs rendszer védelmét biztosító technikai intézkedések kijátszása (Btk.424. §) szerint minősülhetnek.

A jelenleg hatályos Büntető Törvénykönyv szabályozása a személyes adatok védelme és az információs rendszerekkel kapcsolatos tényállások tekintetében összhangban áll az uniós előírásokkal. Ezeket a kereteket az Általános Adatvédelmi Rendelet és a Bűnügyi Adatvédelmi Irányelv alapján az Infotv. határozza meg. A Btk. rendelkezik az uniós jogszabályoknak való megfelelésről. Az egyes szabályozási kérdésekkel kapcsolatban részletesen elemeztem a szakirodalmi álláspontokat, különös tekintettel a személyes adatokkal való visszaélésre vonatkozó tényállásra. A bírói ítélkezési gyakorlat döntő szerepet fog játszani az információs rendszer elleni bűncselekményekkel kapcsolatos pontos jogértelmezés kialakításában.

VIII. Summary

The thesis provides a comprehensive overview of the EU and national legislation on the protection of personal data in the context of the Law Enforcement Directive.

It also analyses in detail the challenges of transposing the Directive into national law and the regulatory issues related to criminal procedure, law enforcement and sanctions. From the perspective of data security and cybercrime protection, it highlights the legal and practical aspects of misuse of personal data and offences against information systems.

The research highlights the importance of the practical application of legislation and the need for harmonisation and uniform interpretation of the law. The final conclusions of the study suggest that close cooperation between the EU and Member States, exchange of best practices and continuous review of the data protection framework are essential to achieve a coherent European data protection regime.

IX. Irodalomjegyzék

Szerzők

Ambrus István. 2021 "Vagyon elleni kriminális cselekmények a modernizálódó kiskereskedelemben." *Ügyészek Lapja* 27, no. 1-2 pp. ISSN 1217-7059.

Ambrus, István. *Digitalizáció és büntetőjog*. Budapest, Magyarország: Wolters Kluwer Hungary, 2021.

Antal Dániel 2010, "A nyilvánosság és a büntetőeljárás," *Studia Iuvenum Iurisperitorium* (5) pp. 217-271.

Arnold, Tom. 2022. "The Early Prediction of Internet Identity Theft and Its Global Impact on Cybersecurity." *Journal of Cybersecurity Research*, 20 (2) p. 32

Bäcker, M. and Hornung, G. 2012, "Data Processing by Police and Criminal Justice Authorities in Europe - The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure", *Computer Law & Security Review*, Vol 28, No. 6, , pp. 627-33.

Bart Custers, Jan-Jaap Oerlemans, és Ronald Pool. 2020. "Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies." *European Journal of Crime, Criminal Law and Criminal Justice*: 121–152.

Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld*. London: Heinemann, 2014

Bederna, Zsolt. 2018 "Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai." *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata* 16, (3) pp.76-103

Békés, Ádám. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." In *A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja*, szerk. P. Polt, B. Miskolczi, T. Török, P. Gasz, Budapest: Opten Informatikai Kft.2016.

Belovics Ervin, Gellér Balázs, Nagy Ferenc, és Tóth Mihály. *Büntetőjog I., Általános rész.* HVG-ORAC. 2014

Belovics, Ervin. "Az emberi méltóság és az egyes alapvető jogok elleni bűncselekmények." In *Büntetőjog II. Különös Rész*, szerk. E. Belovics E.,. Budapest: HVG-ORAC. 2021.

Bendik Tamás 2021. "A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása." In *Magyarozat a GDPR-ról: második, bővített kiadás*, szerkesztette Bendik, Tamás; Árvay, Viktor; Bojnár, Katinka; Eszteri, Dániel; Majsa, Ágnes; Osztopáni, Krisztián; Sziklay, Júlia - Péterfalvi, Attila; Buzás, Péter; Révész, Balázs, pp. 489-506. Budapest, Magyarország: Wolters Kluwer Hungary, pp. 489-506

Bendik Tamás 2020. "A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása." In *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*, szerk. Péterfalvi Attila, 79-109. Budapest, Magyarország: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), pp. 90.

Biegelman, Martin T. *Identity Theft Handbook: Detection, Prevention and Security.* Hoboken, New Jersey: John Wiley and Sons, Inc.2009.

Bolognini, L., "A Proposal for the EU Privacy Law Simplification, Supporting Data-Driven Research in the Law Enforcement Field" Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP), 2020. január 10., <https://www.istitutoitalianoprivacy.it/2020/01/10/a-proposal-for-the-eu-law-simplification-supporting-data-driven>,

Brenner, W. S. 2010. *Cybercrime – Criminal Threats From Cyberspace.* Santa Barbara: Praeger, pp. 39-47.

Brown, A. 2020. "Enhancing Cybersecurity Through Data Protection Measures." *International Journal of Cybersecurity*, 12(4), pp. 321-335.

Brown, A. 2020. "Enhancing Cybersecurity Through Data Protection Measures." *International Journal of Cybersecurity*, 12(4), pp. 321-335.

Brynjolfsson, Erik, and McAfee, Andrew, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.* W.W. Norton & Company. . 2014.

Büntetés-végrehajtás Tudományos Tanácsa. 2015. Korszakváltás a büntetés-végrehajtásban: Útmutató a 2013. évi CCXL (Bv.) törvény megismeréséhez." Budapest: https://bm-tt.hu/wp-content/uploads/2022/02/Korszakvaltas_LO-RES.pdf.

Clough, J. *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2015. pp.10-11.

Cole, Mark D. and Schmitz, Sandra. 2019 "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape." *University of Luxembourg Law Working Paper No. -017* <https://ssrn.com/abstract=3512093> or <http://dx.doi.org/10.2139/ssrn.3512093>.

Czapári, Dóra, és Szőke, Gergely László 2022 "Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása." *JURA* 28, (4) pp. 24-48.

Cséka Ervin, Fantoly Zsanett, Hegedűs István, Kovács Judit, és Maráz Vilmosné *A büntetőeljárás jog alapvonalai. II.* Szeged: Bába Kiadó, 2007 pp. 75-77.

Csiszár, Cs. M. 2019. "Adatvédelem a digitális térben avagy mennyire vagyunk biztonságban." In *Mérleg és Kihívások XI. Nemzetközi Tudományos Konferencia*, szerkesztette Veresné, S. M. és Lipták, K., Miskolc, Magyarország: Miskolci Egyetem Gazdaságtudományi Kar. pp. 62-68

Dimitrova, Diana. and De Hert, Paul. 2018 "The right of access under the Police Directive: Small Steps Forward." In: Medina, M. et al. (szerk.), *Privacy Technologies and Policy*, Lecture Notes in Computer Science, Springer International Publishing, pp. 111–130.

Drechsler, L. 2020, "Comparing LED and GDPR Adequacy: One Standard Two Systems", *Global Privacy Law Review*, Vol.1, No. 2, pp. 93-103.

Dumitrescu, Mihaela-Sorina, and Marica, Mihaela-Emilia. 2019. "Cybercrime in the Digital Era." In Basic International Conference (Ed.), *New Trends in Sustainable Business and Consumption*. Bucharest: Editura ASE. pp. 433-440.

Ebers Martin: Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act In :The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, 2021

<https://ssrn.com/abstract=3900378> or <http://dx.doi.org/10.2139/ssrn.3900378>

Erdei Árpád. *Tanok és tévtanok a büntető eljárásjog tudományában*. Budapest: ELTE Eötvös Kiadó. 2011

Eszteri Dániel, és Péterfalvi Attila. 2022. "Amikor a gépeink tanulnak minket, avagy a mesterséges intelligencia alapú döntéshozatal és profilozás szabályozásának európai unió törekvéseiről." *Századvég* no. 1: pp. 96.

Eszteri Dániel. 2021 "A bűnügyi adatvédelmi irányelv az Infotv. kontextusában." In *Magyarázat a GDPR-ról: második, bővített kiadás*, szerk. Bendik, Tamás; Árvay, Viktor;

Bojnár, Katinka; Eszteri, Dániel; Majsa, Ágnes; Osztopáni, Krisztián; Sziklay, Júlia - Péterfalvi, Attila; Buzás, Péter; Révész, Balázs. Budapest, Magyarország: Wolters Kluwer Hungary, , pp. 489-506.

Eszteri Dániel. 2018 "A bünygyi adatvédelmi irányelv." In *Magyarázat a GDPR-ról*, szerk. Buzás, Péter; Péterfalvi, Attila; Révész, Balázs. Budapest, Magyarország: Wolters Kluwer, , pp. 385-401.

Eszteri, Dániel. 2021 "A bünygyi adatvédelmi irányelv az Infotv. kontextusában." In *Magyarázat a GDPR-ról: második, bővített kiadás*, szerkesztette Bendik, Tamás; Árvay, Viktor; Bojnár, Katinka; Eszteri, Dániel; Majsa, Ágnes; Osztopáni, Krisztián; Sziklay, Júlia - Péterfalvi, Attila; Buzás, Péter; Révész, Balázs, Budapest, Magyarország: Wolters Kluwer Hungary, 489-506

Eszteri, Dániel. 2018 "A bünygyi adatvédelmi irányelv." In: Buzás, Péter; Péterfalvi, Attila; Révész, Balázs (eds.) *Magyarázat a GDPR-ról*. Budapest, Hungary: Wolters Kluwer, , pp. 385-401.

Eszteri, Dániel 2021. "Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás." In *Szemelvények az információs jogokról - a rendszerváltástól napjainkig*, Budapest: Patrocinium Kiadó, pp. 164-193.

Eszteri, Dániel; Péterfalvi, Attila. 2022 "Amikor a gépeink tanulnak minket, avagy a mesterséges intelligencia alapú döntéshozatal és profilozás szabályozásának európai uniós törekvéseiről." *Századvég* (1), pp. 95-119,.

European Union Agency for Cybersecurity (ENISA). (2020). *Threat Landscape for Cybersecurity in the Context of GDPR*. European Union Agency for Cybersecurity.

Fantoly Zsanett és Budaházi Árpád. *Büntető eljárásjogi ismeretek I.* (Budapest: Dialóg Campus Kiadó, 2019.

Fantoly, Zsanett; Herke, Csongor. 2023 "A mesterséges intelligencia a hatékonyabb büntetőeljárás szolgálatában." *Magyar Jog*, 48:(4), pp. 223-228,.

Farina, Katie A. 2021 "Fraud Focus: The Fraudulent Use of Personal Information." *Journal of Financial Crime Prevention* 18, (3) 8.

Fenyvesi Csaba, Herke Csongor és Tremmel Flórián. *Új magyar büntetőeljárás*. Budapest-Pécs: Dialóg Campus Kiadó, 2004

Fenyvesi, Csaba. 2019. "A kriminalisztikai világtendenciák - Különös tekintettel a digitális felderítésre." In *A Bünygyi Tudományok és az Informatika*, pp. 64–82.

Fried, Charles 1968: "Privacy,". *Yale Law Journal* Vol. 77 pp. 475-493.

Furnell, S. 2010. "Hackers, viruses and malicious software." In *Handbook of Internet Crime*, edited by Y. Jewkes and M. Yar, Willan Publishing. pp. 43–45.

Gál, Andor. 2020. "A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről." In *A büntetőjog hazai rendszere megújításának koncepcionális céljai és hatásai*, szerk. M. Hollán, K. Mezei, 134. Budapest: Társadalomtudományi Kutatóközpont Jogtudományi Intézet. pp.133-146.

Gál István László. 2021. "A minősített adattal visszaélés néhány kriminológiai problémaköre." In *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est*, szerk. Barabás Andrea Tünde és Christián László, Budapest, Magyarország: Ludovika Egyetemi Kiadó.....

Gál, István László, és Tóth, Mihály 2016. "Az uniós jog és a magyar jogrendszer viszonya - büntető anyagi jogi jogharmonizáció." In *Az uniós jog és a magyar jogrendszer viszonya*, szerkesztette Tilk Péter, Pécs: PTE Állam- és Jogtudományi Kar, pp. 463-494.

Gáti Balázs 2021. "Az adatvédelem számítástechnikai bűnözéssel összefüggő aktuális kérdései - Adatvédelmi kérdések a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv Tervezetével kapcsolatban." In: Kóhalmi, László (szerk.) PhD Tanulmányok 15. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, pp. 23-58.

Gáti Balázs. 2022 "Az adatvédelmi szabályozás aktuális tendenciái a büntető igazságszolgáltatás területén." In *IV. PhD konferencia kötet*, szerkesztette Bendes Ákos László, Gáspár Zsolt, Gáti Balázs, Projics Nárcisz, Tóth Dávid, Pécs: PTE-ÁJK, Doktori Iskola, pp. 42-61.

Gáti Balázs. 2022."Az adatvédelmi jog fejlődésének főbb állomásai." *Studia Iurisprudentiae Doctorandorum Miskolciensium* 23, no. 1 pp.153-168.

Gáti, Balázs. 2023."A gazdasági válság hatásai a személyes adatok védelmére és annak büntetőjogi aspektusaira." In *Válságok és büntetőjog: Fiatal büntetőjogászok első konferenciája*, szerkesztette Nagy, Melánia; Ripszám, Dóra, Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 67-92.

Gáti, Balázs. 2022."A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései." In *FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI: KONFERENCIAKÖTET – VÁLOGATOTT TANULMÁNYOK*, szerkesztette Bujtár, Zsolt; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics,

Botond; Ferencz, Barnabás; Ázsoth, Szilvia; Szívós, Alexander Roland; Martin, Márton, Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 59-78.

Gáti, Balázs. 2022. "A Schrems II ítélet lehetséges hatásai a nemzetközi jogalkotásra." In *Az internet és a közösségi média jogi kihívásai – Konferenciakötet*, szerkesztette Tóth, Dávid, Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, pp. 18-35.

Gáti, Balázs. 2021. "Az adatvédelem számítástechnikai bűnözéssel összefüggő aktuális kérdései - Adatvédelmi kérdések a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv Tervezetével kapcsolatban." In *PhD Tanulmányok 15*, szerk. Köhalmi, László, Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, pp. 23-58.

Gombos, Katalin. *Az Európai Unió Joga*. Budapest: Patrocinium Kiadó, 2017.

Görög, M., Menyhárd, A., és Koltay, A. "A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül." ELTE ÁJK, Budapest 2017

Grabosky, Peter. *Cybercrime*. Oxford: Oxford University Press, 2016.

Grabosky, Peter. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2: pp. 243-249.

Grund, Borbála. 2021. "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról." *MTA LAW WORKING PAPERS*, 2, pp. 1-37

Gyaraki Réka. 2012. "A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN-kód megadása sikeres vagy biztonságos az internet?!" *Pécsi Határőr Tudományos Közlemények XIII*: pp. 237–238.

Gyaraki Réka. 2023 "Az adatokkal kapcsolatos visszaélések és az információs rendszerben tárolt adatok sértetlensége." In *A kiberyomozói munka büntetőjogi sajátosságai*, szerk. Kovács Zoltán, 90. Budapest, pp.86-113.

Gyaraki, Réka. 2022 "A digitális biztonság új kérdései." In *Metaverzum: Az állam requiemje?*, szerkesztette Beer, Miklós; Gyaraki, Eszter; Kondorosi, Ferenc; Sereg, Szabolcs; Virág, Dániel, Budapest, Magyarország: Kornétás Kiadó pp.33-63.

Háger Tamás. 2014 "A nyilvánosság mint a tisztességes eljárás egyik garanciája a büntetőperben." In: *Pro Futuro* 1, pp.46-61

Hannes Westermann, Michael Joyce, and Benoit Dupont: *Artificial Intelligence in the Context of Crime and Criminal Justice*. Korean Institute of Criminology 2018.

Havasiné Kulcsár, Petra. 2017. "A tárgyalás nyilvánossága, a tárgyalás nyilvánosságának korlátozása. A sajtó jelenléte a büntetőeljárásban: avagy a nyilvánosság fogságában." In: *Büntetőjogi tanulmányok*, 18. köt. Budapest, Magyarország: Matarka Kiadó pp. 51-81.

Herke Csongor 2021. "A kiberbűnözés és a teljesen önvezető járművek." In *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est*, szerk. Barabás Andrea Tünde és Christián László, Budapest, Magyarország: Ludovika Egyetemi Kiadó. pp. 211-221.

Herke Csongor, *Magyar büntető eljárásjog* Pécs: PTE Állam- és Jogtudományi Kar, 2021.

Herke Csongor, *Büntető eljárásjog* Egyetemi jegyzet Pécsi Tudományegyetem Állam- és Jogtudományi Kar Pécs, 2018

Herke Csongor. 2023. "Mesterséges intelligencia a büntetőjogi döntéshozatalban." *Jogtudományi Közlemény* 78, no. 4: pp. 165-176.

Hesz, Tibor és Köhalmi, László. 2009. "A tanúvédelem a terhelt védőjének aspektusából." In *A tanú védelmének elméleti és gyakorlati kérdései*, szerkesztette Mészáros Bence, Pécs: Pécsi Tudományegyetem, Gazdasági Büntetőjogi Kutatóintézet, pp. 97-107.

Hinkel Tamás. 2020. "A mesterséges intelligencia térhódítása a büntetésvégrehajtásban." *Börtönügyi Szemle*, no. 4: pp.13-29.

Hirvonen, P. 2022. "A Review of GDPR Impacts on Information Security." In *PACIS 2022: Proceedings of the 26th Pacific Asia Conference on Information Systems, AI-IS-ASIA: Artificial Intelligence, Information Systems, in Pacific Asia*, Article 83.

Holt, Thomas J., and Bossler, Adam. 2015. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Edited by Richard Wortley. London: Routledge. <https://doi.org/10.4324/9781315775944>

Holt, Thomas J., Bossler, Adam M., and Seigfried-Spellar, Kathryn C. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. London: Routledge. 2022.

Horváth T. XXI. Fejezet az emberi méltóság és egyes alapvető jogok elleni bűncselekményekről. In *Magyar büntetőjog: különös rész*, szerk. I. Görgényi, et al., Budapest: Wolters Kluwer Magyarország. 2020

Gál, István László. "A pénz-és bélyegforgalom biztonsága elleni bűncselekmények," *Új Btk. kommentár: 7. kötet, Különös rész*, (ed. P. Polt), Nemzeti Közsolgálati és Tankönyv Kiadó, Budapest 2013, pp. 193–224.

Jánosi, Andrea. 2022. "Bűnüldözési célú adatkezelés – releváns EU jogforrások, az EU rendszereinek interoperabilitása." *Miskolci Jogi Szemle: A Miskolci Egyetem Állam- és Jogtudományi Karának Folyóirata*, 17:5, pp. 151-161.

Jánosi, Andrea. 2022. "A Magyar büntügyi nyilvántartási rendszer az Európai Unió által megfogalmazott elvárások tükrében." *Miskolci Jogi Szemle* 16, no. 5.: Miskolc, Magyarország. pp. 247-258.

Jóri András. Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. Pécs, 2009.

Jóri András. IV. fejezet. A rendelet hatálya. In *A GDPR magyarázata*, szerk. Jóri András, Budapest: HVG-ORAC Lap- és Könyvkiadó 2018.

Jóri András. *Adatvédelmi kézikönyv*. Budapest: Osiris, 2005.

Jóri András. *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. Pécs, 2009.

Kahn, Charles M., and William Roberds. 2008. "Credit and Identity Theft." *Journal of Monetary Economics* 55: p. 251-264,

Karsai, Krisztina. "Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerkesztette Karsai, Krisztina, pp. 989-996. Budapest, Magyarország: Wolters Kluwer.2019

Király Tibor, *Büntetőeljárás jog* Budapest: Osiris Kiadó, 2000.

Kiss, Tibor.évszám, "Kiberbűnözés." In *Alkalmazott Kriminológia*, szerkesztette Barabás A. Tünde, pp.445-461.

Knoops, Bert-Jaap. 2010. "The Internet and its Opportunities for Cybercrime." *Tilburg Law School Legal Studies Research Paper Series*, 9, pp. 735-754,

Kokott, Juliane – Sobotta, Christoph 2013: "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" *International Data Privacy Law*, 4 pp.222-228.

Kondás Katalin. 2021. "Biometria a börtönben." In: Biztonságtudományi Szemle, OE, 3. évfolyam 4. szám. ISSN 2676-9042., pp. 1-10. [Online]. Elérhető: <https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/185>

Kondás Katalin. 2018. "Adatok védelme a börtönökben." *Hadmérnök* XIII. évfolyam, 1. szám pp. 269-277.

Kóhalmi László. A pénzhamisítással kapcsolatos bűncselekmények. A pénz büntetőjogi fogalma, Büntetőjog II. Különös Rész – Jogi Szakvizsga Segédkönyvek. (ed. Á. Balogh) Dialóg Campus Kiadó, Budapest–Pécs 2005, pp. 411–417.

Kóhalmi László. 2022. "Nyilvánosság és büntetőeljárás." In Az internet és a közösségi média jogi kihívásai, szerkesztette Tóth Dávid. Konferenciakötet. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetésvégrehajtási Jogi Tanszék, Pécs, pp.36- 46.

Kóhalmi, László. "A nemzetközi bűnügyi együttműködés." In *Magyar büntetőjog: Általános rész*, szerkesztette Balogh Ágnes és Tóth Mihály, Budapest: Osiris Kiadó, 2010. pp. 375-386.

Kóhalmi, László 2012. "Európai biztonság avagy az egységes európai büntetőjog víziója." In *A rendészettudomány határkövei: Tanulmányok a Pécsi Határőr Tudományos Közlemények első évtizedéből*, szerkesztette Gaál Gyula és Hautzinger Zoltán, Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, pp. 257-276.

Kóhalmi, László 2013. "The Human Rights in the Criminal Procedure." In: Magdalena Sitek, Gaetano Dammacco, Aleksandra Ukleja és Marta Wojcicka (szerk.), *Europe of Founding Fathers: Investment in the Common Future*. Olsztyn, Lengyelország: University of Warmia and Mazury, Faculty of Law and Administration, pp. 397–407.

Krasznay, Csaba. 2021. "Húsz év a globális kiberbűnözés elleni küzdelemben - A Budapesti Egyezmény értékelése." *Külföldi Szemle*, 20: Különszám, Paper: 9, pp. 191-214

Leiser, M, Custers, B. 2019, " The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680", *European Data Protection Law Review*, Vol. 5, No. 3, , pp. 367-78.

Lynskey, Orla. 2019. "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection Against Predictive Policing." *International Journal of Law in Context* 15, no. 2: pp. 162-176.

Majtényi László. "Az információs jogok." In *Emberi jogok*, szerk. Halmai Gábor és Tóth Gábor Attila, Budapest: Osiris, 2003. pp. 582-583.

Majtényi László. "Az információs jogok," In *Emberi jogok*, szerk. Halmai Gábor és Tóth Gábor Attila Budapest: Osiris Kiadó, 2008, 579–581.

Márki, Dávid. "Az igazságszolgáltatás nyilvánosságának alkotmányjogi vizsgálata: Alapjogi kollíziók a büntetőeljárás, a sajtó és a politika keresztműzében." Szeged, Magyarország: Iurisperitus Kiadó, 2023. https://publicatio.bibl.u-szeged.hu/27808/1/Marki_2023_07_05.pdf

Máté István Zsolt. 2018. "Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe." *Belügyi Szemle*, 66, (7-8), pp. 36-54.

McGuire, M., and Dowling, S. 2013. Cyber-dependent crimes. In *Cyber crime: A review of the evidence* (Research Report 75, Chapter 1). Law, Computer Science. pp. 4-29.

Mezei Kitti. 2018 "Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására." *JURA* 24, no. 1: pp. 349–360.

Mezei Kitti. 2019. "Szervezett bűnözés az interneten." *A bűnügyi tudományok és az informatika*, 125. Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, p.125-147.

Mezei Kitti. 2020. "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre." *Állam- és Jogtudomány* 61,(4), pp 65-81.

Mezei Kitti. 2022. "Diszkrimináció az algoritmusok korában." *Magyar Jog* 2022, no. 6: pp. 336-337.

Mezei, Kitti. 2023. "A kiberbűnözés szabályozási kihívásai a büntetőjogban." https://real.mtak.hu/104974/1/Mezei_UL_201945.pdf, 22.

Miskolczi Barna és Szathmáry Zoltán. 2019. *Büntetőjogi kérdések az információk korában*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., pp. 140-141.

Molnár Gábor 2016. "XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In Kónya Sándor (szerk.), *Magyar büntetőjog – Kommentár a gyakorlat számára*. Budapest: HVG-ORAC, pp. 971–972.

Moore, T. & Anderson, R. 2019. "Rethinking Information Security to Improve Data Privacy," *European Journal of Information Systems*, 28(5), pp. 687-694.

Nagy, Zoltán András, Mezei Kitti. 2018 "Az Európai Unió Bűnügyi Adatvédelmi Irányelvéről." In *A XXI. század biztonsági kihívásai*, szerk. Gaál, Gyula; Hautzinger, Zoltán. Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, pp. 229-234.

Nagy, Zoltán András. 2020. "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor, Budapest: Dialóg Campus pp. 45-64.

Nagy, Zoltán András. *Bűncselekmények számítógépes környezetben*. Budapest: Ad Librum 2009.

Nagy, Zoltán András. 2021. "Mesterséges intelligencia a bűnügyi munkában." In *Sokszínű Kar Konferencia III.: Absztraktfüzet*, szerk. Ürmösné Simon Gabriella és Kudar Mariann, 9. Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar...

Nagy, Zoltán András. 2020 "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor, Budapest: Dialóg Campus 2020.

Nagy, Zoltán András. 2014 "A számítógépes környezetben elkövetett bűncselekmények új szabályozásáról. Háttér és elemzés." *Ügyészek Lapja*, 3-4. sz., pp. 31-45.

Nagy, Klára. 2010. "Adatvédelem a rendőrségi és bűnügyi együttműködés során a Lisszaboni Szerződés után." In *Tanulmányok "Quo vadis rendvédelem? Szabadságjogok, társadalmi kötelezettségek és a biztonság" című tudományos konferenciáról*, szerkesztette Gaál, Gyula és Hautzinger, Zoltán, Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, pp. 81-88.

Naudts, L. "The Data Protection Impact Assessment for Law Enforcement Agencies" (Adatvédelmi hatásvizsgálat a bűnüldöző szervek számára), előadás a 12. Nemzetközi Kommunikációs Konferencián, Bukarest, Románia, 2018. június 15.

Navratil Szonja. Az igazságszolgáltatás nyilvánossága. Összehasonlító elemzés. In *A bírói függetlenség, a tisztességes eljárás és a politika*, szerkesztette Badó Attila, Budapest: Gondolat Kiadó. 2011.

Németh, Kata. 2019 "A büntetőeljárás nyilvánosságának jogszabályi háttérében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." *Debreceni Jogi Műhely* 16, no. 1-2 pp. 291-320.

Nyeste, Péter. 2019. "A bűnüldözési tevékenység során használt fontosabb nyilvántartások." In *A bűnügyi hírszerzés kézikönyve*, edited by Sub Lege Libertas, Budapest: Nordex Nonprofit Kft.; Dialóg Campus Kiadó. ISBN 978-615-5945-79-3 (nyomtatott); 978-615-5945-84-7 pp. 181-199. https://real.mtak.hu/128819/1/Web_PDF_A_bunugyi_hirszerzes_kezikonyve.pdf

Nyiri, Sándor. 2018. "A nyomozóhatóságok és az ügyészség kapcsolata a büntetőeljárásról szóló törvényben," *Belügyi Szemle* 66. évf. 6. szám, pp. 5–16.

Oswald, Marion, Jennifer Grace, Stephanie Urwin, and Geoffrey Barnes. 2018. "Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality." *Information & Communications Technology Law* 27, no. 2: pp. 223-250.

Osztopáni, Krisztián 2018: „Jogalapok” In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest

Palánkai, Tibor. 2019. "Integráció és kohézió az EU-ban." In *Tagállami integrációs modellek*, pp. 27–50.

Pálvölgyi, Ákos. 2014 "A hírérték margóján: személyhez fűződő jogok védelméhez való jog a büntetőeljárásban különös tekintettel a személyes adatok védelmére." *Büntetőjog Szemle*, no. 3: pp. 41-45.

Parti K. és Kiss T. 2017. "Az informatikai bűnözés." In *Kriminológia*, szerk. Borbíró A., Gönczöl K., Kerezsi K., és Lévay M., Budapest: Wolters Kluwer. pp. 491–493.

Péterfalvi Attila – Eszteri Dániel. 2017 "A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata." In *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*, szerk. Görög Márta – Menyhárd Attila – Koltay András, ELTE-ÁJK, Budapest, pp.405-420

Péterfalvi Attila. 2020. "Az adatvédelem fejlődésének történeti áttekintése Magyarországon a GDPR hatálybalépéséig." In *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*, szerk. Péterfalvi Attila. Budapest: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), pp. 29–78

Péterfalvi, Attila; Bendik, Tamás; Tóásó, Bálint. 2019 "A módosított Infotv. és a GDPR alkalmazásának első tapasztalatai." Konferencia előadás, 42. Jogász Vándorgyűlés, Miskolc-Lillafüred, Magyarország., pp. 1-12.

Petrik Ferenc. Alkotmány a gyakorlatban, kommentár a gyakorlat számára, HVG-ORAC, Budapest, 2009.

Porcedda, Maria Grazia. 2012. "Data Protection and the Prevention of Cybercrime - The EU as an Area of Security?" *EUI Working Papers LAW*, No. 25
<https://ssrn.com/abstract=2169340> or <http://dx.doi.org/10.2139/ssrn.2169340>.

Quezada-Tavárez, K., Vogiatzoglou, P. and Royer, S. 2021, "Legal Challenges in Bringing AI Evidence to the Criminal Courtroom", *New Journal of European Criminal Law*, Vol. 12, No. 4, pp. 531-551.

Róth, Erika. 2021. "A digitalizáció és a terhelti jogok érvényesülése a büntetőeljárásban." *Miskolci Jogi Szemle* 16, no. 1, különszám pp. 270-278.

Sajfert, J., and T. Quintel. 2016. "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities." *European Data Protection Law Review* 2, no. 3. pp. 397-408.

Schmehl Gábor Dániel. 2020. "SMART eszközök és egyedi alkalmazások a magyar büntetés-végrehajtásban." *Börtönügyi Szemle*, no. 4: pp. 49-69.
http://epa.niif.hu/02700/02705/00124/pdf/EPA02705_bortonugyi_szemle_2020_4.pdf

Schreiber, T. *Data Protection and Cybersecurity Law*. Oxford: Oxford University Press. 2021.

Schwab, Klaus. *The Fourth Industrial Revolution*. World Economic Forum, 2016.

Sieber, U. 1993. "A számítógépes bűnözés és más bűncselekmények az információtechnológia területén." *Magyar Jog*, no. 2: pp. 105–109.

Simon, Béla, Gyarak, Réka. "Kiberbűncselekmények felderítése és nyomozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss, Tibor, 121-150. Budapest, Magyarország: Dialóg Campus Kiadó, 2020.

Sólyom László. 2004. "Az adatvédelem és információszabadság előtörténete Magyarországon." In *Az elektronikus információszabadság*, szerk. Majtényi László, Budapest: Eötvös Károly Intézet (EKINT), pp. 174-183.

Somssich, Réka. 2020. "A jogharmonizációs kötelezettségek teljesítésének módszertana és eszköztrendszere 15 évvel a csatlakozás után." *Állam- és Jogtudomány LXI*, no. 2: 44-50.

Sorbán, Kinga. 2016 "A digitális bizonyíték a büntetőeljárásban." *Belügyi Szemle*, 64 ,11, pp. 81-96.

Sorbán, Kinga. 2019. "Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában: Felelősség és kötelezettségek." In *Medias Res*, VIII, 1, pp. 84-101,

Szabó I. "Informatikai bűncselekmények." In *Az informatikai jog nagy kézikönyve*, szerk. Dósa I. Budapest: Complex. 2008.

Szabó Máté Dániel. 2005. "Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival." *Információs Társadalom /5*, pp. 44-54.

Szathmáry Z. 2012. "Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban." Doktori értekezés, Pécsi Tudományegyetem ÁJK Doktori Iskolája Informatikai és Kommunikációs Jog Program, Budapest, pp. 79–80.

Szathmáry Zoltán 2019. "A mesterséges intelligencia hatása a büntetőjogi felelősségre." *Ügyészek Lapja*, 26 (3), pp. 37-46.

Szathmáry Zoltán 2022: *Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.*, *Infokommunikáció és Jog*, 2. pp. 6-10.

Szathmáry Zoltán: 2023 "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése II.", *Infokommunikáció és Jog*, 1. (80.), pp. 11-13.

Szendrei, Ferenc. 2019. "Bűnügyi Együttműködés." In *A Bűnügyi Hírszerzés Kézikönyve*, szerkesztette: Szendrei Ferenc, Dialóg Campus Kiadó, pp. 221–242.

Szijártó, István. 2019. "Az Europol és az Eurojust szerepe a közös nyomozócsoportokban." *Ügyészek Lapja*, 26:6, pp. 59-73.

Sziklay Júlia és Bendik Tamás. "Az adatvédelem hazai és európai uniós szabályozása és alapintézményei." Budapest: NKE, 2018.

Szomora Zsolt. "Btk. XXI. fejezet." In *Kommentár a Büntető Törvénykönyvhöz*, szerk. Karsai Krisztina, Budapest: Complex. 2013.

Szomora, Zsolt. "A vagyon elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerkesztette Karsai, Krisztina, Budapest, Magyarország: Wolters Kluwer, 2019.

Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerkesztette Karsai, Krisztina, 492-531. Budapest, Magyarország: Wolters Kluwer, 2019.

Szőke Gergely László. 2013 "Az adatvédelem szabályozásának történeti áttekintése." *Infokommunikáció és Jog*, pp. 107–112.

Szőke Gergely László. 2018. "Big Data and Algorithms in the Public Sector and Their Impact on the Transparency of Decision-Making." In *Central and Eastern European eDem and eGov Days 2018: Conference proceedings*, szerk. Hansen Hendrik, Müller-Török Robert, Nemeslaki András, Prosser Alexander, Scola Dona, és Szádeczky Tamás Wien, Ausztria: Facultas Verlag, pp. 301–311.

Szőke Gergely László. *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*. Budapest: HVG–ORAC Lap- és Könyvkiadó Kft., 2014.

Taylor, S. 2017. "Data Protection Laws and Law Enforcement: A Comparative Analysis." *European Journal of Law and Economics*, 28(1), pp. 89-104.

Tóth Dávid és Nagy Zoltán András. 2015. "Computer related economic crimes in Hungary." *Journal of Eastern-European Criminal Law*, no. 2: pp.165-174.

Tóth Dávid, 2017. "A bankkártyával kapcsolatos bűncselekmények prevenciós eszközei", PEME XV. PhD – konferenciakötet (eds. I. Koncz, I. Szova), Professzorok az Európai Magyarországiért Egyesület, Budapest, pp. 182–192

Tóth Dávid. 2019. "A virtuális pénzekkel kapcsolatos visszaélések." In: Baráth Emőke Noémi – Mezei József (szerk.): *Rendészet-Tudomány-Aktualitások. A rendészettudomány a fiatal kutatók szemével*. Budapest: Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, pp. 242-250.

Tóth Dávid. 2020. "Személyiséglopás az interneten." *Büntetőjogi Szemle*, 1. szám, pp. 116-117.

Tóth, Dávid ? „Az identitáslopás kriminológiai sajátosságai” In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) *A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői* Pécs, Magyarország : Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport pp. 207-213.

Tóth, Dávid. 2023. "The criminal law protection of personal data in Hungary." In *Collection of Papers "Law Between Creation and Interpretation" Vol. 3.*, edited by Čeranić, Dimitrije; Ivanović, Svjetlana; Lale, Radislav; Aličić, Samir, East Sarajevo, Bosnia-Herzegovina: Faculty of Law, University of East Sarajevo. ,pp. 233-246.

Varga Petra, 2018. A nyilvánosság elvének érvényesülése a büntetőeljárásban**Debreceni Jogi Műhely*, XV. évfolyam 1-2. szám, DOI [10.24169/DJM/2018/1-2/9](https://doi.org/10.24169/DJM/2018/1-2/9)

Vogiatzoglou, P. et al. "Assessment of the implementation of the Law Enforcement Directive" Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.209 – 2022.

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press. 2007

Warren, Samuel and Brandeis, Louis 1890: "The Right to Privacy," *Harvard Law Review* IV, no. 5: pp. 193–220., <https://www.jstor.org/stable/1321160?seq=27>

Wicki-Birchler, David. 2020 "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?" *International Cybersecurity Law Review* 1 pp. 63-72. <https://doi.org/10.1365/s43439-020-00012-5>.

Winter, H.B. et al, De verwerking van politiegegevens in vijf Europese landen, Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, 2020.

Felhasznált jogszabályok

(EU) 2016/680 Irányelv a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók

végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről." *Hivatalos Lap L 119* (2016. május 4.): 89–131.

(EU) 2018/1727 Rendelet az Európai Unió ügynökségeként működő Eurojustról,

14/2002. (VIII.1.) IM rendelet – a bírósági ügyvitel szabályairól

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

2003. évi XLVIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról

2009. évi XLVII. törvény a bünyügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bírósági által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bünyügyi és rendészeti biometrikus adatok nyilvántartásáról

2010. évi CIV. tv – a sajtószabadságról és a médiatartalmak alapvető szabályairól.

2010. évi CLXXXV. törvény a médiaszolgáltatókról és a tömegkommunikációról

2011. évi CLXI. törvény a bíróságok szervezetéről és igazgatásáról

2011. évi CLXII. törvény a bírák jogállásáról és javadalmazásáról 22. 43.§-44.§

2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról.

2013. évi CLXV. törvény a panaszokról és a közérdekű bejelentésekről, a törvényt a 2023.évi XXV.törvény, 73.§-a hatályon kívül helyezte, és az hatályos 2023.0.25-től.

2013/40/EU Irányelve(2013. augusztus 12.): Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról." *Hivatalos Lap L 218* (2013. augusztus 14.): 8-14.

2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról.

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

A 2010. évi CIV. törvény, mely a sajtószabadságról és a médiatartalmak alapvető szabályairól

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – A korábbi harmadik pillérhez tartozó vívmányok adatvédelmi szabályokkal való összehangolásának további lépései. COM(2020) 262 final, 2020, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A52020DC02622020>. június 24.

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – Első jelentés az EU biztonsági unió-stratégiájáról," COM (2020) 797 final, 2020. december 9.

A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Mesterséges intelligencia Európa számára."

A büntetés-végrehajtás országos parancsnokának 9/2016. (II.16.) OP szakutasítása a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról

A Számítástechnikai Bűnözésről szóló Egyezményhez csatolt második kiegészítő jegyzőkönyv a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról.*Hivatalos Lap L 63* (28 február 2023): 28–47.

A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról." *Hivatalos Lap L 69/67*, 2005. március 16.

Állásfoglalás a mesterséges intelligenciáról a büntetőjogban, és annak a rendőrség és az igazságügyi hatóságok általi felhasználásáról büntetőügyekben (2020/2016(INI))."

Arkivförordning (1991:446) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivforordning-1991446_sfs-1991-446

Áttekintés az OECD Irányelvekről a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról." Utoljára hozzáférve 2021. szeptember 10. <https://www.oecd.org/sti/ieconomy/15590228.pdf>.

Az Európai Adatvédelmi Biztos Határozata (2020. május 15.) az európai adatvédelmi biztos eljárási szabályzatának elfogadásáról, II. fejezet, 3.cikk(1), https://edps.europa.eu/sites/default/files/publication/20-06-26_edps_rules_of_procedure_hu.pdf

Az Európai Parlament és Tanács. 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról." *Hivatalos Lap* L 8 (2001. január 12.): 1.

Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Unió Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről. *Hivatalos Lap* L 135, 24.5.2016., 53—114. o.

Az Európai Parlament és a Tanács (EU) 2018/1727 rendelete (2018. november 14.) az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről. *Hivatalos Lap* L 295, 2018.11.21., 138—183. o.

Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról." *Hivatalos Lap* L 8 (2001. január 12.): 1–22.

Az Európai Parlament és a Tanács, 1995. 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról." *Hivatalos Lap* L 281 (1995. november 23.): 31–50.

Az Európai Parlament és a Tanács, 2004. Rendelete 460/2004/EK (2004. március 10.): Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról." *Hivatalos Lap* L 77 (13 március 2004).

Az Európai Parlament és a Tanács 2013. Irányelve 2013/40/EU (2013. augusztus 12.): Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról." *Hivatalos Lap* L 218 (2013. augusztus 14.): 8-14.

Az Európai Parlament és a Tanács 2016 Irányelve (EU) 2016/1148 a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről." *Hivatalos Lap* L 194/1 (19 augusztus 2016).

Az Európai Unió Alapjogi Chartája, 2012/C 326/02.

Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata, 2012/C 326/01.
Hivatalos Lap C 326 (2012. október 26.): 47–390.

Bizottság közleménye az Európai Parlamentnek és a Tanácsnak - Első jelentés a bűnüldözésben érvényesítendő adatvédelemről szóló (EU) 2016/680 irányelv alkalmazásáról és működéséről.
COM/2022/364 final.

Brottsdatalog, (2018:1177) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalog-20181177_sfs-2018-1177, (hozzáférés: 2022.07.14)

Bundesgesetzblatt, hatályba lépett 1978. január 1-én.
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl177s0201.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl177s0201.pdf%27%5D__1708963582035.

Bürgerliches Gesetzbuch (BGB), Gesetze im Internet, <https://www.gesetze-im-internet.de/bgb/>

Council of Europe. 2001. *Explanatory Report to the Convention on Cybercrime*. European Treaty Series – No. 185, p. 12. Accessed March 5, 2021. <https://rm.coe.int/16800cce5b>

Code civil, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721

Code pénal, <https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070719>

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy," COM (2020) 605 final

Das Hessische Beamtengesetz in der Fassung vom 16. Februar 1970. URL: <http://starweb.hessen.de/cache/GVBL/1970/00041.pdf>.

Datalog (1973:289). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalog-1973289_sfs-1973-289

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
https://www.bfdi.bund.de/DE/Home/home_node.html

Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." *Official Journal of the European Union* L 333: 80–152.

(EU) 2013/40/EU Irányelv Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról."

Emberi jogok egyetemes nyilatkozata

Emberi Jogok Európai Egyezménye

(EU) 2016/679 Rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)." *Hivatalos Lap L 119* (2016. május 4.): 1–88.

Európai Adatvédelmi Testület. Eljárási Szabályzat, 8. változat." Elfogadva: 2018. május 25.

Európai Gazdasági és Szociális Bizottság. "Véleménye, Fehér könyv a mesterséges intelligenciáról - A kiválóság és a bizalom európai megközelítése," COM(2020)65 final, 2020/C 364/12,. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf.

Föreskrifter om behandling av personuppgifter som rör lagöverträdelser. Datainspektionens författningssamling. Datainspektionen, DIFS 2018:2

Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2007975-med-instruktion-for_sfs-2007-975

Förordning (2013:343) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.,

Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnUG-EU), Deutscher Bundestag, <https://dip.bundestag.de/vorgang/gesetz-zur-anpassung-des-datenschutzrechts-an-die-verordnung-eu-2016-679/79680>.

Javaslat a Mesterséges Intelligenciára Vonatkozó Harmonizált Szabályok Megállapításáról és Egyes Uniós Jogalkotási Aktusok Módosításáról, COM(2021) 206 final, Brüsszel, 2021. április 21.

Javaslat a Tanács Határozata az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményét (108. sz. egyezmény) módosító jegyzőkönyvnek az

Európai Unió érdekében történő megerősítésére a tagállamoknak adott felhatalmazásról, COM(2018) 451 final

Javaslat az elektronikus hírközlés során a magánélet tisztelőben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről szóló rendeletről (elektronikus hírközlési adatvédelmi rendelet), COM (2017) 10 final.

Kreditupplysningslag (1973:1173), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kreditupplysningslag-19731173_sfs-1973-1173,

Lag (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007258-om-behandling-av-personuppgifter-i_sfs-2007-258

Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218,

Lag om Säkerhetspolisens behandling av personuppgifter Utfärdad den 28 november 2019, <https://svenskforsattningssamling.se/sites/default/files/sfs/2019-11/SFS2019-1182.pdf>,

Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról, 2007/C 306/01.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1), <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676/>

LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique , https://www.legifrance.gouv.fr/loda/article_lc/JORFARTI000033202902/

LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (a magyar cím saját fordítás), <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>

Patientdatalag (2008:355), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355

Personuppgiftslag (1998:204), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

Rättsligt ställningstagande IMYRS 2021:1 – innebörden av begreppet ”personuppgifter som rör lagöverträdelse som innefattar brott” i artikel 10 i dataskyddsförordningen, IMYRS 2021:1

Recommendation No. R (85) 10 to Member States Concerning the Practical Application of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the Interception of Telecommunications. <https://rm.coe.int/09000016804e6b5e>.

Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector. <https://polis.osce.org/council-europe-committee-ministers-recommendation-no-r87-15-member-states-regulating-use-personal>.

Recommendation No. R (89) 9 to Member States on Computer-Related Crime." Accessed June 1, 2019. <https://rm.coe.int/09000016804f1094>.

Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology. <https://rm.coe.int/16804f6e76>.

RECOMMENDATION No. R (95) 13 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURAL LAW CONNECTED WITH INFORMATION TECHNOLOGY
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>.

Recommendation No. R (95) 13 to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology.

Recommendation No. R (95) 4 to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services." <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e>.

Recommendations and Declarations in the field of media and information society." In *Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society*, 30-33. <https://rm.coe.int/1680645b44>.

Rendelet (EU) 2018/1725 Rendelet a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről." *Hivatalos Lap* L 295 39–98.

Arkivlag (1990:782) SFS 1990:782-...

Treaty No. 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108).

Treaty No. 181, Kiegészítő jegyzőkönyv az egyének védelméről a személyes adatok automatikus feldolgozása során, a felügyeleti hatóságokról és a határokon átnyúló adatáramlásról.

Treaty Series – No. 185. Convention on Cybercrime. – No. 185. <https://rm.coe.int/1680081561>.

Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU), Gesetz vom 20.11.2019 – BGBl. I 2019, Nr. 41 vom 25.11.2019, S. 1626

Ítéletek / Birósági határozatok

1/2012. számú BJE-határozat.

15/1991. (IV. 13.) AB-határozata.

37138/14 Szabó és Vissy kontra Magyarország, App. no., 2016. január 12., 75-77. pontok.

47143/06 Roman Zakharov kontra Oroszország, App. no., 2015. december 11., 272-285. pont;

873/B/2008. AB határozat.

ABH. 2010, 562

[BH 2019.272](#)

BH 2019.272

BH2013. 146

BH2015. 29

Bírósági Döntések Tára 2019/9/100,

C:2021:504, ECLI:EU

C-131/12 ,<https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=HU>

C-203/15 és C-698/15,

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=188001&pageIndex=0&doclang=HU&mode=req&dir=&occ=first&part=1&cid=397988>

C-205/21. számú Ministerstvo na vatreshnite raboti kontra B. C, Előzetes döntéshozatal – A természetes személyek védelme a személyes adatok kezelése vonatkozásában

C-230/14 Ítélet, <https://curia.europa.eu/juris/liste.jsf?num=C-230/14>

C-293/12 Ítélet, <https://curia.europa.eu/juris/liste.jsf?num=C-293/12>

C-311/18) Ítélet, <https://curia.europa.eu/juris/liste.jsf?num=C-311/18&language=HU>

C-311/18. ítélet Schrems II. ügyben hozott ítélet, ,

<http://curia.europa.eu/juris/document/document.jsf;jsessionid=79A9F6D4C441C1B0E1BB674FF3B58578?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=9719131>

C-34/21 Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium kontra Minister des Hessischen Kultusministeriums

C-439/19 Latvijas Republikas Saeima, , 2021. június 22-i ítélet, ECLI:EU:C:2021:504.

C-505/19, , WS kontra Bundesrepublik Deutschland ECLI:EU:C:2021:376.

C-92/09, Volker und Markus Schecke GbR (Hartmut Eifert (C-93/09) kontra Land Hessen [C-92/09. és C-93/09. sz. egyesített ügyek, ECLI:EU:C:2010:662]

Kúria BHAR.I.537/2017/5. sz. határozata és BH2017. 392.

NAIH- 2868-23/2021.

Weboldalak/URL

Az (EU) 2016/679 rendelettel és az (EU) 2016/680 irányelvvel foglalkozó bizottsági szakértői csoport (E03461); <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461>

CNIL, <https://www.cnil.fr/fr/entree-en-vigueur-de-la-nouvelle-loi-informatique-et-libertes>
DataGuidance, France - Data Protection Overview,
<https://www.dataguidance.com/notes/france-data-protection-overview>

Datareportal. Digital 2019: Global Digital Overview. <https://datareportal.com/reports/digital-2019-global-digital-overview>.

ENISA, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

Európai Parlament. A személyes adatok védelme.
https://www.europarl.europa.eu/ftu/pdf/hu/FTU_4.2.8.pdf.

Integritetsskyddsmyndigheten, <https://www.imy.se>

Pók, László, (2019) 5 kímzó kérdés a Kúria személyes adatokra vonatkozó döntése alapján.
gdpr.blog.hu.

RSM, Impact of the GDPR on Cyber Security Outcomes Final Report ,August 2020,
https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf

Statista. Annual cost of cybercrime worldwide 2017-2028.2023.
<https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>

Sweden - Data Protection Owerweiv, Guidance Note,
<https://www.dataguidance.com/notes/sweden-data-protection-overview>

EDPB/WP állásfoglalások

01/2021 ajánlás a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti
megfelelőségi referenciáról
https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_e_n.pdf

01/2021. számú iránymutatás Az adatvédelmi incidensek bejelentésével kapcsolatos példákra, https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_hu.pdf

01/2022 EDPB Guideline on data subject rights - right of access, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

04/2021. EDPB. Iránymutatás a magatartási kódexekről, mint az adattovábbítás eszközeiről https://www.edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_hu.pdf

05/2021 EDPB Iránymutatás a 3. cikk alkalmazása és az általános adatvédelmi rendelet V. fejezete szerinti, nemzetközi adattovábbításra vonatkozó rendelkezések közötti kölcsönhatásról https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_hu.pdf

05/2022. számú iránymutatás, Az Európai Adatvédelmi Testület 2022. május 12-én elfogadott, az arcfelismerő technológiának a bűnüldözés területén történő használatáról szóló iránymutatása, https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

07/2020 sz. EDPB iránymutatás az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról https://www.edpb.europa.eu/system/files/202310/edpb_guidelines_202007_controllerprocess_or_final_hu.pdf

07/2022 EDPB Iránymutatás a tanúsításról, mint az adattovábbítás eszközéről https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_hu.pdf

4/2019 Guidelines on Article 25 Data Protection by Design and by Default https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_hu

EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_hu

EDPB, https://www.edpb.europa.eu/system/files/202307/edpb_guidelines_202010_art23_adopted_afterpublicconsultation_hu.pdf

EDPB, https://www.edpb.europa.eu/system/files/202404/edpb_guidelines_202201_data_subject_rights_access_v2_hu.pdf

EDPB. Tájékoztató az általános adatvédelmi rendelet alapján az Egyesült Királyságba az átmeneti időszakot követően történő adattovábbításról" (elfogadva 2020. december 15-én). https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_hu.

NAIH/2020/294/4 ügyszámú állásfoglalása

NAIH-4418-5/2012/V, Állásfoglalás a bírósági tárgyalásokról készített MTI tudósítások során nyilvánosságra hozott személyes adatokról.

WP 136, 4/2007, Vélemény a személyes adat fogalmáról. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf,

WP 242 rev.01, 16/HU

https://www.adatvedelmirendelet.hu/wp-content/uploads/wp242rev01_hu.pdf

WP 258, Vélemény a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv ((EU) 2016/680) egyes kulcsfontosságú kérdéseiről– 17., <https://ec.europa.eu/newsroom/article29/items/610178/en> (2022.07.02.)

WP 136. 2007. sz. vélemény a személyes adat fogalmáról https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf

WP 248rev.01 Guidelines on Data Protection Impact Assessment (DPIA), <https://ec.europa.eu/newsroom/article29/items/611236/en>

WP 250rev.01 Guidelines on Personal data breach notification under Regulation 2016/679, <https://ec.europa.eu/newsroom/article29/items/612052>

WP251rev.0117/HU, Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához https://www.naih.hu/files/wp251rev01_hu.pdf

WP260 rev.0117/HU, https://www.naih.hu/files/wp260rev01_hu.pdf