Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

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, 2025

„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 kutató, 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 előmenetelemet.

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

Megtiszteltetés volt számomra velük és minden kedves kollégámmal együtt dolgozni.

Tartalomjegyzék

Bevezetés 7
I.1. A témaválasztás indoklása, aktualitása 9
I.2. A kutatás célja, hipotézisek 13
I.3. A kutatás módszerei 14
I.4. Az értekezés tárgya és felépítése 15
II. Előzmények 16
II.1. Az adatvédelem fogalmával kapcsolatos megfontolások 17
II.2. Az adatvédelmi jog fejlődésének főbb állomásai 20
II.3. Az Európai Unió jelenlegi szabályozása – A személyes adatok védelmének általános jogszabályi háttere és intézményei 23
II.3.1. Az adatvédelmi reform 23
II.3.2. Az Európai Adatvédelmi Biztos, az Európai Adatvédelmi Testület és az Európai Bíróság szerepe 27
II.3.2.1. Az Európai Adatvédelmi Testület (EDPB) 27
II.3.2.2. Európai Adatvédelmi Biztos (EDPS) 30
II.3.2.3 Bűnüldözésű célú releváns irányelvek az EDPB és EDPS gyakorlatában 31
II.3.2.4. Az Európai Unió Bírósága (EUB) 37
III. A Bűnügyi Adatvédelmi Irányelv (LED) - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv és jogharmonizációja 38
III.1. A bűnügyi adatvédelmi irányelv bemutatása 38
III.2. A bűnügyi irányelv jogharmonizációja 56
III.2.1. A bűnügyi irányelv átültetése a magyar nemzeti jogba 58
III.2.1.1. Előzmények 58
III.2.1.2. Implementálás a 2011. évi CXII. törvénybe 59
III.2.2. A bűnügyi irányelv átültetése a német nemzeti jogba 67
III.2.2.1. Előzmények 68
III.2.2.2. A németszövetségi adatvédelmi törvény az adatvédelmi reform után 70
III.2.3 A bűnügyi irányelv átültetése a francia nemzeti jogba 80
III.2.3.1 Előzmények 80
III.2.3.2. A francia adatvédelmi törvény első módosítása, az 1978. január 6-i 78-17. számú törvényhez 82
III.2.3.3. A francia adatvédelmi törvény második módosítása, az 1978. január 6-i 78-17. számú törvényhez 83
III.2.4 A bűnügyi irányelv átültetése a svéd nemzeti jogba 89

III.2.4.1. Előzmények 89
III.2.4.2. Az SFS 2018:218 számú törvény, az EU adatvédelmi rendelete szerinti kiegészítő rendelkezésekkel 90
III.2.4.3. A svéd bűnügyi adatokról szóló törvény SFS 2018:1177 95
III.3. Az egyes nemzeti szabályozások összehasonlító vizsgálata 98
III.3.1. Jogharmonizáció a nemzeti jogrendszer sajátosságai alapján 98
III.3.2. Az egyes nemzeti szabályozások összehasonlítása az Irányelv egyes szempontjai szerint 101
III.3.2.1. Az irányelv hatályának érvényesülése 102
III.3.2.2. A felügyeleti hatóságok 105
III.3.2.3. A jogalapok meghatározása 107
III.3.2.4. Az automatizált döntéshozatal 108
III.3.2.5. Az érintetti jogok 109
III.3.2.6. A naplózás 111
III.3.2.7. A közös kapcsolattartó pont 111
IV. A bűncselekményekhez kapcsolódó személyes adatok védelme 113
IV.1. Elméleti megfontolások a bűnügyi célú adatkezelések kapcsán 113
IV.2. A büntetőeljárás adatvédelmi vonatkozásai 114
IV.2.1. A gyanúsított személyes adatainak kezelése 119
IV.2.2. A tanú személyes adatainak kezelése 122
IV.2.3. A vádlott személyes adatainak kezelése 124
IV.2.4. A sértett személyes adatainak védelme 127
IV.3. A szakértő a büntetőeljárásban és a személyes adatok védelme 128
IV.4. Az adatkezelés jogalapja és az adatvédelem a büntetőeljárási törvényben 130
IV.5. A személyes adatok zártan történő kezelése 132
IV.6. A tárgyalás nyilvánosságának elve és a természetes személyek adatainak védelme 136
IV.7. A bírósági adatkezelési műveletek ellenőrzése 148
IV.8. A büntetés-végrehajtás adatvédelmi vonatkozásai 150
IV.8.1 Általános megfontolások 150
IV.8.2. Jogszabályi háttér 153
IV.8.3. Adatkezelési elvek a büntetés-végrehajtás során 155
IV.8.3.1.A Bv.tv. alapvető rendelkezései 155
IV.8.3.2. Bv.tv. - Az adatkezelésre vonatkozó rendelkezések 159
IV.8.4. A fogvatartott nyilvántartása 164
IV.8.5. Mesterséges intelligencia rendszerek a büntetés-végrehajtásban 169
V. Az adatvédelem és a kiberbűnözés kapcsolata 173

V.1. A kiberbűnözés fogalma 174
V.2. A kiberbűncselekmények jellegzetességei 177
V.2.1 Hacking és adathalász jellegű bűncselekménye 177
V.2.2. Online térben elkövetett zsarolás jellegű bűncselekmények 178
V.2.3. A személyiséglopás jelensége, mint a kiberbűncselekmények sajátos együtt állása 179
V.2.4 Jogszabályi háttér 183
V.3. Személyes adatok, mint a kiberbűncselekmények elkövetési tárgyai 186
V.3.1. A személyes adatok védelmének szerepe a kiberbűnözés elleni küzdelemben ... 187
V.3.2. Az (EU) 2022/2555 Irányelve (NIS 2) és az adatvédelem kapcsolódási pontjai . 190
VI. A személyes adatokkal kapcsolatos bűncselekmények, de lege lata 194
VI.1. Személyes adattal visszaélés 195
VI.1.1. Jogi tárgy 196
VI.1.2.Tényállási elemek és stádiumok 196
VI.1.3. Minősített esetek 200
VI.1.4. Rendbeliség 201
VI.2. Magántitok megsértése 204
2.1. Jogi tárgy és tényállási elemek 204
VI.2.3. Stádiumok és tettesség 206
VI.2.4. Bűncselekményi egység és a bűncselekmények találkozása 207
VI.3. Levéltitok megsértése 208
VI.3.1. Jogi tárgy és tényállási elemek 208
VI.3.3. Stádiumok és tettesség 209
VI.3.4. Minősített esetek 210
VI.3.5. Jogellenesség hiánya 211
VI.3.6. Bűncselekményi egység és a bűncselekmények találkozása 211
VI.4. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények 211
VI.4.1. Tiltott adatszerzés 212
VI.4.1.1. Jogi tárgy 213
VI.4.1.2. Elkövetési tárgy és magatartás 213
VI.4.1.3. Tettesség 214
VI.4.1.4 Minősített esetek 215
VI.4.2. Információs rendszer vagy adat megsértése 215
VI.4.2.1. A bűncselekmény jogi és elkövetési tárgya 216
VI.4.2.2. Elkövetési magatartások 216

VI.4.2.3 Minősített esetek és rendbeliség 220
VI.4.3. Információs rendszer védelmét biztosító technikai intézkedés kijátszása 220
VI.4.3.1. A bűncselekmény tárgya 221
VI.4.3.2 Elkövetési magatartás 221
VI.4.3.3.Rendbeliség 222
VI.4.4. Az információs rendszer felhasználásával elkövetett csalás 222
VI.4.4.1. Jogi tárgy és a tényállás szerkezete 223
VI.4.4.2 Elkövetési tárgy és a bűncselekményi alakzat elkövetési magatartásai 224
VI.4.4.4. Stádiumok 225
VI.4.4.5 Tettesség 225
VI.4.4.6 Minősített esetek 225
VI.4.4.7. Bűncselekményi egység és a bűncselekmények találkozása 225
VI.4.4.8. Elektronikus készpénz-helyettesítő fizetőeszközzel való visszaéléssel megvalósuló alakzat 226
VII. Összefoglalás - Eredmények 229
VII.1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése 230
VII.2 Első hipotézisemmel kapcsolatos eredmények áttekintése - A Bűnügyi Adatvédelmi Irányelv jogharmonizációja 230
VII.2.1. Az egyes tagállami átültések sajátosságai a magyar, a német, a francia és a svéd joggyakorlatban 231
VII.2.2 Az egyes nemzeti szabályozások összehasonlítása az Irányelv alapján 232
VII.3 Második hipotézisemmel kapcsolatos eredmények áttekintése - Bűncselekményekhez kapcsolódó személyes adatok védelme a büntetőeljárás és a büntetés-végrehajtás során . 237
VII.3.2. A bűncselekményekhez kapcsolódó személyes adatok védelme a büntetés-végrehajtás során 241
VII.3.2.1 Adatkezelés a 2013. évi CCXL. törvény (Bvtv.) alapján 241
VII.3.2.2 A fogvatartottak személyes adatainak védelme a 1995. évi CVII. (Bvsztvv.) törvény alapján 242
VII.3.2.3. Mesterséges intelligencia alapú rendszerek a büntésvégrehajtásban 243
VII.4. Harmadik hipotézisemmel kapcsolatos eredmények áttekintése - Az adatvédelem és a kiberbűnözés kapcsolata 244
VII.5. Negyedik hipotézisemmel kapcsolatos eredmények áttekintése - A személyes adatokkal kapcsolatos és az információs rendszerrel kapcsolatos bűncselekmények 247
VII.5.1. Személyes adatokkal kapcsolatos tényállások 247
VII.5.2.Tiltott adatszerzés és az információs rendszer elleni bűncselekmények 249
VIII. Summary 253
IX. Irodalomjegyzék 263

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[1] 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 rendeletet[2] és a bűnüldözési célú adatkezelésre vonatkozó irányelvet.[3]

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.[4] 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[5,6].

---

[1] Gstrein, Oskar J., and Anne Beaulieu. "How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches." *Philosophy & Technology* 35, no. 1 (2022): 3. https://doi.org/10.1007/s13347-022-00497-4.

[2]Európai 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.

[3] Európai 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.*

[4] Eszteri, 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.

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

[6] Nagy Zoltán András, Mezei Kitti. „Az Európai Unió Bűnügyi Adatvédelmi Irányelvéről" 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.[7]

Ahogy a rendeletet, úgy az irányelvet is megelőzték a technikai-ipari forradalom jelentős változásai. [8]Az Unió Biztonsági stratégiája [9] hangsúlyozza, hogy az olyan új technológiák, mint a mesterséges intelligencia, hatékony eszközként használhatók a bűnözés elleni küzdelemben.[10,11] 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.[12,13] 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.[14,15,16] Ebben a kölcsönhatásban értelmezhető az

[7](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.

[8]Szőke Gergely László. *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén.* Budapest: HVG–ORAC Lap– és Könyvkiadó Kft., 2014,

[9] 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,

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

[11] 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.

[12] Schwab, Klaus. *The Fourth Industrial Revolution*. World Economic Forum, 2016.

[13] Ambrus, István. *Digitalizáció és büntetőjog*. Budapest: Wolters Kluwer, 2021, p.290.

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

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

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

adatvédelem is.[17] Szükségessé válhat a jelenlegi szabályozási gyakorlat felülvizsgálata, további pontosítása a büntetőjogi szankciókat, a nyomozást, vádeljárást, a büntetés-végrehajtást és az adattovábbításokat érintő területeken is.

I.1. A témaválasztás indoklása, aktualitása

Témaválasztásom indoka, hogy a bűnügyi személyes adatok védelmének szabályozása, jogharmonizációja és gyakorlata az Európai Unió tagállamaiban eltérő lehet,- ahogy az a hatályos hazai szabályozásban is tapasztalható. - ami kérdéseket vet fel az adatvédelmi normák egységes értelmezése, ennek következtében az adattovábbítás, a határokon átnyúló bűnügyi együttműködés[18,19] szempontjából. Az európai adatvédelmi jogharmonizáció esetében az egyes tagállamok gyakorlatának összevetése rávilágíthat arra, hogy mely területeken szükséges (vagy szükséges-e) további összehangolás vagy jogalkotási intézkedés, hogy a bűnüldözés és az adatvédelem közötti egység biztosított legyen az Unió területén.[20,21]
Az egyes tagállamok jogfejlődése- és jogrendszere meghatározó az uniós jog átültetése területén. Alapvető fontosságú kérdés, hogy az adatvédelmi reform hogyan járul hozzá a

[17] Matos, Sara. "Privacy and Data Protection in the Surveillance Society: The Case of the Prüm System." *Journal of Forensic and Legal Medicine* 66 (August 2019): 155–161. https://doi.org/10.1016/j.jflm.2019.07.001.

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

[19] 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

[20] 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

[21] 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

nemzetközi bűnözés elleni küzdelemhez az egyes tagállamok, köztük Magyarország jogi szabályozásának és gyakorlatának tükrében. [22,23]

Ezen belül fontosnak tartom az Európai Bizottság (továbbiakban Bizottság) által véleményezett és vizsgált gyakorlatot az irányelv nemzeti jogba történő átültetésével kapcsolatban, amely irányadó a büntetőjogi szabályozás területén.[24]

Globalizált világunkban a bűnözés, különösen a számítógépes bűnözés és más, a kibertérrel összefüggő bűncselekmények egyre inkább határokon átnyúló jellegűek.[25,26] 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.[27] 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.[28] Ez az együttműködés, és különösen az elektronikus bizonyítékok gyűjtése és cseréje gyakran személyes adatok átadásával járnak, ezért alapvető fontosságúak a megfelelő adatvédelmi biztosítékok.[29] Erre jó példa a Budapesti Egyezmény 2. Kiegészítő jegyzőkönyve,

---

[22] Kőhalmi, 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

[23] 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

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

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

[26] Ambrus, István. *Digitalizáció és büntetőjog*. Budapest, Magyarország: Wolters Kluwer Hungary, 2021.

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

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

[29]01/2021.számú ajánlás a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti megfelelőségi referenciáról https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_hu.

mely az elektronikus bizonyítékok határon túli továbbításának szabályozása mellett külön fejezetet szentel az adatvédelmi biztosítékoknak.[30,31]

Az ilyen biztosítékok hozzájárulnak a bűnüldöző hatóságok közötti bizalomépítéshez is, gyorsabb és hatékonyabb információcserét biztosítanak, és erősítik a jogbiztonságot a büntetőeljárásokban.[32] Ebben a tekintetben az irányelv fontos eszközkészletet biztosít a 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.[33,34,35]

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.[36,37]

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

[30] 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

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

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

[33](EU) 2016/680, Preambulum 25

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

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

[36] 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.

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

adatgyűjtés exponenciális növekedése új kihívásokat jelentenek a személyes adatok védelme területén.[38,39]

A személyes adatok védelme nem csak az egyének jogainak biztosítását szolgálja, hanem fontos eszköz a számítógépes bűncselekmények elleni küzdelemben is. A Fehér Könyv[40], és a Mesterséges Intelligencia törvénytervezet[41] példái annak, hogy az adatvédelmi kérdések egyre inkább integrálódnak a jogi szabályozásba a technológia fejlődésével párhuzamosan. Az adatvédelmi intézkedések közvetetten segíthetnek megakadályozni a kibertámadásokat.[42] Az adatvédelmi szabályok lehetővé teszik a hatóságok számára, hogy hatékonyabban és gyorsabban nyomozzanak az online bűncselekmények ügyében[43].

A megfelelő adatvédelmi intézkedések nem csak az egyének személyes adatainak védelmét szolgálják hagyományos környezetben, hanem hozzájárulnak a digitális környezetben való biztonság és stabilitás biztosításában.[44,45,46]

---

[38] 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.

[39] Kis Kelemen, Bence. "Személyes adatok védelme fegyveres konfliktusokban." *Jogtudományi Közlöny* 77, no. 10 (2022): 395–402.

[40] 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.)

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

[42] Black, Kyle D., Christina B. Alam, Steven M. Bucher, Ashley J. Giannetti, Lauren D. Godfrey, and Justin D. Wear. "RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY."*Tort Trial & Insurance Practice Law Journal* 54, no. 2 (2019): 403–34. https://www.jstor.org/stable/27010241.

[43] Caruana, Mireille M. (2017). "The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement." *International Review of Law, Computers & Technology* 33 (3): 249–70. doi:10.1080/13600869.2017.1370224.

[44]Csiszár, M. Csaba. (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.

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

[46] 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.

I.2. A kutatás célja, hipotézisek

A kutatás célja, hogy a bűnügyi adatvédelmi irányelvi szabályozás alapján a bűnügyi tudományok területén megvizsgálja a természetes személyek adatainak védelmét a tagállami szintű szabályozás szintjén, ezen kívül a magyar büntetőeljárás, büntetés-végrehajtás és büntetőjogi szabályozás területén, azaz a szektoriális jogszabályozás szintjén.

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 összehasonlító 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.
- 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 megfelelőség kellő szintjének biztosítása érdekében.

2. A személyes adatok védelme területén a szektoriális szabályozás – 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.

I.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.[47] Részletesen elemzem adatvédelmi megközelítésben a vonatkozó ágazati jogszabályokat. 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 részeknél logikai és kritikai elemzéssel kiegészítve.

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

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

A tagállami jogharmonizációs gyakorlatok összehasonlító vizsgálatánál, az adatvédelmi szabályozás területén a nagy hagyományokkal rendelkező tagállamok, mint Németország, Svédország, és Franciaország jogi szabályozását vizsgáltam meg. Az adatvédelem történeti fejlődését figyelembe véve, ezek az államok jelentős szerepet játszottak az adatvédelmi jog kialakulásában és további fejlődésében. Németország volt az első ország, amely adatvédelmi törvényt fogadott el tartományi szinten. 1970-ben a németországi Hessen tartományban vezették be az első adatvédelmi törvényt a világon. Svédország szintén úttörő szerepet töltött

be az adatvédelem területén, hiszen 1973-ban elsőként fogadta el a svéd parlament a svéd adatvédelmi törvényt (Datalagen), amely a nemzeti adatvédelmi jogszabályok sorában az első volt a világon. Franciaország 1978-ban fogadta el az "Informatique Libertès" törvényét, amely átfogóan szabályozta a személyes adatok védelmét és a magánélet tiszteletben tartását.
Az összehasonlító elemzés, és annak történeti megközelítése rávilágíthat arra is, hogy az az irányelv implementációja során hogyan befolyásolják a történeti előzmények a jelenlegi joggyakorlatot.

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 rendelete [48] (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)[49]
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.[50]

[48] (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.

[49] 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.

[50] (EU) 2016/679, 5-6. cikk.

Az egyes rendelkezésekre vonatkozó esetleges korlátozások mellett azonban a GDPR teljes mértékben kizár bizonyos egyéb szabályozást, mint a határellenőrzésre, menekültügyre, a 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.[51]

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.[52]

A bűnügyi irányelv alkalmazásai tekintetében a jogharmonizációs kötelezettség a tagállami jogba való törvényi beépítést írta elő.[53]

II.1. Az adatvédelem fogalmával kapcsolatos megfontolások[54]

Az adatok védelme jogi értelemben a természetes személyek, azaz az érintettek adatainak védelmét jelenti.[55]

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 fedi le ennek általános fogalmi keretét.

---

[51] (EU) 2016/679, 2. cikk (2) (d).

[52] 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

[53] (EU) 2016/680, 62. cikk (1).

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

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

Mint jogi kategória a XIX. század végén jelent meg, az angolszász common law jogrendszerből ered. Warren és Brandeis nevezetes tanulmányához kötődik,[56] és a későbbi jogi értelmezések alapjául szolgált. Warren és Brandeis a fogalmat a magánjogi jogviszonyokban vizsgálták, a 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.[57]

A XX. század során az amerikai és angolszász jogrendszerekben a fogalom és a kapcsolódó jogszabályi keretek számos fejlődésen és értelmezésen mentek keresztül.[58]

A gyakran idézett Charles Fried a privacy lényegét tekintve azt a *„rólunk szóló tudás feletti ellenőrzés gyakorlásának lehetőségével"* azonosítja *(control over knowledge about oneself)*[59].

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.[60]

Jóri szerint „*Az adatvédelem a magánszféra-védelem sajátos jogi szabályozásban megnyilvánuló módja*", és egyben célja is.[61] 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.[62]

---

[56]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.)

[57] Ibid. p.219.

[58] Kohl, Uta. "THE RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW AND TWO WESTERN CULTURES OF PRIVACY." *International and Comparative Law Quarterly*72, no. 3 (2023): 737–69. https://doi.org/10.1017/S0020589323000258.

[59] 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.

[60] 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..

[61] Jóri András. *Adatvédelmi kézikönyv.* Budapest: Osiris, 2005, p.26.

[62] Ibid. p.27.

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 fogalom megjelenése óta többször is jelentősen változott, illetőleg jelenleg is folyamatosan változásban van.”* [63]

A privacy magyar nyelvű értelmezései többnyire annak egy-egy aspektusát ragadják meg, Szabó Máté Dániel a magyar jogrendszer fogalmaival próbálta annak tartalmát visszaadni.[64] „*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*”[65] 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.”*[66] 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.[67] 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*

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

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

[65] Ibid.

[66] Az Alkotmánybíróság 15/1991. (IV. 13.) AB–határozata. Ibid. 51.

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

ismeretek feletti ellenőrzés lehetőségét biztosítják az egyén számára oly módon, hogy a személyes adatok gyűjtését, feldolgozását és felhasználását korlátozzák és ezáltal az egyént védik."[68]

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. Ez a meghatározás a Szőke és Székely féle elveken alapszik, definíciójuk egyszerűsített gyakorlati szempontú megközelítés.

II.2. Az adatvédelmi jog fejlődésének főbb állomásai[69]

Az adatvédelem történeti áttekintése alapján megállapítható, hogy az informatikai szektorban végbement technológiai fejlődés kiemelt szerepet játszott az adatvédelmi jogszabályok kialakításában és evolúciójában.A magyar jogirodalomban megjelent jelentős számú adatvédelmi történeti áttekintés alapján - kiemelve Sólyom[70], Majtényi[71], Jóri,[72] Szőke[73], Péterfalvi[74] kutatásait - az adatvédelmi szabályozás kezdetei az 1970-es évekre tehetők.[75]

Az elektronikus adatkezelés lehetősége hozta magával az első adatvédelmi törvényt Európában a németországi Hessen népesség nyilvántartó adatbázis terve kapcsán.[76] 1973 - és 1978 között

[68] Idézi: Szabó Máté Dániel „Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival." p.52.

[69] Gáti Balázs. "Az adatvédelmi jog fejlődésének főbb állomásai."

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

[71] Majtényi László. "Az információs jogok."

[72] Jóri András. *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.*

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

[74] 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)

[75] Gáti Balázs. "Az adatvédelmi jog fejlődésének főbb állomásai."p. 156.

[76] 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.

ehhez hasonló módon Svédországban, Németországban, Norvégiában, Ausztriában és Franciaországban fogadtak el adatvédelmi tárgyú jogszabályokat.[77]

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 lefektetése.[78] 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*."[79]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.[80] 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*."[81] 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

[77] Ibid.p.109

[78] Gazdasági Együttműködési és Fejlesztési Szervezet. "Áttekintés az OECD Irányelvekről a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról." (hozzáférés 2021. szeptember 10.) https://www.oecd.org/sti/ieconomy/15590228.pdf.

[79] Ibid.p.4

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

[81] Ibid. 1. cikk.

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 személyes adatok feldolgozása során*”.[82] 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.[83]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/EK [84] az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, európai tanácsi és parlamenti rendelet az uniós intézmények és szervek által kezelt személyes adatok védelmét szabályozza. 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.[85]

---

[82] 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.

[83] 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.

[84] 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.

[85] Gáti Balázs. "Az adatvédelmi jog fejlődésének főbb állomásai.", p.158.

Az adatvédelem jogi szabályozása a Big Data korszakában újabb kihívások elé érkezett.[86] [87]
A mesterséges intelligencia, a robotika és az úgynevezett negyedik ipari forradalom által előidézett változásokra a jogalkotásnak is meg kellett felelni. Szükségessé vált egy adatvédelmi reform, teret engedve az innovációnak, egyúttal biztosítani a személyes adatok védelmét.
McDermott[88] és Brayne felhívják a figyelmet,[89] hogy milyen kihívásokat jelent e jog megvalósítása a mindenütt jelenlévő adatfigyelés korszakában, úgy, mint a polgárok kommunikációjának vagy cselekedeteinek szisztematikus nyomon követése az információs technológia és a Big Data, korszakában.

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

II.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.[90] Két évvel később került elfogadásra az 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*.” [91].

[86] 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.

[87] Zhu, FangBing, és Zongyu Song. "Systematic Regulation of Personal Information Rights in the Era of Big Data." *SAGE Open* 12, no. 1 (2022): 1–12. https://doi.org/10.1177/21582440211067529.

[88] McDermott, Yvonne. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*,*4* (1). https://doi.org/10.1177/2053951716686994

[89] Brayne, Sarah. "The Criminal Law and Law Enforcement Implications of Big Data." *Annual Review of Law and Social Science* 14 (2018): 293–308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839.

[90] Emberi jogok egyetemes nyilatkozata, 12. cikk

[91] Emberi Jogok Európai Egyezménye, 8. cikk

Az Unió szervei erre reagáltak az Alapjogi Charta kihirdetésével, [92] ami kötelező erőt csak a Lisszaboni Szerződés 2009. december 1 - i hatályba lépésével nyert.[93] A Charta 7. és 8. cikkében a magánélet tiszteletben tartása és a személyes adatok védelme egymással szorosan összefüggő, de különálló alapvető jogként nyert elismerést.[94]

A Lisszaboni Szerződéssel módosított Európai Unió Működéséről szóló Szerződés (továbbiakban EUMSZ) 16. cikk (2) bekezdése 2008-ban új, önálló jogalapot teremtett az adatvédelmi szabályok elfogadására, az EUMSZ 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 vonatkozó szabályokat.[95] 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 EUMSZ 68. cikke értelmében. A fő célkitűzések között kiemelendő az Unión belüli személyes adatok hatékonyabb védelmének biztosítása.[96]

A személyes adatok védelméhez való alapvető jogot garantáló uniós keret két fő jogszabálya 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 érintettje az Unióban tartózkodik. A rendelet az alapfogalmakat és alapelveket nagyrészt az előző 95/46 EK irányelvre alapozta,

[92] Az Európai Unió Alapjogi Chartája, 2012/C 326/02.

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

[94] 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

[95] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata, 2008/C 115/01. *Hivatalos Lap* C 115, 09.05. 2008, pp. 01-361

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

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.[97]

Az EUDPR kiterjesztette a szabályozást a bűnügyi adatok uniós szervek és hivatalok bűnügyi adatokkal kapcsolatos tevékenységére, az EUMSZ harmadik része V. címe 4. vagy 5. fejezetének hatálya alá tartozó tevékenységek végzése során,[98] függetlenül attól, hogy „*e tevékenységeket fő vagy kiegészítő feladataik körében végzik-e bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása érdekében*."[99] 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.[100,101].

Az e-Privacy javaslat célja az elektronikus hírközlési szektor adatkezelési tevékenységének a GDPR kompatibilis újraszabályozása rendeleti formában.[102]A tervezet szerint az e-Privacy rendelet kiterjedne az ún. OTT - over the top services -, szolgáltatásokra, mint a Skype,

---

[97] 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 előírások. [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 bűnügyi irányelv 36. cikk (3) és (5) bekezdés, 50. cikk (8) bekezdés]"

[98] Az EUMSZ harmadik rész V. cím. 4. (Igazságügyi együttműködés büntetőügyekben) és 5. (Rendőrségi együttműködés) fejezetei.

[99] (EU) 2018/1725 Rendelet, 12. bekezdés szerint „(...) azonban az Europolra és az Európai Ügyészségre addig nem alkalmazandó, amíg nem kerül sor az Europolt 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."

[100](EU) 2018/1725, (12)

[101] Gáti Balázs: "Az adatvédelmi jog fejlődésének főbb állomásai." p.164.

[102] COM (2017) 10 final.

Facebook Messenger, Gmail, iMessage vagy a Whatsapp és a dolgok internetére is - Internet of Things.

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

[103] 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

II.3.2. Az Európai Adatvédelmi Biztos, 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)[104] 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.

II.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 megfelelőséget 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.[105] A GDPR rendelkezett az Európai Adatvédelmi Testület létrehozásáról, egyúttal rendelkezett a Testület feladatairól, az elnökről és az elnökhelyettesekről, valamint a titkárságról.[106]
A bűnügyi adatvédelmi irányelv további feladatokat határozott meg a Testület, az elnök és az elnökhelyettesek, valamint a titkárság számára.[107]
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.

---

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

[105] 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. (hozzáférés 2022.10.08)

[106] „(EU) 2016/679)" 68. cikk (1)-(2).

[107] „(EU) 2016/680", 51. cikk.

- Az irányelv alkalmazásával kapcsolatos kérdések elemzése és az egységes alkalmazás elősegítése céljából iránymutatások, ajánlások és legjobb gyakorlatok kidolgozása. [108]
- 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.

Az EUDPR is meghatároz szabályokat a Testület számára.[109] Az uniós jog egyéb rendelkezései is további feladatokat róhatnak a Testületre. Az általános adatvédelmi rendeletet belefoglalták az Európai Gazdasági Térség (továbbiakban EGT) - megállapodásba, amely előírja, hogy az EGT tag EFTA-államok[110] 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 kifejteni álláspontjukat minden megvitatott kérdésben vagy szavazásra terjesztett témában.[111]
Az Európai Bizottság nem tagja a Testületnek, de annak ülésein, tevékenységeiben és értekezletein részt vehet, szavazati joggal nem rendelkezik.[112]
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

[108] „(EU) 2016/679)" 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"

[109] „(EU) 2018/1725 „42.cikk, 52- 57. cikk

[110] 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.

[111] EUDPR. 3. cikk

[112] 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.

vagy az általános adatvédelmi rendelet szerinti közös képviselőből és az európai adatvédelmi biztosból vagy ezek megfelelő képviselőiből áll.[113]

Az EDPB adatvédelmi reformmal kapcsolatos legfontosabb iránymutatásai a következők: iránymutatás az adathordozhatósághoz való jogról[114], iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához[115], iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról[116], 5/2019 iránymutatás az elfeledtetéshez való jog kritériumairól az általános adatvédelmi rendelet hatálya alá eső, keresőmotorokkal kapcsolatos ügyekben[117], 10/2020 sz. iránymutatás az általános adatvédelmi rendelet 23. cikke szerinti korlátozásokról,[118] 01/2022. sz. iránymutatás az érintettek jogairól – hozzáférési jog.[119]

Az EDPB 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.[120] 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 mechanizmusok révén segítsék az érintetteket jogaik harmadik országban történő gyakorlásában.[121]

---

[113] GDPR. 68. cikkének (4), és 4. cikk (1).

[114] 16/HU WP 242 rev.01, https://www.adatvedelmirendelet.hu/wp-content/uploads/wp242rev01_hu.pdf (hozzáférés 2022.10.08)

[115] 17/HU WP251rev.01, https://www.naih.hu/files/wp251rev01 hu.pdf (hozzáférés 2022.10.08)

[116] 17/HU WP260 rev.01, https://www.naih.hu/files/wp260rev01 hu.pdf (hozzáférés 2022.10.08)

[117] EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_hu (hozzáférés 2022.10.08.)

[118]EDPB, https://www.edpb.europa.eu/system/files/202307/edpb_guidelines_202010_art23_adopted_afterpublicconsultation_hu.pdf (hozzáférés 2022.10.09)

[119]EDPB, https://www.edpb.europa.eu/system/files/202404/edpb_guidelines_202201_data_subject_rights_access_v2_hu.pdf (hozzáférés 2022.10.09)

[120]EDPB, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_hu (hozzáférés 2022.10.09)

[121] 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

II.3.2.2. Európai Adatvédelmi Biztos (EDPS)

Az EDPS az Európai Unió intézményeinek és szerveinek független adatvédelmi tisztviselője. Az (EU) 2018/1725 rendelet VI. fejezete rendelkezik az európai adatvédelmi biztosról.[122] 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.[123] Feladatköre széleskörű, ideértve a panaszok felülvizsgálatát és bírósági jogorvoslatokat,[124] a jogalkotási konzultációt, technológia monitoringot, kutatási projekteket, és a bírósági eljárásokba való beavatkozás lehetőségét az Unió Bírósága elé terjesztett ügyekben.[125] Feladata továbbá az együttműködés a nemzeti felügyeleti hatóságokkal és a nemzetközi együttműködés.[126]

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 tanácskozásra, 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 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.[127]

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

[122] (EU) 2018/1725, 52.- 60 cikk, és 61.- 69.cikk

[123]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

[124] Ibid. 18. cikk

[125] Ibid. III.cím

[126] Ibid. IV.cím

[127] Ibid. 20. cikk.(1),(2),(3),(4)

meg, ezen kívül Europol-rendelet [128], az EPPO rendelet[129] és az Eurojust-rendelet[130] is adatvédelmi hatásköröket ruháztak az Európai Adatvédelmi Biztosra.

Az EDPS és az EDPB jogkörei bár széles körűek, felmerül a kérdés, hogy ezek valóban elegendőek-e az egyre komplexebb adatvédelmi kihívások kezelésére. Noha az intézmények függetlenek és hatáskörükbe tartozik az uniós szervek adatkezelésének ellenőrzése, tényleges befolyásuk mértéke attól is függ, hogy az uniós intézmények milyen mértékben veszik figyelembe ajánlásaikat, valamint milyen gyakran és milyen hatékonysággal élnek szankciós jogköreikkel.

Kiemelendő ezen intézmények és a tagállami hatóságok együttműködésének jelentősége, bár az EDPS valamint az EDPB is elsődlegesen az EU intézményeire fókuszál, az uniós adatvédelmi jog egységes alkalmazása érdekében elengedhetetlen a nemzeti felügyeleti szervekkel való kooperáció. Ennek hatékonysága függ, a hatáskörök megosztásától és elsősorban az együttműködési mechanizmusoktól.

II.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 biztosításához[131] Az EDPB általános adatvédelmi rendeletről szóló több iránymutatása a bűnüldözési célú adatvédelemről szóló irányelv szempontjából is releváns. Ezek közé tartozik az adatkezelő és az adatfeldolgozó fogalmáról[132] az érintettek jogairól, [133] az adatvédelmi

[128] Az Európai Parlament és a Tanács (EU) 2016/794 rendelete a Bűnüldözési Együttműködés Európai Uniós 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.

[129] 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.

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

[131] (EU) 2016/680, Preambulum (7)

[132] 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/202107/eppb_guidelines_202007_controllerprocessor_final_en.pdf. (hozzáférés,2022.10.10.)

[133] 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. (hozzáférés,2022.10.10.)

incidensről értesítésről,[134] az adatvédelmi hatásvizsgálatról,[135] beépített és az alapértelmezett adatvédelemről[136] és az egyedi automatizált döntéshozatalról szóló iránymutatások.[137]

Az EDPB iránymutatásokat fogalmazott meg a bűnügyi adatvédelmi irányelvvel kapcsolatosan is. Ezek közül az irányelv V. fejezetével kapcsolatos - nemzetközi adattovábbítások - szempontjából specifikus iránymutatás[138], és az arcfelismerő technológiák használatára vonatkozó iránymutatás[139] főbb szempontjait 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. 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 harmadik ország által e célból igénybe vett eszközök eltérhetnek az Európai Unióban alkalmazottaktól. A megfelelőségi normának nem kell pontról pontra tükröznie az uniós

---

[134] Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01), https://ec.europa.eu/newsroom/article29/items/612052, (hozzáférés,2022.10.10.)
01/2021. számú iránymutatás Az adatvédelmi incidensek bejelentésével kapcsolatospéldákról, https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_hu.pdf, (hozzáférés,2022.10.10.)

[135] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), https://ec.europa.eu/newsroom/article29/items/611236/en, (hozzáférés,2022.10.10.)

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

[137] 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

[138]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, (hozzáférés,2022.10.10.)

[139] 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_frtlawenforcement_en_1. pdf, (hozzáférés,2022.10.10.)

jogszabályokat, hanem az említett jogszabályok alapvető követelményeit kell megállapítaniuk.[140] A Bizottságnak a megfelelőségi 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. [141,142].

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.

- Az arcfelismerő technológia használatának iránymutatása a bűnüldözés területén a kritikus jogi kereteket és a technológia alapvető jellemzőit hivatott tisztázni. (FRT)[143]

[140] 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 hatékonynak kell lenniük ahhoz, hogy az Unióban biztosított védelemmel lényegében egyenértékű védelmet biztosítsanak”.

[141] Schrems I. ügy, 52. pont

[142] (EU) 2016/680, 47. cikk (5) és Preambulum (82)

[143] Gáti, Balázs. (2022)"A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései." In *FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI:*

(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. Az olyan technológiák alkalmazása, amelyek lehetővé teszik az egyének azonosítását vagy hitelesítését viselkedésük alapján különböző médiumokon keresztül, mint például zárt láncú televíziós rendszerek (CCTV) [144] 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 (artificial intelligence - AI) vagy gépi tanulás (machine learning - ML[145]) 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-egyhez [146] helyzetekben, de alkalmas nagy tömegek és fontos közlekedési csomópontok megfigyelésére is, így szükségszerűen jogi és etikai szempontok szigorú mérlegelését igényli.

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.

[144] A CCTV (Closed-Circuit Television) egy zárt televíziós rendszer, amelyet elsősorban megfigyelési és biztonsági célokra használnak. A rendszer kamerákból, monitorokból és rögzítő eszközökből áll, amelyek lehetővé teszik a vizuális felvételek élő közvetítését vagy későbbi visszanézését.

[145] 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.

[146] 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.

A személyes adatok bűnüldözési kontextusban történő védelme érdekében meg kell felelnie a LED követelményeinek, [147] de alkalmazása azonban számos más alapvető jogot is érinthet, úgymint a Charta 8. cikkében foglalt személyes adatok védelméhez való jogot, és a Charta 7. cikkében foglalt magánélethez való jogot. [148] 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.[149] 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 videófelvételt 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

[147] 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..

[148] 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,(hozzáférés,2022.10.10.)

[149] 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 hozottnak 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.[150] 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

[150] Ha biometrikus adatokat tárolnak, és azokat összekapcsolják az alfanumerikus adatokkal, a hozzáférési kérelmeket az alfanumerikus adatok alapján kell ellenőrizni, hogy ne kezdeményezzenek további biometrikus adatfeldolgozást. 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) preambulumbekezdése 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.[151] Véleményem szerint az arcfelismerő technológia bűnüldözési alkalmazása rendkívül érzékeny terület, amely egyensúlyt kíván a biztonsági érdekek és az alapvető jogok – védelme között. Noha hatékony eszköz lehet a bűncselekmények felderítésében, alkalmazása csak szigorú jogi és etikai garanciák mellett indokolt, mivel a visszaélések és az alapjogokat sértő tömeges megfigyelés kockázata nem elhanyagolható.

II.3.2.4. Az Európai Unió Bírósága (EUB)

Az EUB 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), [152] Digital Rights Ireland (C-293/12),[153] Weltimmo (C-230/14) ügy.[154]

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

[151] EDPB 05/2022, Annex I.II.III.

[152] 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.

[153] 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.

[154] 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 Deutschland [155] és a B kontra Latvijas Republikas Saeima[156] ügyek. A döntéshozatali eljárásokról az irányelv jogértelmezéseivel kapcsolatos ügyekben a következő fejezetben lesz szó.

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

III.1. A bűnügyi adatvédelmi irányelv bemutatása[157]

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 szabályaik voltak irányadók. Példaként említhető, hogy a korábban létrejött Schengeni Információs Rendszer (SIS) működését és a schengeni vívmányokhoz kapcsolódó egyéb eszközöket szabályozó jogszabályok már tartalmaztak olyan specifikus rendelkezéseket, amelyek az érintett személyek jogait, adatvédelmi szempontból is 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

[155] 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.

[156] 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.

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

továbbítására vonatkozó szabályok egységesítésével elősegíteni a tagállamok közötti együttműködést, valamint a közbiztonság magas szintjét is kívánja biztosítani.[158]

A magyar jogirodalomban is fellelhetők az irányelv értelmezései és bemutatásai.[159,160,161]

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

Az Irányelv preambulumból és tíz fejezetből épül fel. A preambulum hivatkozik az Alapjogi Charta 8. cikk (1) bekezdése és az EUMSZ. 16. cikkének (1) bekezdésére, amelyek rögzítik, hogy „*mindenkinek joga van a rá vonatkozó személyes adatok védelméhez*"[162,163], megállapítja, hogy e jogok állampolgárságtól és lakhelytől függetlenek[164,165], 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.[166]

Az irányelv tárgyi hatálya bűnüldözési célból végzett adatkezelésekre terjed ki.[167] 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) bekezdésében[168]

---

[158] De Hert, Paul, and Vagelis Papakonstantinou. "The New Police and Criminal Justice Data Protection Directive: A First Analysis." *New Journal of European Criminal Law* 7, no. 1 (2016): 7–19

[159] 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.

[160] 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.

[161] 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.

[162](EU) 2016/680 Preambulum (1)

[163] 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.

[164](EU) 2016/680 Preambulum (2).

[165](EU) 2016/680 Preambulum (17).

[166](EU) 2016/680 Preambulum (12).

[167] (EU) 2016/680 Preambulum (11).

[168] „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"

meghatározott célok valamelyikét szolgálja, és azt a 3. cikk (7) bekezdésében[169] meghatározott illetékes hatóságok végzik. Ha e feltételek egyike sem teljesül, akkor a GDPR alkalmazandó.

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 EUMSZ V. címe 2. fejezetének - a közös kül- és biztonságpolitikára vonatkozó különös rendelkezések - hatálya alá tartozó tevékenységek során végzett személyes adatkezelésekre.[170]

A nemzetbiztonság fogalmának értelmezésével az EUB is foglalkozott az irányelv kapcsán, mely szerint az hagyományosan az állami szuverenitáshoz kapcsolódik, azaz az állam alapvető funkcióihoz és a társadalom alapvető érdekeihez.[171]

A bűncselekmény fogalmának meghatározása[172] az irányelv szerint értelmezendő, „*az Európai Unió Bírósága (...) általi értelmezésnek megfelelő, önálló uniós jogi fogalomnak minősül*".[173,174]

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

---

[169] „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 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.

[170] (EU) 2016/680, Preambulum (14)

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

[172] (EU) 2016/680, Preambulum (13).

[173] 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.

[174] A bűncselekmény fogalmának az EUB és az EJEB vonatkozó esetjogának elemzése kapcsán a fogalom lefedi 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"

b) pontja szerint továbbá illetékes hatóság lehet bármely más szerv vagy szervezet, amelyet a tagállam joga megbízott azzal, hogy ugyanezen bűnüldözési célokból közfeladatot lásson el és közhatalmat gyakoroljon.[175]

Az irányelvtől eltérő cél tekintetében a GDPR-t kell alkalmazni. Ilyen tevékenység például a hatósági jogkör gyakorlása, valamint ha a bűncselekmények nyomozása, felderítése és a védeljárás 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.[176]

A személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelésére a 45/2001/EK európai parlamenti és tanácsi rendelet alkalmazandó[177], amely rendeletet az (EU) 2018/1725 rendelete – EUDPR - váltotta fel.

Az irányelv a preambulumban utal a személyes adatok kezelésének alapelveire, kiemeli a jogszerű, tisztességes és átlátható adatkezelés elvét. A tisztességes adatkezelés elvét elkülöníti a Charta 47. cikke, és az EJEE 6. cikkében meghatározott tisztességes eljárás fogalmától.[178]

A tájékoztatáshoz való jogot, valamint az ehhez kapcsolódó korlátokat, a jogszerű, átlátható,[179] és tisztességes adatkezelés, a megfelelő szintű biztonság és bizalmas kezelés elvét, a célhoz kötöttség, szükségesség és arányosság elvét, a pontosság elveit fogalmazza meg.[180]

A GDPR és LED elvek bizonyos értelemben különböznek egymástól, példa erre az 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

---

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

[176] (EU) 2016/680, Preambulum (11) és 3. cikk. (2).

[177] 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.

[178] (EU) 2016/680, Preambulum (26)

[179] 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.

[180] (EU) 2016/680, Preambulum (26) – (30).

érdekek védelme érdekében az átláthatóság különböző szintjeit követeli meg, például a nyomozati eljárás során. [181]

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 elvének megfogalmazása is a bűnüldözés sajátos igényeinek figyelembevételére és a személyes adatok védelme mellett a tisztességes eljárás tiszteletben tartásának biztosítására is törekszik.[182]

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.[183]

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.[184] 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.[185]

---

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

[182] 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.

[183](EU) 2016/680, Preambulum (31).

[184] (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

[185] (EU) 2016/679 6. cikk.(1) e)

Az irányelv kötelezi a tagállamokat a közérthető tájékoztatás jogának biztosításhoz[186], valamint az érintett hozzáférési jogának biztosításához[187], illetve a helyesbítéshez, törléshez való érintetti jogokat stb.[188]. Ugyanakkor 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 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.*" [189].

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*."[190] Az érintetti jogok gyakorlását lehetővé kell tenni a felügyeleti hatósághoz történő panasztétel jogával és a hatóság elérhetőségével.[191]

Kiemelendő, hogy az érintettek jogai önmagukban nem akadályozzák a bűnüldöző szerveket abban, hogy olyan tevékenységeket folytassanak, mint a titkos nyomozás vagy a videó megfigyelés[192].

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 biztosítékokat 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.[193]

---

[186] (EU) 2016/680, Preambulum (38), (39).

[187] (EU) 2016/680, Preambulum (43), (44), és 13. cikk.

[188] (EU) 2016/680, 13. cikk. (e).

[189] (EU) 2016/680, Preambulum (20).

[190] (EU) 2016/680, Preambulum (42).

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

[192] (EU) 2016/680, Preambulum (26).

[193] EU) 2016/680, Preambulum (38)

A preambulum szabályozza továbbá a megfelelőség, a felügyeleti hatóságok,[194] és a harmadik országba történő továbbításra vonatkozó rendelkezéseket.[195]

A szabályozás a kötelező kölcsönös segítségnyújtás szabályait is rögzíti, és általános együttműködési kötelezettséget ír elő[196]. Kimondja továbbá, hogy az EDPB hatásköre kiterjed az ezen irányelv hatálya alá tartozó adatkezelési tevékenységekre[197]. Az irányelv ezen kívül kártérítési jogot biztosít az érintettek részére abban az esetben, ha jogsértés, vagy jogellenes adatkezelés következtében kár érte őket[198].

A harmadik országba történő továbbítással kapcsolatban megállapítja, hogy az adatok harmadik országba csak akkor továbbíthatók, ha az bűnüldözési célból szükséges, és a Bizottság megfelelőségi határozatot fogadott el az érintett harmadik országban nyújtott védelemi szintjéről[199]. Megfelelőségi határozat hiányában az adattovábbítás csak megfelelő biztosítékok alapján lehetséges,[200] azonban különleges körülmények fennállása esetén is előírja az adatok továbbítását[201].

Az I. fejezet – az általános rendelkezések - a tárgyat és célokat, a hatályt, és a fogalommeghatározásokat tartalmazza.[202] 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*"[203]

Az irányelv 3. cikke a „Fogalommeghatározások" tizenhat fogalmat határoz meg, köztük a profilalkotás, az illetékes hatóság, az adatkezelő, adatfeldolgozó és a címzett fogalmát.[204]

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

---

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

[195] (EU) 2016/680, Preambulum (67)- (75)

[196] (EU) 2016/680, Preambulum (77), 40. cikk (b).

[197] (EU) 2016/680, Preambulum (84) 51.cikk.

[198] (EU) 2016/680, Preambulum (88) 56. cikk.

[199] (EU) 2016/680, Preambulum (64), 36. cikk (1).

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

[201] (EU) 2016/680, 38. cikk.

[202] (EU) 2016/680, 1 cikk– (2) a), b).

[203] (EU) 2016/680, 1 cikk– (2) a), b).

[204] (EU) 2016/680, 7.–10. pont.

különbségtételt, az adatkezelés jogszerűségét, a különös adatkezelési feltételeket, valamint a személyes adatok különleges kategóriáinak kezelését és az egyedi ügyekben történő automatizált döntéshozatalt szabályozza.[205]

Az alapelveket a preambulum kapcsán már érintettem, itt most a személyes adatok különleges kategóriáinak[206] kezelését 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”*[207]

A tárolásra és a felülvizsgálatra vonatkozó határidőkkel kapcsolatban az irányelv előírja, hogy azok betartását eljárásjogi intézkedésekkel kell biztosítani.[208]

Az érintettek különböző kategóriái közötti különbségtételről a preambulumban már szintén volt szó.[209] 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. [210]

Az EJEB és az EUB ítélkezési gyakorlatára, valamint a LED (26) preambulumbekezdésére való hivatkozással az adatminimalizálás elvének való megfelelés többek között azt követeli meg,

---

[205] (EU) 2016/680, 4.– 11. cikk.

[206] „(…) 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”

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

[208] (EU) 2016/680, 5. cikk.

[209] (EU) 2016/680, 6. cikk.

[210] 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.”

hogy az adatokat ne tárolják tovább, mint amennyi idő az elérni kívánt célhoz szükséges, és csak akkor, ha az adatkezelés célja észszerűen nem teljesíthető más eszközökkel. [211]

A LED újdonsága a tárolási határidőkre és a tárolás szükségességének időszakos felülvizsgálatára vonatkozó külön rendelkezés,[212] amely megerősíti a tárolás korlátozásának elvét.[213]

A LED átültetés értelmezése kapcsán a jogirodalomban az érintettek kategorizálásra vonatkozó LED-rendelkezések statikussága a besorolást illetően aggályokat is felvetett. Ugyanis döntéseket kell hozni a bűncselekmény szereplőinek osztályozására vonatkozóan már a büntetőeljárás korai szakaszában, miközben ezek a döntések sokszor még „tévesek".[214] A bűnügyi nyomozásokat ugyanis a változékonyság jellemzi, 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.[215] 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.[216]

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

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

[212] (EU) 2016/680, 5. cikk,

[213] (EU) 2016/680, 4. cikk (1)

[214] Leiser, Mark.and Custers, Bart." The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680" p.369

[215] Winter, Heinrich B. et al, (2020) „De verwerking van politiegegevens in vijf Europese landen, Rijksuniversiteit Groningen - Pro facto" , WODC rapport 3031

[216] 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.[217]

A LED tartalmaz egy "különleges adatkezelési feltételek" elnevezésű rendelkezést, amely tovább pontosítja a célhoz kötöttség elvét, abban az esetben, amikor a bűnüldözési célokból kezelt személyes adatok nem bűnüldözési célokra kerülnek felhasználásra, 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.[218] Ez a záradék különösen fontossá vált a bűnüldözési eszközökkel kapcsolatos tudományos kutatás során, amely gyakran valós adatok felhasználását teszi szükségessé.[219]

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.[220]

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*

[217] Bäcker, Matthias. és Hornung Gerrit, (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.

[218] (EU) 2016/680, 9. cikk

[219] Bolognini, Luca., 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, (hozzáférés,2022.10.10.)

[220] 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".[221] Az érintett jogosult tájékoztatást, és magyarázatot kapni 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 bűnügyi nyomozások és büntetőeljárások során megillető jogokat[222].

Az automatizált döntéshozatali információkra vonatkozó tilalom az egyéni döntéshozatalra összpontosít, a kollektív vagy csoportos profilalkotást figyelmen kívül hagyva. Ez a szabályozás bizonyos esetekben akadályt jelenthet, 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.[223] Kérdéseket vet fel az, hogy hogy mi minősül automatizált döntésnek, milyen mértékű és jellegű emberi beavatkozásra van szükség.[224,225]

A hozzáférési jog korlátozása szükséges és arányos intézkedés kell, hogy legyen 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*".[226]

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

[221] (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.

[222] (EU) 2016/680, 12.– 18. cikk.

[223] 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.

[224] 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.

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

[226] (EU) 2016/680, 15. cikk (1) a) – e)

szabályozó 17. cikk biztonsági hálót jelent mind az illetékes hatóságok, mind az érintettek számára.[227] Az illetékes hatóságok dönthetnek úgy, hogy a folyamatban lévő vizsgálatok[228] védelme érdekében nem teszik lehetővé az érintettek számára az adatkezelés ellenőrzését, míg az érintettek lehetőséget kaphatnak arra, hogy a felügyeleti hatóság legalább az adatkezelés jogszerűségét ellenőrizze.[229]

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 minősül.[230]. A WP29 megállapítása szerint, a LED nem teljesen 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.[231] Ugyanezt a felfogást fogadja el a szakirodalom, amely a felügyeleti hatóságok e hatáskörét az adatkezelés jogszerűségének egyfajta független felügyeleteként fogja fel, összhangban az EJEB ítélkezési gyakorlatával.[232,233].

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 bűnügyi nyomozás vagy büntetőeljárás során kezelt bírósági határozat, vagy jegyzőkönyv vagy ügyirat tartalmazza*”.[234]

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*".

---

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

[228] (EU) 2016/680 13. cikk (3), 15. cikk (3) és 16. cikk (4)

[229] (EU) 2016/680 17. cikk (3),

[230] "Vélemény a bűnüldözési irányelv (EU 2016/680) néhány kulcskérdéséről", WP258, 2017. november 29. pp.23-24.

[231] Ibid. pp. 23-24.

[232] 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.

[233] Sajfert, Juraj and Quintel, Teresa "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities." p.340

[234] (EU) 2016/680, 18. cikk.

A IV. fejezet - Adatkezelő és adatfeldolgozó, az általános kötelezettségek, a személyes adatok biztonsága, és az adatvédelmi tisztviselő szakaszokból épül fel[235]. 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.[236]

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.*”[237] Ilyen elvek például a WP 29 ajánlása szerint a szükségesség és arányosság elvei, ha a rendszer automatikusan korlátozza az adatokhoz való hozzáférést [238]

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 e helyett 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

[235] (EU) 2016/680, 19 – 34. cikk.

[236] (EU) 2016/680, Preambulum (61), (62).

[237](EU) 2016/680, 20. cikk.

[238] 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 (hozzáférés 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.[239]

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,[240] és mind az adatkezelőknek, mind a rendszerfejlesztőknek egyértelmű lehetőséget biztosít arra, hogy a jövőbeli adatfeldolgozási műveletek kidolgozásának és tervezésének korai szakaszában biztosítékokat építsenek be.

---

[239] Sajfert, Juraj.and Quintel, T. "Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities", p.342

[240] Naudts, Lauren."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, p.72 (hozzáférés 2022.07.02.)

Az V. fejezet - A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása - személyes adatok továbbításaira vonatkozó általános elveket, az 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 le[241].

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.[242] A Bizottság az Európai Unió Hivatalos Lapjában és annak weboldalán teszi közzé a megfelelőségi határozatról szóló jegyzéket.[243] 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) preambulumbekezdése tovább pontosítja, ez magában foglalja azokat a "*jogilag kötelező erejű kétoldalú megállapodásokat*" is, amelyek alapján a tagállamok közvetlen együttműködést folytatnak a külföldi bűnüldöző szervekkel.[244]

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,

[241] (EU) 2016/680, 35– 40. cikk.

[242] (EU) 2016/680, 36. cikk (1) a), b), c).

[243](EU) 2016/680, 36. cikk (8).

[244] COM (2020) 262 final.

annak szabályait, illetékességét, hatásköreit, tevékenységi jelentéseit.[245] Ezek a feladatok egyúttal a tagállomokra rótt kötelezettségek is a felügyeleti hatóságokkal kapcsolatban.[246].

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.[247] A 80. preambulumbekezdés 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 preambulumbekezdés megjegyzi, hogy ez olyan szervekre is vonatkozhat, mint az ügyészség.[248]

A VII. fejezetben – Együttműködés – a kölcsönös segítségnyújtás és az Európai Adatvédelmi 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.[249]

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

---

[245](EU) 2016/680, 41– 49. cikk.

[246] A megfelelőség adatvédelmi felügyeleti hatóságok általi felügyelete alapvető fontosságú, és a Charta 8. cikkének (3)bekezdésében is szerepel.

[247] Custers, Bart, Linda Louis, Maria Spinelli, és Kalliopi Terzidou. "Quis Custodiet Ipsos Custodes? Data Protection in the Judiciary in EU and EEA Member States." *International Data Privacy Law* 12, no. 2 (2022): 93–112. https://doi.org/10.1093/idpl/ipac002.

[248] 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”

[249] (EU) 2016/680, 51. cikk.

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.[250] Az érintettek képviseletét a tagállami rendelkezésnek megfelelően létrehozott nonprofit jellegű szerv, szervezet vagy egyesület láthatja el, mely az érintettek jogainak és szabadságainak a személyes adataik vonatkozásában biztosított védelme területén tevékenykedik.[251]
A záró rendelkezések fogalmazza meg a tagállami jogba való átültetés vonatkozó szabályait.[252] *„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”*

Öszefoglalva, a bűnüldözési célú adatkezelés jogi szabályozása az elmúlt évtizedekben egyre összetettebbé vált, különösen az Európai Unió szintjén, ahol az adatvédelem és a közbiztonsági szempontok közötti egyensúly megteremtése folyamatos kihívás elé állítja a jogalkotókat. Az (EU) 2016/680 irányelv e két szempont összehangolására tett kísérletet, célja, hogy egységes normarendszert biztosítson a bűnüldözési hatóságok számára, miközben az egyének alapvető jogai nem sérülnek indokolatlanul.
Az irányelv egyik központi sajátossága, hogy az adatkezelési elvek tekintetében szorosan követi a GDPR által lefektetett struktúrát, ugyanakkor a bűnüldözési célok miatt egyes területeken rugalmasabb, más esetekben pedig szigorúbb követelményeket támaszt. A célhoz kötöttség és az adatminimalizálás elve, amelyek a magánszféra védelmét hivatottak biztosítani, a bűnügyi nyomozások esetében sajátos értelmezést nyernek.[253] A LED előírja, hogy a személyes adatokat nem lehet határozatlan ideig tárolni, és azok megőrzése kizárólag addig indokolt, amíg az eredeti adatkezelési cél teljesül. Ez az elv elméletileg szilárd adatvédelmi garanciát jelent, ugyanakkor a gyakorlati megvalósítás során felmerül az a probléma, hogy a büntetőeljárások hossza és dinamikája gyakran nem teszi lehetővé a tárolási határidők egyértelmű meghatározását. Az irányelv ugyan előírja a tárolási szükségesség rendszeres

[250](EU) 2016/680, 52–54 cikk.

[251](EU) 2016/680, 55.cikk.

[252](EU) 2016/680, 63.cikk.

[253] Marquenie, Thomas. "The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework." *Computer Law & Security Review* 33, no. 3 (2017): 324–340. https://doi.org/10.1016/j.clsr.2017.03.007.

felülvizsgálatát, azonban kérdéses, hogy a tagállamok mennyire tudják ezt egységes módon végrehajtani, különösen olyan esetekben, ahol a bűnügyi nyomozások akár évekig is elhúzódhatnak.

Egy másik kritikus pont az érintettek kategorizálásának kérdése. A LED megkülönbözteti a tanúkat, gyanúsítottakat, terhelteket és sértetteket, azonban a büntetőeljárások sajátosságaiból adódóan ezek a kategóriák sok esetben nem maradnak változatlanok. Egy tanúból idővel gyanúsított lehet, egy sértettből pedig akár terhelt is, miközben az adatkezelés eredeti logikája nem feltétlenül követi ezt a változást. A merev kategorizálás ezért könnyen vezethet jogsérelmekhez, ha az adatkezelők nem biztosítják az adatállományok aktualizálását a büntetőeljárás előrehaladtával. Az ilyen típusú adatkezelési struktúrák statikussága nem felel meg a nyomozások dinamikus jellegének, előfordulhat, hogy az érintetti státuszokhoz kötött adatkezelési garanciák érvényesítése ennek következtében nem megfelelő.

Az automatizált döntéshozatal és a profilalkotás kérdése szintén az irányelv egyik legösszetettebb és legvitatottabb területe. A LED elviekben tiltja azokat az automatizált döntéshozatali mechanizmusokat, amelyek az érintettre hátrányos jogkövetkezménnyel járnak, ha azok kizárólag algoritmikus alapon születnek. Ez az elv az adatvédelem szempontjából kiemelten fontos, hiszen a mesterséges intelligencia és a gépi tanulás térnyerésével a bűnüldözési hatóságok egyre inkább a prediktív rendészeti modellekre támaszkodnak. Az irányelv azonban nem tér ki kifejezetten azokra a helyzetekre, amikor kollektív profilalkotás történik, például egy adott bűnözési gócpont azonosításakor. Ez a szabályozási hiányosság aggályokat vet fel, hiszen a prediktív algoritmusok általában csoportos alapon működnek, és nem egyéni szinten hoznak döntéseket, ami megnehezíti annak meghatározását, hogy mikor minősül egy döntés automatizáltnak, és milyen mértékű emberi beavatkozás szükséges ahhoz, hogy az valóban megfeleljen az alapjogok védelmének.

Az érintettek jogainak korlátozása szintén az egyik legvitatottabb terület. A LED ugyan lehetővé teszi a hozzáférési, helyesbítési és törlési jogok korlátozását bűnüldözési célok érdekében, azonban ezek a korlátozások csak akkor lehetnek jogszerűek, ha azok szükségesek és arányosak. A jogalkalmazási gyakorlatban azonban nem egyértelmű, hogy a tagállamok mennyire indokolják megfelelően ezen jogok korlátozását, és milyen biztosítékokat nyújtanak annak érdekében, hogy az érintettek jogai ne sérüljenek indokolatlanul. A bűnügyi nyilvántartásokhoz való hozzáférés, valamint azok módosításának és törlésének lehetősége különösen problematikus, hiszen a tagállami gyakorlatok jelentősen eltérhetnek abban, hogy milyen eljárásokat biztosítanak az érintettek számára az adataik helyesbítésére.

A harmadik országokba történő adattovábbítás szintén a LED egyik neuralgikus pontja. Az irányelv szigorú feltételeket támaszt az uniós polgárok adatainak Európai Unión kívüli továbbításával kapcsolatban, különösen akkor, ha azok olyan országokba kerülnek, amelyek nem rendelkeznek megfelelő adatvédelmi biztosítékokkal. Bizonyos kivételes esetekben azonban – például terrorizmus vagy más súlyos bűncselekmények megelőzése céljából – az irányelv lehetőséget ad arra, hogy az adattovábbítás még akkor is megtörténjen, ha a célország nem biztosít az uniós normáknak megfelelő adatvédelmet. Ez az elv elméletileg indokolt lehet a nemzetbiztonsági érdekek védelmében, ugyanakkor a gyakorlatban visszaélésekhez is vezethet, ha a tagállamok nem alkalmaznak megfelelő garanciákat az ilyen adattovábbítások ellenőrzésére.

A LED tehát számos fontos előrelépést jelent a bűnüldözési célú adatkezelés uniós szabályozásában, ugyanakkor végrehajtása jelentős kihívásokkal jár. Az egyes tagállamok közötti végrehajtási eltérések, az érintettek jogainak korlátozása, valamint az új technológiai fejlemények – különösen az automatizált döntéshozatal és a mesterséges intelligencia térnyerése – arra utalnak, hogy a jogalkotónak és a jogalkalmazóknak folyamatosan figyelemmel kell kísérniük az adatvédelmi garanciák tényleges érvényesülését. Az adatvédelem és a bűnüldözési érdekek közötti egyensúly megtalálása nem pusztán jogalkotási kérdés, hanem a jogalkalmazási gyakorlat finomhangolását is szükségessé teszi.

III.2. A bűnügyi irányelv jogharmonizációja

Az Európai Bizottság 2022. július 25-én tette közzé a (fentiekben tárgyalt) bűnüldözésben érvényesítendő adatvédelemről szóló irányelv alkalmazásáról és működéséről szóló jelentését.[254] Ezt követően értékelő tanulmány készült az Állampolgári Jogi, Bel- és Igazságügyi Bizottság (LIBE) megbízásából, amely a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásának kritikai értékelését tartalmazta[255]

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

[254] 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.

[255] 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

nemzeti jogszabályokba történő átültetés tényleges 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 2020-ban elfogadta „A korábbi harmadik pillérhez tartozó vívmányok adatvédelmi szabályokkal való összehangolásának további lépései" című közleményt.[256] 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,[257] az uniós intézmények, a nemzeti felügyeleti hatóságok és a civil társadalmi szervezetek különböző forrásai alapján készítették, és 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. [258]

A LIBE kérésére készült tanulmány megállapításai - mely részben a Bizottság jelentésén és más kapcsolódó anyagokon alapulnak, [259] foglalkozik a LED hatályával, az alapelvekkel, az érintteti jogokkal, az adatkezelői kötelezettségekkel, és a harmadik országokba való továbbításával a jogharmonizáció kapcsán. A tanulmányok ajánlásokat fogalmaztak meg a tagállamok

[256] 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.

[257] COM (2022) 364 final, Brüsszel, 2022.7.25.

[258] (EU) 2018/ 1725, 98. cikk (2)

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

részére,[260] valamint a nemzeti illetékes hatóságok és a nemzeti felügyeleti hatóságok részére is. Általánosságban a LED szorosan 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.
Véleményem szerint a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásának jogharmonizációs kihívásai rámutatnak arra, hogy az uniós és nemzeti szabályozások közötti egyensúly megteremtése folyamatos felülvizsgálatot és az érintettek jogainak proaktív védelmét igényli.

III.2.1. A bűnügyi irányelv átültetése a magyar nemzeti jogba

III.2.1.1. Előzmények [261]

Magyarországon az 1992. évi LXIII. törvény[262] - Avtv. - 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 Alkotmánybíróság (AB) 15/1991. (IV.13) határozata a személyes adatok védelmét információs önrendelkezési jogként határozta meg. A későbbiekben is fontos szerepet töltenek be az AB. határozatai a magyar adatvédelmi szabályozásban.
Az 1981-es Európa Tanács egyezmény hazai kihirdetése az 1998. évi VI. törvény[263]- 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

[260] Ibid.pp. 9-10.

[261] Gáti Balázs: "Az adatvédelmi jog fejlődésének főbb állomásai."

[262] 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."

[263]1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

anyag védelméről szóló 1995. évi LXVI. törvény. Az adatvédelmi törvény második módosítása az 1999. évi LXXII. törvény[264] 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. [265] Ez a módosítás kiterjesztette a személyes adatok kezelésére vonatkozó szabályokat, valamint az adatvédelmi biztos feladatait és jogkörét meghatározó rendelkezéseket, új fogalmakkal bővítve azokat. [266]

2011-ben az Alaptörvény – a korábbi Alkotmány által meghatározott alapjogi szintet megőrizve, számos AB. döntést is a tételes jog szintjébe épített, kimondta a független adatvédelmi felügyeleti hatóság létrehozásának szükségességét, amely az „Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény" (Infotv.) [267] alapjául szolgált. Ez a törvény és annak későbbi módosításai integrálták az adatvédelmi jog harmadik generációjának kulcsfontosságú elemeit.

III.2.1.2. Implementálás a 2011. évi CXII. törvénybe[268]

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.)[269] A módosító jogszabály

[264] 1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

[265] 2003. évi XLVIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról

[266] 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 Információszabadság 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."

[267] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[268] Gáti Balázs: "Az adatvédelmi jog fejlődésének főbb állomásai."

[269] 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.

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. korábban teljességgel lefedte a magyar adatvédelmi szabályozás területeit, kiegészítve az ágazati jogszabályokkal. Tekintettel arra, hogy a GDPR rendeleti formában jött létre, az közvetlenül alkalmazandó a tagállamokban, így a korábbi szabályozási rendszert a már említett Módtv. változtatta meg.

Szükséges volt, a GDPR által teljességgel szabályozott tárgykörök kivonására a rendelet hatálya alá tartozó jogviszonyokban. Ugyanakkor a GDPR közvetlen alkalmazhatóságához feltétlenül szükséges rendelkezések szabályozása, a bűnügyi irányelv átültetése, és a belső jogban történő teljes körű szabályozása, az uniós jog hatályán kívüli adatkezelési jogviszonyok szabályozása, és "a*z uniós jog által lehetővé tett, a GDPR-t és a bűnügyi irányelvet kiegészítő, az alkotmányossági és a nemzetközi jogi követelményekből fakadó rendelkezések szabályozása*"[270] is megoldásra várt.

A GDPR mindenféle adatkezelési műveletre vonatkozik, kivéve a személyes adatok természetes személy általi kizárólag saját személyes céljait szolgáló adatkezelésekre.[271]

A GDPR-nak való megfelelés 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. törvény [272], az emberi genetikai adatok védelméről szóló 2008. évi XXI. törvény, az állampolgárok személyi adatairól és lakcímnyilvántartásáról 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 felhasználásáról szóló törvény[273], az 1995. évi

[270] Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018. p.17.

[271] 2018. évi XXXVIII. törvény 1. §., Infotv. 2. §. 6.

[272] 1993. évi XCIII. törvény a munkavédelemről

[273] 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.

CXIX. törvény a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok felhasználásáról[274] és a panaszokról és a közérdekű bejelentésekről szóló törvényt.[275]

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.[276]

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 bűnügyi 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:

„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”

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 bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére is e törvényt kell alkalmazni.”*

[274] 1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

[275] 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.

[276] Infotv. 2. § (5) b). az adatkezelő vagy az általa megbízott, illetve az utasításai alapján eljáró adatfeldolgozó olyan adatkezelési műveletet végez, amely:

ba) Magyarországon tartózkodó érintettek számára történő áruk vagy szolgáltatások nyújtásával összefügg, függetlenül attól, hogy az érintettek részéről fizetés szükséges-e ezen termékekért vagy szolgáltatásokért, vagy

bb) az érintettek Magyarország területén tanúsított viselkedésének megfigyelésével áll kapcsolatban, amennyiben az adatkezelés célja az érintett viselkedésére vonatkozó információk gyűjtése és elemzése.

A nemzetbiztonsági és honvédelmi célú adatkezelés tágabb értelmezést jelent az irányelvi meghatározáshoz képest, a szabályozás szükségességét azonban az alapjogi szabályozás adja, mely törvényi szabályozást irányoz elő.

A módosított törvény a további fejezeteiben a kiegészítésekkel a GDPR végrehajtásához szükséges szabályozást és a korábbi szabályozás elemeit is tartalmazza,[277] valamint a személyes adatok védelmén túl, az információ biztonságot, a felügyeleti hatóságokkal kapcsolatos garanciákat, az eljárási szabályokat is jogszabályba foglalja, ahogy erre a fejezet címek is utalnak.[278] A törvény megtartotta a korábbi, információ biztonságot szabályozó funkcióját.

A NAIH –l kapcsolatos jogszabályok,[279] a bírósági adatkezelési műveletek ellenőrzése [280] az Infotv.-ben külön fejezetet kapott.[281]

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”*[282]

Az Infotv. a bűnügyi személyes adatok kezelésére vonatkozóan főszabály szerint továbbra is a különleges adatok kezelésének feltételeire vonatkozó szabályokat alkalmazza.[283]

---

[277] 2018. évi XXXVIII. törvény, 1. § (5) – 5. § (1) – (3), Infotv. 2. § (2)

[278] 2018. évi XXXVIII. törvény, 19. § (2a)(2b).

[279] Infotv. V. FEJEZET

[280] Infotv. VI/A. FEJEZET

[281] 2018. évi XXXVIII. törvény, 29. § . Az Infotv. a VI/A. Fejezettel egészült ki, a bírósági adatkezelési műveletek ellenőrzése címmel.

[282] 2018. évi XXXVIII. törvény, 2. § (6) , Infotv. 3. § 10. a.

[283] 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

A bűnügyi irányelv adatkezelése az Infotv.- ben a bűnüldözési célú adatkezelések[284] szerint szerepel a korábbi alkalmazásnak megfelelően, elkülönítve azt a személyes adatok büntetőjogi védelmétől.[285]

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"*[286]

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.[287]

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 szolgának.[288]

---

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

[284] Infotv. 3. § (10) a.)

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

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

[287] Infotv. 5. § (1) d). Az érintettnek tisztában kell lennie, azzal, hogy ezek az adatok nyilvánosak, és bárki számára Elérhetők.

[288] 2018. évi XXXVIII. törvény, 5. §, Infotv. 7. § (1).

Az érintetti jogokkal kapcsolatban a továbbiakban kiemelném azokat a jogokat, melyben az Infotv. ténylegesen megjeleníti azokat a korlátozásokat, amelyek a bűnüldözési célú adatkezelésekkel kapcsolatosak, és amelyeket az Irányelv 23. cikke együttesen tárgyal.[289]

A tájékozódáshoz való jog: a törvény 14. szakaszának a) pontja rendelkezik az "*előzetes tájékoztatáshoz való jogró*l". 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.[290]

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.[291]

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

[289] (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.

[290] 2018. évi XXXVIII. törvény, 9. §, Infotv. 16. § (1)

[291] Infotv. 16. § (3)

szükséges annak biztosításához. A feltételek azonosak a tájékoztatási joggal kapcsolatban leírtakkal.[292]

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 meghatározott 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.[293]

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.[294] 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.[295]

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.[296] Ezen kívül feltétel, hogy nem sérti az egyenlő bánásmód követelményét, az adatkezelő vagy az adatkezelő nevében eljáró vagy általa utasított

---

[292] 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.

[293] „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

[294] Infotv. 21. § (1).

[295] Infotv. 21. § (2). A 16. § (3) bekezdés *a)–f)* pontjában meghatározott valamely érdek biztosításához.

[296] Infotv. 6. §

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

Az adattovábbítás feltételei[297] között részletesen szabályozza a bűnüldözési célú adatkezelés esetén nemzetközi adattovábbítás feltételeit a korlátozásokkal együtt.[298] Az EU/EGT valamely tagállamába történő adattovábbítás nem igényel további megfelelő biztosítékokra vagy eltérésekre való szabályozást.

A GDPR-ral összhangban az adatkezelők vagy adatfeldolgozók személyes adatokat továbbíthatnak harmadik országbeli adatkezelőknek vagy adatfeldolgozóknak, ha: az adattovábbítás az Európai Bizottság megfelelőségi határozatán alapul[299], 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 teljesülnek[300],*
- *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 képviseletében eljáró más szerv vagy személy előzetesen jóváhagyta, vagy a közvetett*

[297] 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.

[298] 2018. évi XXXVIII. törvény, 6. § , Infotv. 10. § (2) -12. § (2)

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

[300] 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 beszerzése[301] *ezen érdekek sérelme nélkül a nemzetközi adattovábbítást megelőzően nem lehetséges.*[302] *''*

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.[303]

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 Infotv. tételesen azonban nem különíti el, hanem egységes szerkezet alatt tárgyalja a bűnügyi irányelv rendelkezéseit a korábbi törvény szerkezetének megfelelően, a GDPR alkalmazásához feltétlenül szükséges szabályozást beépítve, és deregulálva a GDPR közvetlenül hatályosuló szabályait.

III.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.''*[304]

[301] Infotv. 10. § (2). *ca.)*

[302] Infotv. 10. § (2).

[303] Megállapította: 2018. évi XXXVIII. törvény 32. §. Hatályos: 2018. VII. 26-tól

[304] (EU) 2016/680, 1. cikk (3).

Németország volt az első EU-tagállam, amely a GDPR-nak való megfelelést a német szövetségi adatvédelmi törvény keretén belül - Bundesdatenschutzgesetz[305] (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.

III.2.2.1. Előzmények

Németország, pontosabban Hessen tartomány is adatvédelmi történelmet írt. Mint ismeretes a világ első adatvédelmi törvénye itt jött létre.[306] 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 világossá 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"[307] (BDSG) - (Törvény az adatfeldolgozás során a személyes adatokkal való visszaélés elleni védelemről[308]) címmel. Célja, hogy megakadályozza a kormányzati szervek, és a vállalatok korlátozás nélkül felhasználhassák a személyes adatokat. Ezért megállapították, hogy az ilyen adatok feldolgozása csak akkor engedélyezett, ha az érintett ehhez hozzájárult, vagy a szövetségi

[305] "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. (hozzáférés 2022.07.02.)

[306]Das Hessische Beamtengesetz in der Fassung vom 16. Februar 1970. URL: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf. (hozzáférés 2022.07.02.)

[307]Bundesgesetsblatt, 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. (hozzáférés 2022.07.02.)

[308] saját fordítás

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.[309] 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 Biztos[310] egyben az Információszabadság Szövetségi Biztosa is, és gondoskodik e törvény rendelkezéseinek betartásáról.

[309] 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 (hozzáférés 2022.07.02.)

[310] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit https://www.bfdi.bund.de/DE/Home/home_node.html (hozzáférés 2022.07.02.)

III.2.2.2. A németszövetségi adatvédelmi törvény az adatvédelmi reform után [311]

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)[312]. 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-et harmonizálja. A 16 tartomány mindegyike új állami adatvédelmi törvényt fogadott el a GDPR-nap való megfelelést illetően 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 - együttesen értelmezendők.

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

A németszövetségi adatvédelmi törvény négy részből, hét fejezetből és nyolcvanhat szakaszból épül fel.

[311] 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)."

[312] 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

Az I. rész Közös rendelkezések címszó alatt a törvény hatályát, és a fogalommeghatározásokat tartalmazza az első fejezetben [313], a második fejezet a személyes adatok feldolgozásának jogalapját, ezen belül a személyes adatok állami szervek általi feldolgozását, és a nyilvánosan hozzáférhető helyek videó megfigyelését tárgyalja.[314]

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.[315]

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 a GDPR hatálya alá esik. [316]

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.[317]

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 esetében[318] 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.

[313] BDSG 1. § (1), (2)

[314] BDSG 1. § (3), (4)

[315] BDSG 1. § (1)

[316] BDSG 1. § (4)

[317] BDSG 3. §

[318] BDSG 3. § (1),(3)

Ha a videokamerás megfigyelés során gyűjtött adatokat egy adott személyhez kötik, az érintett személyt az (EU) 2016/679 rendelet 13. és 14. cikkének megfelelően tájékoztatni kell az adatkezelésről, e törvény 32. §-a megfelelően alkalmazandó.[319,320]

A harmadik fejezet részletesen foglalkozik a köztestületek 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 hatáskörét.[321] A 14. szakasz kiemeli, hogy a szövetségi biztos az (EU) 2016/680 irányelv hatálya alatt, annak a 60. cikke szerinti feladatot is ellátja.[322]

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.[323]
- A BDSG 61§ (1) bekezdése megfelelően alkalmazandó az adatalanyokra is, ha a Szövetségi Biztos nem foglalkozik a panasszal a 60. cikk értelmében, vagy nem

[319] BDSG (3. § 4)

[320] 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 autóbuszközlekedési létesítmények esetében a jelenlévő személyek életének, egészségének és szabadságának védelmét nagyon fontos érdeknek kell tekinteni.

[321] BDSG 5. § – 16. §

[322] (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."

[323] BDSG 61.§ (1)

tájékoztatja az adatalanyt a panasz előre haladásáról vagy eredményéről három hónapon belül.[324]

Az ötödik fejezet az Európai Adatvédelmi Testületben történő képviseletről szól,[325] a hatodik fejezet a jogorvoslati lehetőségeket szabályozza.[326]

Németországnak a szövetségi adatvédelmi hatóságon kívűl, 16 állami adatvédelmi hatósága is van, amelyek mindegyike a GDPR hatálya alá is 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 területén[327] A magánszervezetek szemszögéből a „fő szabályozó" az az illetékes állami hatóság, amely a GDPR-nak való megfelelés szerinti ellenőrzésre illetékes.[328]

A BfDI feladatait illetően kiemelném, hogy az (EU) 2016/680 irányelv végrehajtására is elfogadott jogszabályokat.[329] 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 felelősségekkel kapcsolatban a BfDI hatáskörébe tartozik a Szövetség állami szerveinek felügyelete.[330] A BDSG 16. szakasza előírja, hogy a BfDI rendelkezik a GDPR 58. cikkében említett hatáskörökkel.[331]

---

[324] BDSG 61.§ (2)

[325] BDSG 17.§ – 19.§

[326] BDSG 20.§ – 21.§

[327] BDSG 40. §

[328] 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.

[329] BDGSG 14. §.(5) (6) (7) (8)

[330] BDGSG 9. §.

[331] 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 biztosítania

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.[332] 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.[333]

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.[334,335]. 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

---

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.

[332] BDSG 22. § - 44.§

[333] BDSG 24. §

[334] BDSG 22. §,(1)

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

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.[336]

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. Ezek a hozzáférési jog (GDPR 15. cikk), a 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.[337]

Az adatokhoz való hozzáférést illetően a német szövetségi törvény további korlátozásokat ír elő a GDPR 15. cikkével kapcsolatban.[338]

---

[336] BDSG 27. §, 28. §.

[337] 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 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 információszolgáltatás 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.

[338] BDSG 34. § (1)

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.[339]

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.[340]

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 szabályozást, a bűnügyi adatvédelmi irányelv tulajdonképpeni átültetését tartalmazza.

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.[341]

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*

[339] 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 GDPR nem automatizált feldolgozás szerinti tárgyi hatálya alá tartoznak.

[340] BDSG 28. § (4)

[341] BDSG 45.§ - 86.§

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."*[342] A LED németországi végrehajtásakor például az úgynevezett Ordnungswidrigkeitenre[343] is alkalmazhatóvá vált, amely nem minősül büntetőjogi szabálysértésnek 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 végrehajtási rendelkezéseinél szabályozott 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 szervezetfelelős a 45. szakaszban említett célokért [344] és
- az Európai Bizottság az (EU) 2016/680 irányelv 36. cikkének (3) bekezdése alapján megfelelőségi határozatot fogadott el.[345]
- a személyes adatok továbbítása megfelelőségi 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

[342] 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.

[343] Közigazgatási szabálysértés

[344] EDPB, Európai Bizottság

[345] BDSG 45.§ (1)

jogszabályoknak megfelelően és az alapvető emberi jogokkal összhangban kezeljék.[346,347]

Adattovábbítás megfelelő biztosítékokkal[348] és az adattovábbítás megfelelő biztosítékok nélkül[349] 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 kapcsán, [350] 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 információkérésekre és a felügyeleti intézkedésekre, mint például a konzultációk, vizsgálatok és vizsgálatok lefolytatására irányuló megkeresésekre,[351]
- minden szükséges intézkedést megtesz annak érdekében, hogy a kölcsönös segítségnyújtás iránti megkeresésre haladéktalanul, de legkésőbb a kérelem kézhezvételétől számított egy hónapon belül válaszoljon,[352]
- csak akkor tagadhatja meg a kérelem teljesítését, ha nem illetékes a megkeresés tárgyára vagy az általa végrehajtandó intézkedésekre, vagy a felszólítás teljesítése jogszabályba ütközne,[353]

---

[346] BDSG 45.§ (2)

[347] 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.

[348] BDSG 80.§

[349] BDSG 81.§

[350] BDSG 82.§

[351] BDSG 82.§ (1)

[352] BDSG 82.§ (2)

[353] BDSG 82.§ (3)

- 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,[354]
- a másik állam felügyeleti hatósága által kért információkat rendszerint elektronikus úton, szabványos formátumban adja meg,[355]
- 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,[356] 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.[357]

A felelősség és szankciók tekintetében a kártérítésre a német polgári törvénykönyv. szabályait[358] kell alkalmazni.[359]

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 implementálja az a bűnügyi adatvédelmi irányelvet, és egy törvényi szerkezetben határozza meg a GDPR végrehajtási szabályait, és az attól eltérő korlátozásokat, szabályozási módokat.

A német adatvédelmi törvény –és annak bűnüldözési célú adatkezelésre vonatkozó része – egy komplex és szigorúan szabályozott rendszert alkot, amely egyszerre követi az uniós jogi kereteket, ugyanakkor figyelembe veszi a szövetségi struktúrából eredő sajátos igényeket is.

A közös rendelkezéseknél lefekteti a törvény hatályát és a kulcsfontosságú fogalommeghatározásokat. Az egyik lényeges elem, hogy a törvény személyi hatálya nemcsak a Szövetség és a tartományok állami szerveire terjed ki, hanem azokra az igazságügyi szervekre és magánszervezetekre is, amelyek közhatalmi funkciókat látnak el. Ez a megközelítés

[354] BDSG 82.§ (4)

[355] BDSG 82.§(5)

[356] BDSG 82.§ (6)

[357] BDSG 82.§ (7)

[358] Bürgerliches Gesetzbuch (BGB), Gesetze im Internet, https://www.gesetze-im-internet.de/bgb/(hozzáférés 2022.07.02.)

[359] BDSG 83.§

összhangban van az Európai Unió adatvédelmi szabályaival, ugyanakkor a tagállami végrehajtás szempontjából megkülönbözteti a német modellt más jogrendszerektől, amelyek jellemzően szűkebb körben határozzák meg az adatkezelés alanyait.

III.2.3 A bűnügyi irányelv átültetése a francia nemzeti jogba[360]

Franciaországban 2018. júniusban hirdették ki, és lépett hatályba a 2018. június 20-i 2018-493. számú törvény[361], a francia adatvédelmi jogszabály módosítása az uniós adatvédelmi reformnak megfelelően.

A francia törvény- a magyar és német jogszabályhoz hasonlóan - a GPDR nemzeti végrehajtásához kapcsolódó rendelkezések mellett, e törvényi szabályozás keretében implementálja a bűnügyi célú adatkezelést.

III.2.3.1 Előzmények

Franciaország első adatvédelmi törvénye 1978. január 6-án lépett életbe, amely egyúttal létrehozta a francia adatvédelmi hatóságot, a „la Commission Nationale de l'Informatique et des Libertés (CNIL) - t."[362] Az 1974-ben az úgynevezett „SAFARI" botrányt követően jött létre a CNIL, a francia közigazgatás azon terve kapcsán, hogy társadalombiztosítási számon keresztül összekapcsolják a névleges állományokat, így szükség volt a személyes adatok felhasználásának szabályozására.[363]

A francia adatvédelmi törvény az 1978. január 6-i 78-17. számú törvény (Informatique Libertè) „Az adatkezelésről, a fájlokról és a szabadságjogokról"[364], melyek egyes cikkeit, rendelkezéseit már az uniós adatvédelmi reform előtt is módosították, többek között a személyes adatok

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

[361] LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personalles (1)

[362] A Számítástechnikai és Szabadságjogok Nemzeti Bizottsága (saját fordítás)

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

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

védelméről szóló 95/46/EK irányelv végrehajtásáról szóló 2004. augusztus 6-i 2004-801 számú törvénnyel.[365]

Franciaországban a 2016-1321 számú „A digitális köztársaságról szóló törvény”[366] előre vetítette az általános adatvédelmi rendeletet, az elektronikus szolgáltatásokra vonatkozó az adatgazdaság, az online adatok védelmének, és a digitális hozzáférés jogszabályainak megalkotásával.[367]

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 végrehajtási rendelkezést ekkor még nem szabályozott, úgymint 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”[368] törvény új változatban van hatályban.[369] Tartalmazza a korábbi módosító törvény említett hiányosságait. Az

---

[365] 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/ (hozzáférés, 2022.07.12.)

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

[367] France – „Data Protection Overview”

[368] 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)

[369] 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.

Informatique et Libertés törvény nem hivatott teljes mértékben lefedni a GDPR rendelkezéseit,- azt nem is tehetné meg, - 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. június 1-én módosított törvényt együtt kell értelmezni. A 2019-s adatvédelmi törvény teljes körűen alkalmazható valamennyi Franciaországhoz tartozó tengerentúli területen is.

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

A francia adatvédelmi hatóság, a CNIL [370] honlapja szerint, az első módosított törvény a GDPR-ral ellentétes rendelkezéseket megszűntette és kiegészítette a szükséges rendelkezésekkel, beleértve az alábbiakat.[371,372]

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).

Ezen felül 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

---

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.

[370] A Számítástechnikai és Szabadságjogok Nemzeti Bizottsága (saját fordítás)

[371] CNIL, https://www.cnil.fr/fr/entree-en-vigueur-de-la-nouvelle-loi-informatique-et-libertes (2022.07.12)

[372] 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
/ (hozzáférés, 2022.07.12.)

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 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. A Conseil d'Etat jogosult ideiglenesen felfüggeszteni a nemzetközi adattovábbítást, ha a CNIL ezt indokoltnak tartja (27. cikk).

III.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 közvetlen 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).[373]

[373] 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.

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

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. [374]

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. [375] 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.. [376]

A CNIL, a GDPR jelentése és alkalmazása szerinti nemzeti felügyeleti hatóság.[377] A fogalmak nagy részét nem határozza meg, hivatkozik a GDPR adott cikkeire.[378] Az alapelvek a GDPR-nak megfelelőek.[379]

A törvény a GDPR 33. cikkére hivatkozik a CNIL-nek történő adatvédelmi incidens bejelentésére vonatkozóan.[380]

A személyes adatok különleges kategóriáinak kezelése meghatározott kivételekkel tilos.[381]

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,

[374] Informatique et Libertés, Article 8. I.

[375] Informatique et Libertés, Article,3. I.- II.

[376] Informatique Liberté n°78-17, 3. cikk II. szakasz

[377] Informatique et Libertés, Article 2. I.

[378] Informatique et Libertés, Article 1- 7.

[379] Informatique et Libertés, Article 4.

[380] Informatique et Libertés, Article 58.

[381] Informatique et Libertés, Article 6. kivételek: Article 44.

- az általuk kezelt szellemi tulajdonjogok vagy a szellemi tulajdonjogok megsértésének áldozatai nevében eljáró közös jogkezelő szervezetek, és
- a bírósági határozatokban foglalt nyilvános információk újra felhasználói feltéve, hogy a feldolgozásnak nem célja, és nem is jár azzal, hogy lehetővé tegye az érintett személyek újbóli azonosítását.[382]

Az érintetti jogoknál[383] is közvetlenül 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.[384]

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.[385]

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,[386] újságírói, irodalmi vagy művészi alkotási cél,[387] vagy bűncselekmények megelőzése, kivizsgálása és büntetőeljárás alá vonása esetében történik.[388]

A hozzáférési jog, a bűncselekmények megelőzésével, kivizsgálásával, felderítésével vagy büntetőeljárás alá vonásával, illetve az állam nevében hozott büntetőjogi szankciók vagy

[382] 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 közlésekor lehetséges-e a személyek újbóli azonosítása.

[383] Informatique et Libertés, Article 48.

[384] Informatique et Libertés, Article 48.

[385] Informatique Liberté n°78-17, 107. cikk IV. szakasz

[386] Informatique et Libertés, Article 79.

[387] Informatique et Libertés, Article 80.

[388] Informatique et Libertés, Article 107., 108.

szabadságelvonással járó végzések végrehajtásával kapcsolatos adatkezelés tekintetében nem korlátozott, kivéve, ha a személyes adatokat bírósági határozat vagy bírósági akta tartalmazza.[389] 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 bírája felelős azért, hogy az érintett nevében elvégezze a szükséges javításokat.[390]

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.[391] Nincsenek azonban ilyen korlátozások az állambiztonsággal - és védelemmel kapcsolatos adatkezelésre,[392] valamint a bűncselekmények megelőzése, kivizsgálása és üldözése céljából végzett adatkezelésre vonatkozóan.[393]

---

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

[390] A helyesbítéshez való jog nem vonatkozik az irodalmi, újságírói vagy művészeti feldolgozásra sem.

[391] 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.

[392] Informatique et Libertés, Article 120.

[393] 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 EDPB[394] és a CNIL[395] részéről is. Franciaországban főszabály szerint tilos az EGT-régión kívülre 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 kívülre továbbító adatfeldolgozóknak általában végrehajtható szerződéses megállapodásokra[396] 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.[397]
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. [398’399]

---

[394] 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"

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

[396] Például az Európai Bizottság által kiadott általános szerződési feltételekre

[397] Informatique et Libertés, Article 87.

[398] Informatique et Libertés, Article 89.

[399] 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 [400], 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.[401]

Az illetékes hatóságokkal kapcsolatos kötelezettségek is megegyeznek az irányelvben közzétettel. Az egyes szabályozások gyakorlati megvalósítását illetően a francia illetékes hatóságok és bizottságok szerepelnek felelősként.[402]

[400] Informatique et Libertés, Article 112.

[401] Informatique et Libertés, Article 100.

[402] 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 rendelet végrehajtási szabályozással együtt történt meg, jelenleg egységes szerkezetben ez a törvény hatályos. A GDPR közvetlen hatályosulását a törvény közvetlen hivatkozásokkal biztosítja. 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.

Véleményem szerint Franciaország adatvédelmi szabályozása a bűnüldözési célú adatkezelés területén jól illeszkedik az uniós jogi keretekhez. A fokozatos harmonizáció eredményeként kialakult egységes jogszabályi struktúra biztosítja a GDPR és a LED követelményeinek való megfelelést.

III.2.4 A bűnügyi irányelv átültetése a svéd nemzeti jogba

III.2.4.1. Előzmények

Svédország volt az első ország Európában, amely adatvédelmi jogszabályokat fogadott el - SFS 1973:289[403] - az 1973-as adattörvény beiktatásával. Ez a törvény hozta létre a Svéd Adatvédelmi Hatóságot - Integritetsskyddsmyndigheten (IMY).[404]

A következő svéd személyes adatokról szóló törvény, az - SFS 1998:204[405] 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

---

[403] Datalag (1973:289)https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289 (hozzáférés,2022.07.15.)

[404] Integritetsskyddsmyndigheten, https://www.imy.se (hozzáférés: 2022.07.15.)

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

kiegészítő rendelkezéseit tartalmazó törvény - SFS 2018:218[406] - lépett hatályba. A törvényen kívül egy másik a GDPR kiegészítő rendelkezéseit tartalmazó rendeletet - SFS 2018:219[407] – is elfogadták. Ez azt jelenti, hogy a svéd adatvédelmi rendszer a vonatkozó nyilvántartási rendelettel együtt értelmezendő.[408]

Ezeket kiegészítik azonban ágazati adatkezelési tevékenységekre irányuló törvények, úgymint a svéd betegadatokról szóló törvény - SFS 2008:355,[409] amely szabályozza a személyes adatok kezelésének módját az egészségügyi szektorban. A svéd hitelinformációs törvény - SFS 1973:1173[410] - védi az egyének magánéletét a hitelinformációs szolgáltatásokkal kapcsolatban. Az SFS 2018:1177 számú törvény[411] 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 végrehajtását szabályozó 2018:218 számú törvénnyel együtt része az EU adatvédelmi reformcsomagjának.

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

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

---

406 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.)

407 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, (hozzáférés,2022.07.15.)

408 Sweden - Data Protection Overview, Guidance Note, https://www.dataguidance.com/notes/sweden-data-protection-overview, (hozzáférés,2022.07.01)

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

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

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

A GDPR 2. cikkében foglaltakkal ellentétben a törvény [412] kiterjeszti a GDPR hatályát a személyes adatok kezelésére is az alábbi esetekben:

- olyan tevékenység, amely kívül esik az uniós jog hatályán, és
- az Európai Unióról szóló szerződés V. címe 2. fejezetének hatálya alá tartozó tevékenységek végzése esetén is alkalmazható.[413]

A törvény hatálya azonban nem terjed ki, a Svéd Fegyveres Erők Külföldi Hírszerző Műveleti és Katonai Biztonsági Szolgálatára - SFS 2007:258[414]-, a Nemzetvédelmi Rádióállomás működésére - SFS 2007:259[415] -, vagy a Svéd Biztonsági Szolgálat által a személyes adatok kezeléséről szóló törvényre - SFS 2019:1182 [416].

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 gyermekre vonatkozik, függetlenül attól, hogy az adatkezelő vagy adatfeldolgozó hol található. [417]

Az érintetti jogok esetében,[418] a tájékoztatási joggal és a hozzáférési joggal kapcsolatosan általános kivételt állapít meg a tájékoztatás és a személyes adatokhoz való hozzáférés alól [419]

[412] SFS 2018:218, 1. ch. 2 .§.

[413] 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 terméknyújtáshoz vagy szolgáltatásnyújtáshoz kapcsolódik, vagy Svédországban tanúsított magatartásuk nyomon követéséhez szükséges.

[414] 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.)

[415] 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.)

[416] Lag om Säkerhetspolisens behandling av personuppgifter Utfärdad den 28 november 2019, https://svenskforfattningssamling.se/sites/default/files/sfs/2019-11/SFS2019-1182.pdf, (hozzáférés: 2022.07.15.)

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

[418] SFS 2018:218, 5. ch. 1.§.

[419] GDPR 13. és 14. cikk

azokban az esetekben, amikor más jogszabályok tiltják az információk közlését az érintettekkel.[420]

A helyesbítési-, a törlési-, az adatkezelés korlátozásához való-, **t**iltakozási-, adathordozhatósághoz való joggal kapcsolatosan nincsenek nemzeti eltérések. Általánosságban megfogalmazható, hogy a törvény felhatalmazza a kormányt[421], hogy további rendeleteket bocsásson ki a GDPR korlátozásokra vonatkozó cikkei alapján. [422] 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 következik.[423]

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.

---

[420] 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

[421] SFS 2018:218, 5. ch. 3.§.

[422] GDPR 23. cikke, 89. cikkének (2) bekezdése és 89. cikkének (3) bekezdése alapján

[423] 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.)

Az adattovábbítás esetén a korlátozások a különleges adatok kategóriáira vonatkoznak.[424] A GDPR V. fejezetében meghatározott, határokon átnyúló adattovábbításra vonatkozó korlátozások a személyes adatoknak az EU/EGT régión 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 gyermek 13 éves vagy idősebb[425]. Azonban az IMY által kiadott jogszabály[426] 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 2007:975[427]. 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*”.[428]

A megfelelőség ellenőrzése és az ellenőrzések lefolytatása mellett az IMY jogosult adatvédelmi jogszabályokat kiadni. Az IMY többek között törvénysértésekkel kapcsolatos személyes adatok feldolgozására vonatkozó jogszabályt - DIFS 2018:2[429] - alkotott, amely kifejezetten a magánszemélyek bűncselekményekkel és jogsértésekkel összefüggő személyes adatainak kezelésére vonatkozik.

---

[424] 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.

[425] SFS 2018:218, 2. ch. 4 .§

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

[427]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 (hozzáférés:2022.07.15.)

[428] saját fordítás

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

Az IMY emellett állásfoglalást is kibocsátott a bűncselekményekkel összefüggő személyes adatok kezeléséről, amely összhangban áll a svéd adatvédelmi törvény előírásaival.[430,431]

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 feldolgozhatják, ha az adatkezelés az archiválási rendelkezéseknek való megfelelés érdekében szükséges[432]

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 tevékenységet.[433] 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 szükséges.[434] Az IMY azonban kijelentette, hogy nem engedélyezett a büntetőjogi felelősséget megállapító ítéletekre vonatkozó adatok feldolgozása az érintetti hozzájárulása alapján.[435]

---

[430] SFS 2018:218, 2. ch. 8 .§.

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

[432] SFS 2018:218, 3. ch. 8.§

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

[434] SFS 2018:218, 5. ch.

[435] 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.

III.2.4.3. A svéd bűnügyi adatokról szóló törvény SFS 2018:1177 [436]

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 - 2013:329[437] számú törvényt. A hatályba lépés előtt történt jogsértésekre, valamint a hatálybalépés előtt bejelentett határozatok elleni fellebbezésekre továbbra is a régebbi szabályozás vonatkozik.[438]

A törvény a személyes adatoknak a bűnmegelőzési és bűnüldözési feladatokat ellátó hatóságok, úgymint a svéd rendőrség, a svéd adóhatóság és a svéd vámhatóság által végzett adatok kezelésére és feldolgozására vonatkozik, és a GDPR-al azonos az elveken alapul.

A hatóságoknak 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, úgy, mint a 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 címeket viseli.

Első fejezete az általános rendelkezések keretében[439] a célokat illetően megfogalmazza az uniós ajánlásokat. A hatályát illetően kiemelném, hogy 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 nem vonatkozik a személyes adatok fegyveres erők általi kezeléséről szóló törvény (2021:1171), illetve a fegyveres műveletekkel kapcsolatos törvény által meghatározott adatkezelésekre (2021:1175) sem.[440] Amennyiben az alkotmányban szereplő más törvény vagy rendelet e törvénytől eltérő rendelkezést tartalmaz, azt a rendelkezést kell alkalmazni[441]

---

[436]Brottsdatalag, (2018:1177) .

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

[438] SFS 2018:1177 , Övergångsbestämmelser, 2. , 5-6.

[439] SFS 2018:1177,1 ch.

[440] SFS 2018:1177, 1 ch. 4. § A.

[441] SFS 2018:1177, 1 ch., 4. §.

A fogalom meghatározások terén a regisztrált, a harmadik ország és harmadik fél fogalmait is meghatározza.[442]

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. fejezete [443] 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 szövegkörnyezetből vagy más módon, azt külön közzététellel kell egyértelművé tenni.[444] Ezt a személyes adatok egyes kategóriának kezelésénél is láthatjuk, ha a szövegkörnyezetből vagy más módon nem derül ki, hogy a személy melyik kategóriába tartozik, azt külön közzététellel szükséges egyértelművé tenni.[445] A törvény 3. 4. 6. és 7. fejezetei a bűnügyi irányelvvel azonos szabályozást írnak elő.

A törvény bűnügyi célú adattovábbításokkal kapcsolatosan konkrét követelményeket tartalmaz a személyes adatokat 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.[446]

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,

[442] SFS 2018:1177,1 ch., 6. §

[443] SFS 2018:1177, 2 ch. 1-23.§.

[444] SFS 2018:1177, 2 ch.

[445] SFS 2018:1177, 2 ch. 9. § .

[446] Brottsdatalag (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.[447,448]

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.[449] 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 szükséges [450]. 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.[451]

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 Unión belüli rendőrségi és igazságügyi együttműködés során a személyes adatok védelméről szóló egyes rendelkezésekről szóló - 2013:329 [452] - törvényt, így a személyes adatok bűnügyi célból történő kezelésére az 2018:1177 számú törvény szolgál. Az általános adatvédelmi rendelet végrehajtási szabályozását az SFS 2018:218 törvény és a GDPR kiegészítő rendelkezéseit tartalmazó rendeletet - SFS 2018:219– együttesen alkotja. Ez a jogi struktúra biztosítja az uniós adatvédelmi reformcsomag egységes alkalmazását Svédországban. A svéd bűnügyi adatokról szóló törvény (SFS 2018:1177) hatálya kiterjed a bűnmegelőzési és bűnüldözési feladatokat ellátó hatóságokra, mint például a svéd rendőrség, az adóhatóság és a vámhatóság. Nem vonatkozik azonban a nemzetbiztonsági adatkezelésekre, így például a Svéd Biztonsági Szolgálat és a fegyveres erők adatkezeléseire
A felügyeleti hatóság, az Integritetsmyndigheten (IMY), kulcsszerepet játszik az adatvédelmi jogszabályok betartásának ellenőrzésében, és rendelkezik jogalkotási hatáskörrel is.

[447] Brottsdatalag (2018:1177),), 2. ch. 1. §. 1.-3 .

[448] A megfelelő védelmi szinteket a törvény 2. fejezetének 3. és 4. szakasza szabályozza.

[449] Brottsdatalag (2018:1177).

[450] Brottsdatalag (2018:1177), 8. ch.1. – 2. §.

[451] Brottsdatalag (2018:1177), 2 ch. 20. §

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

Összességében a svéd adatvédelmi rendszer három fő pilléren nyugszik: az általános adatvédelmi törvény (SFS 2018:218), a bűnügyi adatokról szóló törvény (SFS 2018:1177), valamint az ezek kiegészítésére szolgáló rendeletek és az IMY által kiadott szabályozások. Ez a rendszer biztosítja az EU adatvédelmi szabályainak hatékony nemzeti szintű végrehajtását és az érintettek jogainak védelmét.

III.3. Az egyes nemzeti szabályozások összehasonlító vizsgálata

III.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.[453]

A magyar szabályozás ezen elvek mentén, az információszabadságról 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 információszabadság törvény megalkotásához. A Nemzeti Adatvédelmi és Információszabadság Hatóságot a korábbi törvény hozta létre.

Az Infotv. a harmonizált szabályok mellett megtartotta a korábbi rendelkezéseket, és a változások kiemelésével implementálta az irányelvet, valamint lehetővé tette a GDPR közvetlen alkalmazását, egyúttal kiegészítve az uniós jog hatályán kívüli adatvédelmi szabályokkal.[454]

---

[453] Palánkai, Tibor.(2019.)"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

[454]„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"
Sziklay Júlia , Bendik Tamás. "Az adatvédelem hazai és európai uniós szabályozása és alapintézményei." Budapest: NKE, 2018, p.17.

A törvény a bűnügyi személyes adatok kezelésére vonatkozóan továbbra is a különleges adatok kezelésének feltételeire vonatkozó szabályokat alkalmazza**.** A nemzetbiztonsági célú adatkezelések és a honvédelmi célú adatkezelések – mint a nemzeti jog által szabályozandó adatkezelési jogviszonyok – szintén az Infotv. hatálya alá tartoznak. A törvény megtartotta az információ biztonság szabályozását a korábbiaknak megfelelően.

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 igazították. 2001 májusától hatályba léphetett a felülvizsgált szövetségi adatvédelmi törvény, majd 2006. január 1-én pedig hatályba lépett az információszabadságról 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 implementálja az irányelvi szabályokat. 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 egy törvényi keretben ülteti át az EU 2016/680 rendeletét, és egészíti ki azt a GDPR végrehajtási szabályaival. 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 bűnügyi adatvédelmi irányelvet valamint hivatkozott az általános adatvédelmi rendelet, vonatkozó helyeire. 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 perrendtartást[455] és a Büntető Törvénykönyvet [456]. Végül e módosításokkal a 78-17. számú törvény felépítésében és szövegében is változott, külön fejezet cím alatt szabályozza a bűnügyi 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.

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- hoz alakított nyilvántartási szabályokat 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 irányelvét 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 egységes szerkezeti keretben, 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

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

[456] Code pénal, https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070719/, (hozzáférés: 2022.07.15).

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.

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

A Bizottság jelentései alapján,[457,458] 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. [459]
A Bizottság tagállami szakértői csoportot hozott létre, hogy segítse a tagállamokat abban, hogy a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet beépítsék nemzeti jogukba.[460]
A megfelelőségi 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

[457] COM (2020) 262 final, 2020

[458] COM (2022) 364 final, 2022

[459] Ibid.2.1.

[460] 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

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 az alábbiakban a teljesség igénye nélkül néhány irányelvi szempontot kiemelve teszek összehasonlítást az általam vizsgált német, francia, svéd és a magyar harmonizáció során, megemlítve, ha ahhoz kapcsolódik a Bizottság jelentését is.

III.3.2.1. Az irányelv hatályának érvényesülése

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

- A magyar joggyakorlat ezt jól tükrözi, és e két feltétel szempontjából megfelel az irányelvnek. A LED a közbiztonság érdekében végzett feldolgozási tevékenységekre is vonatkozik, a nemzetbiztonsági- és honvédelmi célú tevékenységekre azonban nem.[461] Az Infotv. kiterjesztette a törvény hatályát a nemzetbiztonsági- és honvédelmi célú adatkezelésekre is „az *Infotv. előírásainak teljességét rendelte el alkalmazni”.* [462.]
- A német BDSG 45. szakasza az (EU) 2016/680 irányelv hatályával kapcsolatban egyértelműen megjelöli az irányelv szerinti bűnügyi 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”*.[463] Alkalmazható azokra a közigazgatási szabálysértésekre is, amely nem minősülnek büntetőjogi szabálysértésnek

[461] A LED 2. cikke (3) bekezdésének a) pontja és a LED (14) preambulumbekezdése.

[462] „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; bűnügyi irányelv 2. cikk (3) bekezdés a) pont] körébe tartozó jogviszonyokra is - főszabály szerint - a bűnüldözési 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.

[463] Bürgerliches Gesetzbuch, BGB, 11. § (1) 8.

és csak pénzbírság formájában kiszabott közigazgatási szankciókkal sújthatók. A BDSG tárgyi hatálya ebben a tekintetben eltér a bűncselekmény szűkebb értelmezését alkalmazó országokban megfigyelhető joggyakorlattól, amelyek a hasonló közigazgatási szankciókat nem tekintik a LED végrehajtása alá tartozónak.[464]

- A francia 78-17. számú adatvédelmi törvény a 87. cikkben határozza meg az irányelv szerinti hatályt. Eszerint ezt „*kell alkalmazni a személyes adatoknak a bűncselekmények 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 előjogok gyakorlásával megbízott bármely más szerv vagy szervezet (a továbbiakban: illetékes hatóság) általi kezelésére.*" A 87. cikk külön kitér a hatóságok GDPR szerinti adatkezelési céljaira. A 2018. júniusi törvényben még szerepelt a nemzetbiztonság védelme az adatkezelés céljai között, a jelenleg hatályos törvényben már nem szerepel.[465]
- 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."*[466] 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.[467] Nem vonatkozik továbbá a személyes adatok fegyveres erők általi kezeléséről szóló törvényre, illetve fegyveres műveletekkel

[464] 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.

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

[466] 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.

[467] SFS 2018: 1177, 1.ch.4.§

kapcsolatos törvény által meghatározott adatkezelésekre. Az illetékes hatóság fogalmát a törvény 6. szakasza határozza meg, nevesítve a bűnüldözési célt.

A „bűncselekmény” fogalmának pontos meghatározása kulcsfontosságú annak eldöntéséhez, hogy egy adott adatfeldolgozás a LED alkalmazási körébe tartozik-e. Az Európai Unió Bírósága (EUB) szerint a bűncselekmény büntetőjogi jellegének megítéléséhez három szempont releváns: a nemzeti jog szerint a cselekmény bűncselekménynek minősül-e, a cselekmény belső természete, az elkövetőre kiszabott büntetés súlyosságának mértéke.
A LED (13) preambulumbekezdése szerint a „bűncselekmény” fogalma autonóm jellegű, ami azt jelenti, hogy a tagállami jog nem alakíthatja át a bűncselekmény jogi besorolását kizárólag a LED alkalmazhatósága érdekében.
A GDPR és a LED alkalmazási körének elhatárolása különösen a bűncselekmények és a közigazgatási bűncselekmények közötti határvonal meghúzása kapcsán merül fel bizonyos tagállamokban. Egyes nemzeti jogszabályok olyan adatfeldolgozási célokra is hivatkoznak, amelyek nem tartoznak a LED 1. cikkének hatálya alá, például a közrend vagy a közbiztonság veszélyeztetésének eseteire. Ez a kérdés azért különösen fontos, mert néhány tagállam úgy véli, hogy egyes közigazgatási szervek (például a pénzügyi információs egységek, azaz FIU-k) a LED hatálya alá tartozó feladatokat is elláthatnak. Az általam vizsgált országok gyakorlatában ez nem lelhető fel.

A legtöbb tagállam jogszabályai átfogóan szabályozzák az illetékes hatóságok által a LED céljaira végzett adatfeldolgozást. Ezzel szemben néhány tagállam kimerítő felsorolást nyújtott a nemzeti jogszabályokban a LED szerinti illetékes hatóságokról. Egyes tagállamok kivételt is tettek bizonyos típusú illetékes hatóságok vagy adatok feldolgozásának tekintetében.[468]
A hatály tekintetében a többlettartalom, mint a magyar szabályozás esetén a nemzetbiztonsági és honvédelmi célú adatkezelés véleményem szerint nem jelent kollíziót. A magyar jogalkotó a bűnügyi adatvédelmi irányelv szabályait alkalmazva (átvéve) hozta létre az eltérő cél tekintetében az adatvédelmi szabályokat.

[468] COM (2022) 364 final, 2022, 2.2.1

III.3.2.2. A felügyeleti hatóságok

Az adatvédelmi felügyeleti hatóságok irányítása és jogkörei tekintetében a 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 irányelvben megszabott hatáskörökön túl is biztosított jogokat a hatóságokra, úgymint 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. Jogköreit tekintve, azok a tartományok hatóságain keresztül valósulnak meg.
- Svédország esetében az egyes illetékes hatóságok – köztük a rendőrség – felügyeletét a GDPR tekintetében illetékes felügyeleti hatóság az IMY és a Svéd Biztonsági és Integritásvédelmi Bizottság [469] 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.[470] 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.

Az igazságszolgáltatás függetlensége és a felügyelő hatóságok kapcsolata: a hatóságok nem jogosultak az igazságszolgáltatással összefüggő adatkezeléseket felügyelni. Ez a szabályozás megjelenik 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.[471]

[469] SINT,www.sakint.se

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

[471] Infotv. 38.§ (2b)

- A német szövetségi biztos nem jogosult felügyelni a bírói minőségükben eljáró szövetségi bíróságokat.[472]
- Franciaországban a CNIL nem rendelkezik hatáskörrel a bíróságok által végzett adatkezelési műveletek felügyeletére, ha azok igazságszolgáltatási minőségükben járnak el.[473]
- 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 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- es számú törvény 8. cikk f.) pontja alapján a CNIL haladéktalanul tájékoztatja az ügyészséget, a meghatározott feltételek mellett a büntetőeljárási törvénykönyv (Code de procédure pénale) 40. cikkében foglaltaknak megfelelően, minden olyan bűncselekményről vagy szabálysértésről, amelyről tudomást szerzett, és előterjesztheti észrevételeit a büntetőeljárásban, a büntetőeljárási törvény 41. cikkében meghatározott feltételek szerint[474] 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.[475]

[472] BDSG 9.§ (2)

[473] Informatique Liberté n°78-17 19.cikk V.

[474] Informatique Libertés 8. cikk f)

[475] 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

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 Libertés 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.

III.3.2.3. A jogalapok meghatározása

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

- 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 megismétlése elegendő lenne 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 német adatvédelmi 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 a közös rendelkezések (GDPR és LED) az 5. és 6. cikk által meghatározott általános szempontokat sorolja fel, az utóbbi a különleges adatokkal kapcsolatos tiltó intézkedéseket részletezi.
- 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.

III.3.2.4. Az automatizált döntéshozatal

Minden tagállam tiltja az automatizált döntéshozatalt, amikor különleges kategóriájú személyes adatok kezeléséről van szó kivéve, ha a megfelelő garanciák biztosítottak a Bizottság jelentése szerint. Tilos az olyan profilalkotás is, amely hátrányos megkülönböztetést eredményez.[476] 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.[477]

- Az Infotv. 6. szakaszának ba), és bb) bekezdése rögzíti az érintett emberi 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.

[476] (EU) 2016/680 11 cikk. (2), (3)

[477] COM (2022) 364 final 2.2.6

III.3.2.5. Az érintetti jogok

Az érintettek jogaival kapcsolatban az irányelv szerinti korlátozás lehetőségével valamennyi általam vizsgált 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.[478]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.[479] A német jogalkotó emellett a hozzáférés megtagadását kibővítette: az adatkezelő akkor is korlátozhatja a hozzáférési jogot, ha az adatokat csak jogszabályi követelmények miatt tárolják.[480,481]

A Bizottság jelentése alapján a hozzáféréssel kapcsolatban – LED 14. cikk - csak néhány nemzeti jogszabály fogadott el eltérő megfogalmazást vagy további követelményeket.[482]

- 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.[483] A hozzáférési jog akkor is megtagadható, ha az érintett nem ad elegendő információt ahhoz, hogy az adatkezelő aránytalan erőfeszítés nélkül

[478] BDSG Section 13. (3)

[479] BDSG Section 34.

[480] BDSG Section 57.

[481] 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.

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

[483] Vogiatzoglou, Plixavra. et al. "Assessment of the implementation of the Law Enforcement Directive" p.104.

megtalálja a személyes adatait. Kérdéses, hogy ezek az indokok összhangban vannak-e a LED-del.[484]

Az érintettek kategóriái közötti irányelv által meghatározott különbségtétel mindegyik általam vizsgálat tagállam esetén jelen van.
Az alábbi példák a gyanúsítottra vonatkoznak.

- 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 készülnek 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 készülnek.
- 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 készülnek elkövetni*
- A svéd Brodsdatalag 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 szövegkörnyezetből 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 a C-205/21. ügyben hozott EUB ítélet kapcsolódik az irányelv érintettek kategóriái szerinti különbségtételhez.[485] Az ítélet 83. pontja kimondja, hogy a tagállamoknak biztosítaniuk

[484] 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.

[485] 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

kell, hogy az adatkezelők egyértelműen különbséget tegyenek az érintettek különböző kategóriáinak adatai között, a 84. pont szerint azonban ez nem abszolút jellegű, tehát minden egyes esetben külön kell meghatározni azt.[486]

III.3.2.6. A naplózás

A bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 25. cikke a meghatározza azokat a minimális információtípusokat, amelyeket az automatizált adatkezelési rendszerben a naplóknak 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.

III.3.2.7. A közös kapcsolattartó pont

Az általam vizsgált tagállamok esetében a magyar, a francia és a svéd átültetés tartalmazza ezt az irányelv 22. cikkének megfelelően.

---

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..

[486] 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.

- 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.[487]

Összefoglalva a tagállamok között tapasztalhatók eltérések a bűnügyi irányelv átültetésében a nemzeti jogszabályok vizsgálatakor. A Bizottság jelentése szerint különösen a "bűncselekmény", "közbiztonság" és "illetékes hatóság" fogalmak nemzeti értelmezési különbségei jelentek meg, ami befolyásolhatja a hatály fogalmának értelmezését. Az értelmezési eltérések abból is adódnak, hogy nincs egységes meghatározás ezekre a fogalmakra. A Bizottság jelentései alapján ugyanez látható még 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 (közös) ügyintézési pont létrehozásának következetlen 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

[487] COM (2022) 364 final

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, e szabályozások nemzetközi kontextusban segíthetik a tagállamokat abban, hogy az adatvédelmi elveket hatékonyan integrálják nemzetközi együttműködéseikbe.

IV. A bűncselekményekhez kapcsolódó személyes adatok védelme

IV.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 feltételek 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 fogalom[488] maga is jogszabály által szabályozott rendelkezési jogosultság az érintett személyes adatai felett. Az

[488] 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;”

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 bűnügyi típusú adatkezeléseket is - során jellemzően az előbbi mérleges példával ellentétben az adatkezelők rendelkezési jogosultsága 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.

IV.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.[489] Kőhalmi László szavaival élve, „*rendkívül fontos kérdés az emberi jogok garantálása a büntetőeljárás során, és bár a törvénytisztelő állampolgárok*

[489] Kőhalmi, 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.

*többsége csak ritkán kerül kapcsolatba a joghatósággal "ügyfélként", véleményem szerint jobb, ha sok bűnöst szabadon engednek, mintsem hogy egyetlen ártatlan embert elítéljene*k."

Az Infotv. rendelkezik a bűnüldözési célú adatkezelésekről.[490] 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, azaz kategorizálását az alábbiak szerint:[491]

„(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

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.[492] Ezzel összhangban a 2017. évi XC. törvény (továbbiakban: Büntetőeljárási 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. [493]

[490] Infotv. 3.§ (10) a.)

[491] Infotv. 5.§ (7)

[492] Infotv. 7. §.

[493] Be. 97. § (1)

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”. [494]

A büntetőeljárás kezdeti szakasza a nyomozás, melynek fő célja az elkövető azonosítása és a bűncselekmény körülményeinek tisztázása. Ebben az időszakban az eljáró hatóságok arra törekszenek, hogy megtalálják és megőrizzék azokat a bizonyítékokat, amelyek a további jogi lépések alapját képezik.[495] Ezt követően az azonosított és rendelkezésre álló bizonyítékokat a hatóságok részletesen elemezve készítik elő a büntetőjogi felelősségre vonás folyamatát.[496] Tremmel Flórián hangsúlyozza,[497] 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

---

[494] 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

[495] 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, *Büntetőeljárási jog* (Budapest: Osiris Kiadó, 2000),” p.305.

[496] 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).

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

vagy a kihallgatás, csak azok számára nyitottak, akiket a Be. részvételre kötelez vagy lehetővé teszi számukra.[498]

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. [499]

A rendőrség bűnüldözési tevékenységéhez kapcsolódóan gyűjtött és tárolt személyes adatok felhasználása kizárólag bűnüldözési célokat szolgálhat. Különleges adatok[500], ezen kívül mint 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.[501] 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.[502]

[498]Antal Dániel. (2010) "A nyilvánosság és a büntetőeljárás," *Studia Iuvenum Iurisperitorium* (5), p.219. https://epa.oszk.hu/02500/02567/00005/pdf/EPA02567_Studia_Iuvenum_Iurisperitorum_5_2010_217-271.pdf (hozzáférés ideje: 2022. augusztus 31.).

[499] Infotv., 5. § (4)

[500] 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."

[501] Be. 97. § (1)

[502] Infotv., 5. § (6)

A bűnügyi személyes adatok[503] is a különleges adatok kategóriáinak elve szerint kezelendők.[504] A bűnüldözési adatkezelés folyamatában alapvető fontosságú a tényeken alapuló adatok elkülönítése azoktól az adatoktól, amelyek következtetéseken, véleményeken, elemzéseken vagy becsléseken alapulnak.[505]

A nyomozási szakaszt a bírósági eljárási szakasz követi.[506]

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.[507] A büntetőügyekben eljáró illetékes hatóságok a nyomozó hatóság, az ügyészség, és a bíróság.

A magánszemélyeket illetően a Be. megkülönböztet büntetőeljárásban részt vevő személyeket és segítőket.[508]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

[503] 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.

[504] 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.

[505] Infotv. 5.§ (7)" Bűnüldözési célú adatkezelés esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó (…) egyértelműen megkülönbözteti az érintettel kapcsolatba hozható tényeket és az A jelentős

[506] 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.

[507] Fantoly Zsanett és Budaházi Árpád, *Büntető eljárásjogi ismeretek I.* (Budapest: Dialóg Campus Kiadó, 2019), p. 39. „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."

[508] Fantoly Zsanett és Budaházi Árpád, *Büntető eljárásjogi ismeretek I.* p.40.

eljárás alá vont jogi személy.[509] A segítők és egyéb más szereplők közül a tanút és a szakértőt emelném ki. 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.[510]

IV.2.1. A gyanúsított személyes adatainak kezelése

A gyanúsított fogalmának különös jelentősége van a személyes adatok védelme szempontjából, hiszen a bűnügyi irányelv- amint az korábban tárgyalásra került - 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 elítéltnek.[511] Amennyiben a nyomozó hatóság valakit gyanúsítottként[512] 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.[513]

A gyanúsított személyes adatainak védelmével kapcsolatban kulcsfontosságú, hogy megfelelő intézkedések biztosítsák az adatok illetéktelenek általi hozzáférésének megakadályozását és azt, hogy illetéktelen személy ne értesülhessen arról, hogy az érintettet gyanúsítottként hallgatja meg a nyomozó hatóság.[514]

---

[509] Be. 37.§

[510] Infotv. 7.§

[511] Fantoly Zsanett és Budaházi Árpád, *Büntető eljárásjogi ismeretek I.*, p.50; Be. 38. § (2)

[512] Infotv.7.§. a) „akik tekintetében alapos okkal feltételezhető, hogy bűncselekményt vagy szabálysértést követtek el vagy bűncselekményt készülnek elkövetni," megfelelően a LED.6. cikk.a.) pontjának.

[513] Be.39.§ (3) b) A gyanúsított és vagy terhelt köteles lakcímét, értesítést címét , tartózkodási helyét, elérhetőségét, telefonszámát, e-mail címét és annak megváltozását az eljáró hatóságnak bejelenteni.

[514] Be. 113. § (2) bekezdés.

A Be. előírja a papíralapú idézések és értesítések zárt borítékban történő kézbesítését.[515] Amikor a gyanúsítotti kihallgatására kerül sor, a nyomozásért felelős személy felhívja a gyanúsított figyelmét, hogy azonosságának egyértelmű megállapítása érdekében köteles nyilatkozni nevéről, születési nevéről, születési helyéről és idejéről, anyja nevéről, állampolgárságáról, személyazonosító okmányainak adatairól, lak- és értesítési címéről, tartózkodási helyéről, valamint telefonos és egyéb elérhetőségeiről.[516]

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.[517]

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.[518]

A gyanúsított személyazonosságának rögzítésekor nem szükséges az összes, a Büntetőeljárási 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.[519] Ez valóban megfelelne az adatminimalizálás elvének[520], de kérdés, hogy milyen adat elég az azonosításhoz, ugyanakkor, ha az adat a természetes személyes adattal kapcsolatba hozható, (vagy az helyreállítható)[521] márpedig az azonosítás ezt a célt szolgálja, ez az érintett szempontjából mekkora jelentőséggel bír. Az azonosíthatóság kérdésével a Kúria is foglakozott, melyről még a későbbiekben lesz szó. Miután a személyes adatok rögzítése megtörtént, a gyanúsítottat tájékoztatják az eljárás során fennálló jogairól és

[515] 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.

[516] Be. 184. § (2)

[517] Btk. 342. § (1) c) pont.

[518]Be. 637.§ (1), c), „Perújításnak van helye (…)a terhelt az ügydöntő határozatban nem a valódi személyazonosságával szerepel és ez a határozat kijavításával nem orvosolható”

[519] Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.56

[520] GDPR 5.cikk.c)

[521] Infotv. 4. § (3). „A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható”

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.[522]

Az eljárási cselekményekkel kapcsolatos tájékoztatásnak ki kell terjednie a személyes adatok zártan kezelésének lehetőségére, magára a tájékoztatási jogra, valamint arra, hogy hogy az eljárási cselekmény során megismert adatok és az eljárási cselekményen tapasztaltak személyes adatnak, adott esetben védett adatnak minősülnek, és annak kezelése csak jogszabályban meghatározottak szerint lehetséges, valamint ki kell terjedjen a tájékoztatás az ügyiratok megismerésére való jogosultságára is.[523,524] Az eljárás dokumentumait a terhelt és annak védője a terhelt gyanúsítotti kihallgatása után, a sértett a rá vonatkozó bűncselekmény kapcsán, és az egyéb érdekelt személyek, valamint a vagyoni érdekeltek az őket érintő ügyekben megismerhetik, ha ezt külön kérelemmel kezdeményezik.[525] Ez a jog a dokumentumok megismerésére az eljárás összes ügyiratára vonatkozik. Ez magában foglal minden, a bíróság, az ügyészség és a nyomozó hatóság által összegyűjtött, a büntetőeljárás résztvevői által benyújtott vagy hozzácsatolt iratot, továbbá minden egyéb bizonyítási eszközt is.[526]

Ha az eljárás során jelentős mennyiségű dokumentumot gyűjtöttek össze, amelyek átvizsgálása még nem zárult le, a bíróság, az ügyészség és a nyomozó hatóság korlátozhatja a dokumentumokhoz való hozzáférés jogát, vagy bármely hozzáférési módot az adott dokumentumok esetében, amíg az átvizsgálás be nem fejeződik. Ez a korlátozás, ha a törvény másként nem rendelkezik, legfeljebb a dokumentumok beszerzését követő három hónapig tarthat, erről a hatóság határozatot hoz.[527] Ugyancsak határozatot kell hoznia a bíróságnak, ha más okból korlátozza a hozzáférési módot, mint például ha a bármely dokumentumhoz való

[522] 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”

[523] 100/2018. (VI. 8.) Korm. rendelet, 42.§.(3). h), (i)

[524] Be.39.§. (1). j)

[525] Be.100.§. (1). a)-c)

[526] Be.100.§. (2).

[527] Be.100.§. (6b).

hozzáférési mód törvénysértő lenne, vagy az adott dokumentum jellegéből adódóan lehetetlen,[528] ha a védett adatok védelme megköveteli azt.[529]

A nyomozás során történő eljárási cselekményekkel kapcsolatosan más hatóságok közreműködése is szükségessé válhat, az érintetti jogok nem változnak.[530]

A nyomozás során készült jegyzőkönyv tartalmazza a Be. előírásait, és ezenkívül a 100/2018. (VI. 8.) Korm. rendelet alapján[531] 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.[532]

IV.2.2. A tanú személyes adatainak kezelése

Amennyiben a nyomozó hatóság valakit tanúi minőségben kíván meghallgatni, tanúként történő idézésre kerül sor.[533] A tanú a Be. szerinti egyéb érdekelt kategóriába tartozik. 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.[534] 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.[535]

---

[528] Be.100.§. (6c).

[529] Be.100.§. (6d).

[530] 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.

[531] 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.

[532] 100/2018. (VI. 8.) Korm. rendelet, 5.§ (2)

[533] 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.

[534] Be.113. § (1)

[535] Be. 113. § (2)

A tanúk meghallgatása sorrendben, egymás után történik az eljárás során. A meghallgatás elején a tanú személyazonosságának ellenőrzésére kerül sor, amely személyi igazolvány, útlevél, jogosítvány vagy bármely más, a személyazonosság igazolására alkalmas okirat alapján történhet.[536] A tanú részére kizárólag a vallomását tartalmazó jegyzőkönyvről, jegyzőkönyv-részletről adható ki iratmásolat, így értelemszerűen ők a teljes iratanyag megismerésére és másolatára nem jogosultak.[537]

A büntetőeljárás során illetékes hatóság vagy bíróság bármikor, saját kezdeményezésre vagy a tanú, illetve képviseletében 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 e 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 adatai szerepelnek az ügy irataiban, például a jegyzőkönyvekben, és azok, akik jogosultak az iratok megtekintésére, hozzáférhetnek ezekhez az adatokhoz.[538] 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.[539] A különösen védett tanú esetében a védő sem ismeri a tanú semmilyen adatát vagy személyét.[540]

---

[536] Be. 85-88. §

[537] Az iratokról történő másolatadásra vonatkozó rendelkezéseket kell alkalmazni a kép- vagy hangfelvételről, a képet és hangot egyidejűleg tartalmazó felvételről készített másolat kiadására is.

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

[539] Be. 25.§

[540] 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.

A tanú személyes adatainak zártan kezelése az információs önrendelkezéshez való joggal összhangban áll.[541]
A Be. ezen rendelkezései biztosítják, hogy a büntetőeljárás során a tanúk személyes adatai megfelelő védelemben részesüljenek.

IV.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.[542]
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.[543] A vádirat tartalmazza a vádlott nevét, születési helyét és idejét, lak- 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.[544] 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 vádakat, a vádak tényállását és a cselekmények jogi megítélését.[545] Ez megfelel az Infotv. rendelkezésnek, miszerint az adatokat olyan módon kell kezelni, hogy „*biztosítva legyen a személyes adatok*

[541] ABH. 2010, 562. „Nincs alkotmányos alap vagy cél, ami lehetővé tenné a nyomozó hatóság, az ügyész vagy a bíróság számára, hogy a tanú fenyegetettségének objektív alapjait vizsgálva és a kérelem teljesíthetőségét mérlegelve megtagadják ezt a kérelmet."

[542] Be. 391. § (1) bekezdés.

[543] Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.58.

[544] Be. 497. §.

[545] Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.58.

megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével,(…) szembeni védelmet is ideértve."[546]

A jogszabályok értelmében a jogalkotó előírja,[547] hogy azokat a papíralapú ügyiratokat, melyek átvételéhez jogi következmények kapcsolódnak, vagy amelyek átvételének igazolása szükséges, hivatalos iratként kell postázni[548] 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.[549]

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.[550]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.[551], [552]

A tárgyalási jegyzék adatvédelmi szempontból kiemelt jelentőséggel bír a bírósági eljárásokban.

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*

[546] (EU) 2016/680 4. cikk f) és Infotv. 4.§.(4a)

[547] 12/2018. (VI. 12.) IM rendelet

[548] 12/2018. (VI. 12.) IM rendelet 30. §

[549] 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."

[550] Be. 499. § (2) bekezdés

[551] A bírósági ügyvitel szabályairól szóló 14/2002. (VIII. 1.) IM rendelet 19. § (2), (3) bekezdés.

[552] Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p.59.

a személyes adatok védelme áll összeütközésben egymással."[553] 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.[554]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.[555]
Véleményem szerint a beépített adatvédelem elvét figyelembe véve, az adatkezelőnek- jelen esetben a bíróságnak - 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.[556]

[553] Németh, Kata. (2019) "A büntetőeljárás nyilvánosságának jogszabályi hátterében 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.

[554] 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."

[555] Be. 499. § (1) bekezdés.

[556] Németh Kata: A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." p.62.

IV.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.[557] 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,*[558] *a büntetőeljárási jogairól és kötelességeiről a bíróságtól, az ügyészségtől és a nyomozó hatóságtól felvilágosítást kapjon.*[559]A sértett jogosult arra is, hogy kérelmére tájékoztassák az őt érintő bűncselekménnyel összefüggésben.[560] Az érintettek jogait megillető jogosultságok körén belül a hozzáférési jog alapján a Be. ezen rendelkezése 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 részét képezik. (bíróság, ügyészség vagy nyomozó hatóság részére)[561]

A sértettnek a nyomozás és a bírósági eljárás során járó jelenléti és irat megtekintési 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 irat betekintési 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 tájékozódási jog[562] adatkezelési célból szükséges korlátozása.[563]

A sértett jogosult az eljárás során beadványok benyújtására, észrevételek megfogalmazására, kérdések feltevésére a vádlottnak, szakértőknek, tanúknak, továbbá kérdésfeltevés

[557] Be.50. §

[558] Be.51. §, (1) d)

[559] Be.51. § (2) e)

[560] Be. 51. § (5) a) – f)

[561] Be. 51. § (6) (b)

[562] Infotv.14§.a) előzetes tájékozódáshoz való jog

[563] 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."

kezdeményezésére, valamint a bizonyítási eljárás lezárulta után jogosult - az ügyész perbeszédét követően,- felszólalni.
A sértettet a büntetőeljárási jogairól és kötelezettségeiről tájékoztatni kell, nem csak kérésre.
A vádemelés tényéről az ügyészségnek, 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 képviselete 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.[564] 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, ügyészséggel vagy nyomozó hatósággal közölni.[565]
Sértetti jogutódlás esetén ugyanezen kötelezettségei és jogai vannak a jogutódnak.[566]
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.[567]

IV.3. A szakértő a büntetőeljárásban és a személyes adatok védelme

A szakértő a büntetőeljárásban az egyéb érdekeltek 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 jogosult a szakértő azokat az adatokat megismerni, melyek a feladatának teljesítéséhez szükségesek, az eljárás ügyiratait is – kivéve, amit a törvény kizár, - megismerheti.[568]

[564] Be. 51. §, (1) d), e), (5), 93. §, (b)

[565] Be.51§. (6). b)

[566] Be. 52. §

[567] Be. 65. §, 69. §, 70/B. §,

[568] Be.192.§. a)

A szakértőt illetően a szóbeli előterjesztés előtt az eljáró bíróságnak meg kell állapítani a szakértő személyazonosságát.[569] A bírósági eljárásokban a szakértői meghallgatás során a tanúkihallgatás szabályait kell megfelelően alkalmazni.[570] 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 felolvastatni.[571]

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. taxatíve felsorolja az erre vonatkozó lehetséges feltételeket[572], köztük az erkölcsi okból történő elrendelést is. Mándi véleményével egyetértve, azonban egyedi esetekben a zárt tárgyalás „erkölcsi okból" történő elrendelése megoldást kínálhat.[573] „*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*"[574]

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.*" [575] 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.*"[576] Amint az adat kikerül a bírósági kontextusból, ismét személyes vagy különleges adatnak minősül, ami azt jelenti, hogy eredeti keletkezése szerinti módon kell megóvni és védeni azt.

---

[569] Be. 196.§ (2)

[570] Be. 529. § (1)

[571] Be. 530. § (1)

[572] Be. 436.§ (4)

[573] Mándi Veronika, "A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata," p. 59

[574] 58/1995. (IX. 15.) AB határozat.

[575] Németh, Kata. „A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." p.70.

[576] 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.

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 a tekintetben, hogy többszörös „feladatot" jelentene az eljáró szervek számára, hiszen még büntetés-végrehajtási fázisban is kerülhet sor bírósági adatkezelésre, valamint ebben az esetben az érintett személyes adatai többféle minősítésben részesülnének. Ugyanazon adatot az eljárás különböző fázisaiban más néven szerepeltetni még adatvédelmi okból sem szerencsés, a tévedés, az esetleges adatvesztés lehetősége miatt sem.
Az adatok zártan történő kezelése megoldást jelenthetne, azonban a Be. szerinti személyes adatok zártan történő kezelése [577]esetén sem az egészségügyi adatok, sem más különleges adatok nem kerülnek külön felsorolásra. Azaz az illetékes hatóságok az előbbi adatok vonatkozásában nem rendelhetik el a zártan kezelést.

IV.4. Az adatkezelés jogalapja és az adatvédelem a büntetőeljárási 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.[578] 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.[579]
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.

[577] Be. 99.§. (1)

[578] Be. 97.(1). §

[579] 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.[580]

A zárt adatkezeléssel kapcsolatosan meg kell említenünk az iratokhoz való hozzáférések jogát az e- ügyintézés területén. Róth, a digitális ügyintézés ismertetése során 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.[581]

Amennyiben az érintett adatkörre vonatkozó jogszabály másként nem rendelkeznek, 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.[582]

[580] Be. 98. § (1). – (2)

[581] Róth, Erika. (2021) "A digitalizáció és a terhelti jogok érvényesülése a büntetőeljárásban." *Miskolci Jogi Szemle* 16, no. 1, különszám pp.270-278.

[582] Be. 98.§ (3), Infotv. 4.§,(2.)

A büntetőeljárás során kezelt személyes adatok és védett adatok törlése kizárólag a Be. ("*e törvény*") előírásainak megfelelően történhet az eljárás befejezéséig.
A büntetőeljárásban megismert személyes adatok – amennyiben azok egyedi azonosításra alkalmatlanná válnak – statisztikai célokra felhasználhatók.[583]

IV.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.[584]
A kérelmet a sértett, a vagyoni jogokban érintett személy, valamint az egyéb érintett vagy az őket segítő személyek nyújthatják be[585] valamint a sértettek védelmében a bíróság, az ügyészség és a nyomozó hatóság kezdeményezés nélkül is dönthet a személyes adatok zárt kezeléséről.[586]
A bíróság, az ügyészség és a nyomozó hatóság az érintettek hozzájárulásával feloldhatja bizonyos személyes adatok ilyen módon történő kezelését.[587]
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.[588]
A zártan kezelt iratokból a zárt adatkezeléstől érintetlen részeket az általános szabályoknak megfelelően hozzáférhetővé kell tenni, például olyan kivonat készítésével, amely a zártan

[583] Be. 98. § (3). – (4) - (5)
[584] Be. 99.§ (1)
[585] Be. 99.§ (2)
[586] Be. 99.§ (3)
[587] Be. 99.§ (4)
[588] 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 büntetőeljárási feladatok 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.[589]

A Be. az adatvédelmi szabályozástól függetlenül is szabályozza az eljárás ügyiratainak megismerését és zártan kezelését.[590] 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 ügyiratra, 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 irat betekintési 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 ügyiratokra vonatkozó külön rendelkezések.[591]

---

[589] Be. 99.§ (8)- (10)

[590] A Büntetőeljárási 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 adatából, valamint, hogy az ügyiratok megismerése ne vezessen a zártan kezelt dokumentumok felfedéséhez.

[591] 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.[592]

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.[593]

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.[594]

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.[595]

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.

[592] Be. 100 §. (1) – (9)

[593] Be. 101 §. (1)

[594] Be. 101 §. (2)

[595] Be. 101 §. (3)

ügyészség vagy a nyomozó hatóság tekintheti meg. Azt is biztosítaniuk kell, hogy hogy a zártan kezelt ügyirat, illetve annak tartalma az eljárás egyéb ügyirataiból és adataiból ne váljon megismerhetővé.[596]

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.[597]

A zártan történő kezeléssel kapcsolatban azonban nem csak a sértett, a vagyoni érdekelt, és az egyéb érdekelt adatiról van szó, hanem ezek segítőit 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 ezt módosítandó, a NAIH beadvánnyal fordult az Igazságügyi Minisztériumhoz, tekintettel arra, hogy a jogi képviselő számára kötelező az elektronikus ügyintézés,[598] melynek kapcsán személyes adatai megismerhetők.

2018. január 1-től a büntetőeljárásokban részt vevő állami szervek, mint a nyomozó hatóságok, az ügyészség, a bíróságok és a büntetés-végrehajtási szervek számára kötelezővé vált az elektronikus kapcsolattartás az ekkor vagy azt követően kezdődő eljárásokban.[599] Róth megjegyzi, hogy a digitalizáció hatása nem korlátozódik csupán az elektronikus kapcsolattartásra és a szélesebb körű e-ügyintézésre, hanem már korábban is jelentős mértékben átszőtte 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.[600]Az e-Papír szolgáltatással kitöltött űrlap és csatolmányai részei a büntetőeljárás

[596] Be. 102. § (1)-(3)

[597] 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.

[598] 2015.évi CCXXII. törvény 9.§.(1)

[599] 2015. évi CCXXII. törvény

[600] Róth, Erika. "A digitalizáció hatása a büntetőeljárásra.". p.166

valamennyi folyamatának, és az űrlap az okiratok sorsát osztja, attól függetlenül nem kezelhető.[601] A NAIH 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 üggyel nem összefüggő személyes adatai - az irat betekintési jog során - ne legyenek megismerhetők.[602] Ezzel kapcsolatban osztom a NAIH álláspontját.

Összefoglalva, a Be. XVI. fejezete az eljárás ügyiratainak megismerése és zárt kezelésével foglalkozik. Az eljárás ügyirataihoz a terhelt és annak jogi képviselője, a terhelt gyanúsítotti 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.[603]
A megismerés joga nem érvényes a zártan kezelt eljárás dokumentumaira, valamint nem befolyásolja az információk zártan történő kezelésének kötelezettségét.[604]

IV.6. A tárgyalás nyilvánosságának elve és a természetes személyek adatainak védelme

A tárgyalás nyilvánosságának elve a tisztességes eljárás egyik alapvető követelménye, amely a bírósági eljárások átláthatóságát és a jogállamiság érvényesülését szolgálja. Ugyanakkor ez az elv ütközhet a természetes személyek adatainak védelmével, különösen akkor, ha az érintettek magánélete vagy más érzékeny adatai is nyilvánosságra kerülhetnek a bírósági eljárás során. A nemzetközi és európai jogi normák egyaránt elismerik a nyilvánosság követelményét, ugyanakkor lehetőséget biztosítanak arra, hogy meghatározott esetekben – például nemzetbiztonsági érdekek, közrend védelme vagy az érintettek személyiségi jogai miatt – a nyilvánosságot korlátozzák.

[601]100/2018. (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.

[602] NAIH/2020/4229/2 ügyirat szám

[603] Be.610.§ (1)-(4)

[604] Be. 610.§ (5)

„A nyilvánosság elve – mint a Be.-ben egyedüliként 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.”[605]

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 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 alapelvként kezelik, hogy a büntetőügyekben hozott ítéleteket nyilvánosan kell kihirdetni, ám a PPJE lehetővé teszi kivételek alkalmazását is, különösen, amikor a fiatalkorúak érdekei mást igényelnek.[606]

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.[607]

Az igazságos, független és pártatlan eljáráshoz való jog mindenkit megillető, alkotmányos szinten biztosított alapvető jog. Az Alaptörvény a XXVIII. cikkében rögzíti ezt az

---

[605] Fantoly, Zsanett és Budaházi, Árpád. „Büntető eljárásjogi ismeretek” p.37.

[606] 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.

[607] 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

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,[608] illetőleg a bírósági ügyvitel szabályairól szóló rendelet[609], valamint a sajtóról szóló törvény[610,611], is rendelkezik róla.

Cséka a nyilvánosságot általános elvként azonosítja a büntetőeljárásban, 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. [612]

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.[613]

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.[614]

Petrik Ferenc szerint a tisztességes eljáráshoz való jog (fair trial) elengedhetetlen részeleme a

---

[608] 2011. évi CLXI. törvény a bíróságok szervezetéről és igazgatásáról

[609] 14/2002. (VIII.1.) IM rendelet – a bírósági ügyvitel szabályairól

[610] 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."

[611] 2010. évi CLXXXV. törvény a médiaszolgáltatókról és a tömegkommunikációról

[612] Cséka Ervin, Fantoly Zsanett, Hegedűs István, Kovács Judit, és Maráz Vilmosné.(2007.) *A büntetőeljárási jog alapvonalai. II.* Szeged: Bába Kiadó, pp. 75-77.

[613] Erdei Árpád. (2011.) *Tanok és tévtanok a büntető eljárásjog tudományában*. Budapest: ELTE Eötvös Kiadó.

[614] 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.

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.[615]

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.[616]

Márki véleménye szerint a büntetőeljárás alapvető szabályait, a büntetőeljárási 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 .[617]

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.[618]

Németh szerint a társadalmi nyilvánosság és a nyilvánosság tájékoztatáshoz való joga bár összefügg, nem tekinthető azonos fogalomnak.[619] A bírósági tárgyalások nyilvánosságát a Be. rendeli el[620], hangsúlyozva, hogy ezek a tárgyalások nyitottak mindenki számára, nem csak az

---

[615] 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.

[616] 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

[617] Márki, Dávid. "Az igazságszolgáltatás nyilvánosságának alkotmányjogi vizsgálata: Alapjogi kollíziók a büntetőeljárás, a sajtó és a politika keresztttüzében." p.146

[618] 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

[619] Németh, Kata, A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre.” p.58

[620] 436. § (1) A bíróság tárgyalása nyilvános.

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 egymást. Ez a megkülönböztetés két fontos dimenzió – a társadalmi nyilvánosság és a tárgyalótermi nyilvánosság – közötti határvonalat jelöli ki.[621]

A Büntetőeljárási törvény (Be.) részletesen meghatározza, hogy a büntetőeljárás különböző szakaszaiban mely hatóságok felelősek a nyilvánosság tájékoztatásáért. A nyomozás lezárásáig a nyomozó hatóság erre kijelölt tagja[622] 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.[623] Az egyes hatóságok belső szabályzatai döntik el, hogy ki jogosult az adott információ szolgáltatási feladatok ellátására.[624]

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 segítségével[625] – kívánják a nyilvánosságot tájékoztatni. A törvény mindenki számára lehetővé teszi, hogy bírósági tárgyalásokról a médiarendszeren keresztül tájékoztatást kapjon. Kép-, hang-, vagy kép- és hangfelvételek

---

[621] Németh, Kata, A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." p.59

[622] 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.

[623] 2011. évi CLXII. törvény a bírák jogállásáról és javadalmazásáról 22. 43.§-44.§

[624] Be. 107. § (2)

[625] 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.

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 érintettek hozzájárulásával készülhetnek. A hallgatóság létszámának korlátozása semmilyen formában nem korlátozhatja a nyilvánosság tájékoztatáshoz való jogát.[626]

Az eljáró hatóság az információszolgáltatást, 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.[627] 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.[628]

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.[629]

Háger szerint a tárgyalás nyilvánosságának korlátozására vonatkozó okok két fő kategóriába sorolhatók: az egyik a rendfenntartás és a bizonyítási folyamat zavartalan lefolytatásának szükségessége, a hallgatóság életkorával kapcsolatos szabályozás, a másik erkölcsi okból, titokvédelmi-vagy tanúvédelmi érdek miatt kerül a nyilvánosság korlátozásra.[630] Az 14 év

---

[626] Be. 108. § (1) – (3)

[627] „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

[628] Be. 109. § (1)

[629] Be. 110. § (1) – (2)

[630] Háger Tamás. "A nyilvánosság, mint a tisztességes eljárás egyik garanciája a büntetőperben." In: Pro Futuro 2014/1, p. 52

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.

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.[631] 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. §).”*[632]

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 „média rendszer” részét értelmezhetjük, mert külön szabályozás nem vonatkozik rá.[633] 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.[634] 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

---

[631] 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 fiatalkorú érdekében (még a terhelt is kizárható). Lásd: Herke, Csongor *„Büntető eljárás”,* p.100.

[632] Ibid., 101.o

[633] Németh, Kata, A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre.” pp. 60-62

[634] Faisal, Kamrul. "Journalism vs. Data Privacy: The GDPR Dilemma in Reporting Crimes." *Internet Policy Review* 11, no. 3 (2024).

megfontolnia a hallgatóság létszámának korlátozását, a zárt tárgyalás elrendelését, amelyet erkölcsi okokból, a különleges bánásmódot igénylő személyek védelmében, valamint minősített és egyéb védett adatok védelmében lehet alkalmazni.[635] 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 tevékenyégük kapcsán is adatkezelőknek minősülnek.[636], [637]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, Büntetőeljárási törvényben, a bíróságok szervezetéről és igazgatásáról szóló törvényben, és a korábban már felsorolt egyéb vonatkozó ágazati jogszabályoknak.

---

[635] 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 ítéletrendelkező 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 elhangzottakról tájékoztatást nem adhatnak.(…)"

[636]Infotv. 25.L§. a) Annak ellenére, hogy állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot látnak el ebben a minőségükben, nem kötelezettek adatvédelmi tisztviselő kijelölésére.

[637] 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.

Adatvédelmi aggályok a tárgyalási jegyzék kifüggesztése, a tárgyalás nyilvánossága vagy zárt tárgyalás elrendelése, valamint az ítélethirdetés nyilvánossága, és a bírósági tárgyalásokról szóló tudósítás kapcsán merülnek fel.

Az aggályokra adott válaszokat a bűnügyi adatkezelést szabályozó keretrendszer, azaz a bűnügyi irányelv nyomán, az Infotv. által előírt rendelkezések tartalmazzák.

Egyrészt az adatkezelésnek meg kell felelnie a jogszerűség, a törvényesség[638] és a célhoz kötöttség alapelveinek.[639] 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.[640]

Másrész a bűnügyi 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 védeljárás során, az érintetti jogok és korlátozások tekintetében rendelkezhet.[641,642]

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.

---

[638] 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.

[639] 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.

[640] 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.

[641] Infotv. 7.§ (1) a) – d)

[642] Infotv. 7.§ (4)

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: - „*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.*

Azaz a 436. szakasz (4.) bekezdése a javasolt módosítással egyben a következő. „*(4) 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, b) különleges bánásmódot igénylő személy védelme érdekében, illetve c) 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** *„zárt tárgyalást rendelhet el."*

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.[643] Az

[643] NAIH/2020/294/4 ügyszámú állásfoglalása.

állásfoglalás hivatkozik BDT2019. 4060. számon közzétett bírósági határozatra[644], 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 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 állásfoglalása[645] irányadó. A bírósági eljárások során kialakított ítéletek nyilvános kihirdetése egyrészről a társadalmi normák érvényesítését szolgálja az elkövetőkkel szemben, másrészről 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. 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 előélethez fűződő hátrányok idővel történő eltörlésére. Ez a gyakorlat jelentős hatással van az érintettek magánéletére és társadalmi reintegrációjukra. Ezért felmerül a kérdés,

[644] Megjelent: Bírósági Döntések Tára 2019/9/100, Szegedi Ítélőtábla 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."

[645] 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 változatát Idézi, az elvi szempontok helytállóak.

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, 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.[646] Képi-és hangeszközök 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.[647]

IV.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 büntetőeljárási 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.[648] A kifogást az alapügyben eljáró bíróságnál írásban lehet előterjeszteni.[649] 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.[650] A személyes adatok bírósági kezelésével kapcsolatos kifogásokat a bíróság az alapügy

[646] 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 közerkölcsöt, 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."

[647] Kőhalmi László. "Nyilvánosság és büntetőeljárás." Pécs, 2022.p.41

[648] Infotv.71./A.§ (1) (2)

[649] Infotv. 71./A.§ (3)

[650] Infotv. 71./A.§ (4)

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.[651]

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 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.[652] 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.[653]

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

[651] Infotv.71./B.§ (1) - (6)

[652] Infotv.71./C.§ (1) - (3)

[653] Infotv. 64. § (5)

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 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. meghatározott[654] 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.

IV.8. A büntetés-végrehajtás adatvédelmi vonatkozásai

IV.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 büntetőeljárási kényszerintézkedések,

[654] 2017. évi XC. törvény 143. § (3) bekezdését, valamint 144. § (3) bekezdését és (8) bekezdés *a)* pontja alapján.

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 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. [655]

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, logisztikai menedzselésük, valamint az adatkezelésük[656] 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, a GDPR és az Infotv. értelmében. Az intézmények és intézetek is természetesen ellátják az adatkezelési tevékenységet.[657] A büntetés-végrehajtási rendszer egy integrált modellt képvisel, mely az

[655] Kondás Katalin. (2018.) "Adatok védelme a börtönökben." *Hadmérnök* XIII. évfolyam, 1. szám (március): 270.

[656] 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.

[657] 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)

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.[658] 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 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 zárakat 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,

[658]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.

egyúttal 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.[659]
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 elektronikus megfigyelési eszköz által rögzített felvételt és az abban szereplő személyes adatot – a Bv. tv. 150. § (7) bekezdésében meghatározott korlátok között –kezeli[660]*.”*
Véleményem szerint a büntetés-végrehajtás adatkezelési gyakorlata különösen érzékeny terület, amely egyszerre igényli a fogvatartottak jogainak védelmét és a biztonsági szempontok szigorú érvényesítését. Az adatvédelem és a büntetés-végrehajtási intézmények működésének egyensúlya kritikus jelentőségű, különös tekintettel az az új technológiákra, úgy, mint a biometrikus azonosítás és az intelligens megfigyelési rendszerek bevezetése.[661]

IV.8.2. Jogszabályi háttér

A büntetés-végrehajtási jogviszony[662] 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 bűnügyi adatvédelmi irányelv szerint az Infotv. biztosítja.

[659]Kondás 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
[660] Bvsztv 27/F.§
[661] Shutova, Albina A. "Patients' Personal Data, Including Biometrics, as Objects of Criminal Law Protection." *The International Journal of Law in Changing World* 1, no. 2 (2022): 45–58.
[662] Bvtv.7. §

Általánosságban elmondható, hogy büntetés-végrehajtás során az egyes büntetés-végrehajtási tevékenységek, mint adatkezelési célok, a 2013. évi CCXL. törvény[663] (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.) [664] adatvédelmi rendelkezéseket tartalmaz a fogvatartottak nyilvántartására vonatkozóan a törvény V. fejezetében.

Ide sorolható továbbá, a 2009. évi XLVII. törvény[665] (továbbiakban Bnytv.), amely a bűnügyi nyilvántartási rendszerről szól, amelynek IX. fejezete tartalmazza a vonatkozó adatvédelmi szabályokat. A Bnytv. szerint bűnügyi nyilvántartások a bűntettesek 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 bűnügyi nyilvántartások kezelésének feladatát a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság végzi.

A Bnytv. a bűnügyi nyilvántartások mellett külön rendelkezik a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, ami a daktiloszkópiai nyilvántartást és a DNS-profilnyilvántartást 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. [666]

---

[663] 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról. A törvény az adatkezelés jogalapját szolgáltatja.

[664] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

[665] 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról

[666] 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 büntetésvégrehajtáshoz, de megemlítem a rendőrség eModus rendszerét, melynek jelentős szerepe van a nyomozati munkában.

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.[667]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.

Különleges egészségügyi adatok kezelésével kapcsolatos esetekben az 1997. évi XLVII. törvény (továbbiakban Eüak. tv) [668], valamint az 1997. évi CLIV. törvény (továbbiakban Eü.tv) [669] az irányadók.

IV.8.3. Adatkezelési elvek a büntetés-végrehajtás során

IV.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 Büntetőeljárási 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 hatálya[670] a következő területeket öleli fel:

---

[667] 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.

[668] 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

[669] 1997. évi CLIV. törvény az egészségügyről. Különösen a 24. §, 137. § szakaszok.

[670] 2013. évi CCXL, 2. §

- 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 büntetés-végrehajtás során.[671] Ennek alapján az állam felelős a büntetések, intézkedések és szabálysértési elzárást érintő végrehajtásért, beleértve az utógondozást is. Az elítéltekre és más jogcímen fogvatartottakra a törvények és határozatok által meghatározott korlátozások alkalmazandók. Ezen kívül 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.[672] 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 eljárt bíróság területileg illetékes büntetés-végrehajtási bírójának. Ez magában foglalja a kézbesítési cím bejelentését és annak változását,

[671] 2013. évi CCXL, 5. §

[672] 2013. évi CCXL, 8.§

valamint a lakcímtől eltérő tartózkodási hely és annak változása esetén történő bejelentést is. E rendelkező rész kifejezetten érinti az elítélt személyes adatait.

Az elítéltnek jogérvényesítése lehetősége van, [673] 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.[674]

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 információkéréssel 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 nélkülözhetetlenül szükséges adatokra korlátozódhat, az adatkezelés céljának és a kért adatok körének pontos megjelölésével. Ezen kívül 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 eljárt 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 sújthatják[675] valamint a nemi élet szabadságát és nemi

[673] 2013. évi CCXL, 10.-11.§

[674] 2013. évi CCXL, 12.§. A törvény tételesen felsorolja a tájékoztatás tartalmi elemeit.

[675] Btk. XV. fejezet

erkölcsöt sértő bűncselekményekre.[676,677]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.[678]

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.[679] 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 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.[680]

Az elektronikus kapcsolattartás szabályai kapcsán a Be. szabályai az irányadók.[681]

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

---

[676] Btk. XIX. fejezet

[677] 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

[678] 2013. évi CCXL, 13.§ (5)

[679] 2013. évi CCXL, 26.§

[680] 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.

[681] 2013. évi CCXL. 26/A. §

zártan kell kezelni, értesítések és hivatalos iratok kézbesítése csak a védelmet ellátó szerven 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 szerven keresztül zajlik.[682]

IV.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 elzárás végrehajtásához kapcsolódóan kezelt adatok szigorú szabályozása, biztosítva ezzel a személyes adatok védelmét és a törvényesség elvét. [683]

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 szerv számára lehetővé váljon a büntetések, intézkedések, bizonyos kényszerintézkedések és a szabálysértések elzárásának végrehajtásához szükséges adatok hatékony kezelése.[684] 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 jogerőre emelkedésének napja, valamint a kiszabott büntetések vagy intézkedések részletei.[685]
2. Személyes adatok: az elítéltek és egyéb jogcímen fogvatartottak személyazonosító adatai, állampolgársága, lakcíme, elektronikus kapcsolattartási adatai és egyéb releváns személyes információk.[686]

[682] 2013. évi CCXL. 26/B. §

[683] 2013. évi CCXL IV. fejezet 76 §

[684] 2013. évi CCXL 76, § (1)

[685] 2013. évi CCXL 76.§ (2) a.

[686] 2013. évi CCXL 76. § (2) b.

3. Speciális adatkörök: A családi állapot, iskolai végzettség, szakképzettség, valamint a kényszergyógykezeltekkel kapcsolatos adatok kezelése.[687] Ezen túlmenően a törvény előírja a törvényes képviselők, védők, és az elítéltek családtagjaik személyes adatainak kezelését is. amennyiben az szükséges.[688]
4. Az adatkezelés korlátozásai: A törvény meghatároz bizonyos korlátozásokat és kivételeket, melyek meghatározzák, hogy mely adatok nem tekinthetőek meg, illetve mely esetekben korlátozódik az adatokhoz való hozzáférés.[689]
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.[690]
9. Elektronikus megfigyelés: A törvény részletezi az elektronikus megfigyelési eszközök által rögzített adatok kezelésére vonatkozó szabályokat, beleértve az ilyen adatok felhasználását biztonsági kockázatelemzés során.[691]
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.[692]
11. Sajátos 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.[693]

[687] 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.

[688] 2013. évi CCXL 76.§ (2) c).- (u-f).

[689] 2013. évi CCXL 78.§ (1)-(4)

[690] 2013. évi CCXL 79.§

[691] 2013. évi CCXL 76.§ (3) a.)

[692] 2013. évi CCXL 76.§ 3.a

[693] 2013. évi CCXL 77.§ - 78. §

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.[694]
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.[695]

A büntetés-végrehajtás során keletkezett irat megismerésének joga[696] - megfeleltethető az Infotv. szerinti hozzáférés jogának - alapvető a személyes adatok védelme szempontjából.

A büntetőeljárás során keletkező okmányokhoz bizonyos feltételek mellett hozzáférhetnek az érintettek, védőik, valamint egyéb jogosultak. Ez magában foglalja az iratokba 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.[697]

Összegezve 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.[698]

A büntetés-végrehajtás 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. [699]

A Bv.tv.150. szakasza az elektronikus megfigyelési eszközök használatára vonatkozóan az adatkezelés céljait részletezi, amelyek elsősorban a végrehajtás rendjének és a fogvatartás

[694] 2013. évi CCXL 79. §

[695] 2013. évi CCXL 81. §

[696] Megállapította a 2017.évi CXCVII törvény 421.§ (1), hatályos 2018. VI.1-től

[697] Eüak.tv és Eü.tv.

[698] 2013. évi CCXL 76 § (2)

[699] 2013. évi CCXL 76 § (3b)

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-részlegen[700] vagy magánzárkában helyezkednek el. Az elektronikus megfigyelőeszközök alkalmazása e 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.[701] Bizonyos esetekben a büntetés-végrehajtás 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 iránti előterjesztéshez, továbbá a jogsegélykérelem elintézéséhez és a bűnügyi jogsegélyről szóló jogszabályokban meghatározott vagy nemzetközi egyezményből eredő egyéb feladatai teljesítéséhez szükségesek. [702]

A büntetés-végrehajtás során a rendőrség is jogosult az érintettek adatainak kezelésére, tekintettel arra, hogy az általuk foganatosított kényszerintézkedések beleszámítanak a kiszabott büntetés időtartamába. Jogosultságuk vonatkozik az őrizetbe vett személyek, letartóztatottak,

[700] Hosszúidős Speciális részleg

[701] 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 végezett biztonsági kockázatelemzés céljából. Ez a gyakorlat a 1995. évi CVII. törvény 27/A. § (1) bekezdése és a 150. § (7) bekezdésében meghatározott korlátoknak megfelelően történik.

[702]2013. évi CCXL. 77 § (1)

szabálysértési elzárás alatt állók, pártfogó felügyelet alatt állók, valamint az előállított vagy szállított személyek adatainak kezelésére. [703]

Amennyiben törvény eltérően nem rendelkezik, az adatokat a büntetés, az intézkedés, a kényszerintézkedés vagy a szabálysértési elzárás végrehajtásának befejezésekor, vagy végrehajthatóságának megszűnésekor törölni kell.[704] A Bv. Sztv. 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 büntetés-végrehajtás kapcsán megemlítendő a pártfogó felügyelet intézménye.[705] 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. [706]

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. Ez a bekezdés kiterjeszti az adatkezelés lehetőségeit kutatási és elemzési célokra, azonban kizárólag anonim formában.[707]

Véleményem szerint a személyes adatok kezelése során a büntetés-végrehajtás területén a jogi keretek megfelelnek az adatvédelmi követelményeknek, azaz a törvényi szabályozás a GDPR és az Infotv. szabályait lefedi. A jogszabályi háttér tekintetében nem csak törvényi szabályozás, hanem rendeletek, utasítások, szabályzatok is tartalmaznak adatvédelmi előírásokat az egyes

[703] 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 előállítása, szállítása, és a reintegrációs őrizet végrehajtásához szükséges adatokat ismerheti meg és kezelheti.

[704] 2013. évi CCXL 79 § (1)

[705] 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.”

[706] 2013. évi CCXL 80 § (1)

[707] 2013. évi CCXL 81 § (1)

területeknek megfelelően. A jogszabályok hierachiájában azonos szintű törvények - Bvtv. és Eüaktv. ellentmondásait a jogalap meghatározása oldhatja fel.
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.[708]
A büntetés-végrehajtási 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.

IV.8.4. A fogvatartott nyilvántartása

A fogvatartottak nyilvántartásáról a BvSztv. 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, lakcímeket, 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.[709]
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. Ezen felül

[708] 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.

[709] Bvsztv 28.§, (1)

nyilvántartásba veszik a hivatalos minőségben kapcsolatot tartó személyeket is, beleértve a személyes adatokat és a hivatalos kapcsolatot igazoló okmányok adatait.[710]

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.[711] 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.[712]

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.[713]

A fogvatartottak adatai – személyazonosításra alkalmatlan formában – statisztikai és tudományos célokra is felhasználhatók.[714]

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 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.[715]

---

[710] Bvsztv 28.§ A. (1)- (3)

[711] 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.

[712] Bvsztv 28/B. §- (1) 2017. évi XC. törvény 52. §-a alapján

[713] Bvsztv 29.§ (1) - (3

[714] Bvsztv 29.§ (4)

[715]Bvsztv 9/A. § (1)

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. [716]

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.[717]

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.[718]

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, amennyiben bizonyos adatok, például a fogva tartás 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.[719]

[716] Bvsztv 9/A. § (3)

[717] Bvsztv 9/A. § (4)

[718] Bvsztv 9/A. § (5)

[719] Bvsztv 30.§

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.[720] 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.[721]

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.[722]

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.[723]

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 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

[720] Kondás, Katalin. "Adatok védelme a börtönökben." *Hadmérnök* 13, no. 1 (2018 március): 269-277.

[721] Ibid., 274.o

[722] A büntetés-végrehajtás országos parancsnokának 9/2016. (II.16.) OP szakutasítása a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról

[723] Bvsztv 31.§ - 32.§

hatóságai megfelelnek bizonyos adatvédelmi és jogállamisági követelményeknek, amelyek összhangban állnak az Irányelv és az Infotv. előírásaival.

A NAIH éves beszámolóit 2020-tól áttekintve az adatvédelmi jog megsértését illetően, számos esetben tapasztalható, hogy a jogellenes adatkezelés oka gyakran az adatkezelés jogalapjának hiánya, az arányosság és a szükségesség elveinek megsértése. Az adatvédelmi incidensek számos területen jelentkeztek, kezdve a büntetőeljárások és a büntetés-végrehajtás során keletkezett adatok jogosulatlan hozzáférésétől az egészségügyi adatok kezeléséig.[724, 725, 726]

Büntetés-végrehajtási intézetben a fogvatartottról készült pszichológiai vélemények megismerésének kérdése kapcsán, adatvédelmi incidensnek minősült a NAIH esetei szerint:

- az érintett hozzáférési jogának megsértése, tájékoztatáshoz való jog, adatkezelés jogalapja és célhoz kötöttsége, ennek kapcsán
- az adatvédelmi elvek és jogok érvényesülése a büntetés-végrehajtásban,
- a központi nyilvántartás és az adatkezelés szabályainak hiányos volta, az Infotv. 14. § b) pontjának megsértése, az Infotv. 17. §-ának rendelkezéseinek megsértése – mint a hozzáférési jog sérelmei[727]

Bv. intézetben a fogvatartottak egészségügyi személyes adatainak kezelése során a pontosság elve sérült, amennyiben a papír alapú és a számítógépes nyilvántartás adatai nem egyeztek meg, és a nyilvántartásokból nem volt egyértelműen megállapítható, hogy a bejelentő milyen gyógyszeres kezelésben részesült és milyen rendszerességgel. Ez megsértette az Infotv. 4. § (4) bekezdését.[728]

Az adatbiztonság szintén lényeges kérdés, mivel a technikai és szervezési intézkedések hiányosságai jelentős veszélyt jelenthetnek az érintettek személyes adatainak védelmére. Fogvatartottnak szóló hivatalos irat felbontása történt büntetés-végrehajtási intézetben, az ügyészség nem rendelte el minden esetben a hivatalos irat zárt borítékban történő kézbesítését, lehetővé téve a büntetés-végrehajtási intézet számára, hogy indokolatlanul megismerje a fogvatartottnak szóló hivatalos irat tartalmát.[729]

---

[724] NAIH beszámoló a 2020. évi tevékenységről p.100,. https://www.naih.hu/eves-beszamolok (hozzáférés, 2023.02.20)

[725] NAIH beszámoló a 2021. évi tevékenységről p.105.,. https://www.naih.hu/eves-beszamolok, (hozzáférés, 2023.02.20)

[726] NAIH beszámoló a 2022. évi tevékenységről, https://www.naih.hu/eves-beszamolok, (hozzáférés, 2023.02.20)

[727] Ibid. p.72.

[728] Ibid. p.77.

[729] Ibid. p.78.

Az eseteket elemezve, az adatvédelmi elvek és jogok érvényesítése elengedhetetlen a jogsértő adatkezelések elkerülése érdekében. 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.

IV.8.5. Mesterséges intelligencia rendszerek a büntetés-végrehajtásban

A 2021. október 6-i keltezéssel kiadott Európai Parlament állásfoglalása[730] 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 hőképességű 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, ítélkezési gyakorlatok kezelése és a joghoz való hozzáférés javítása terén. Az állásfoglalással egyetértve, Herke hangsúlyozza, hogy a mesterséges intelligencia alkalmazása során szigorúan be kell tartani az etikai és jogi kereteket. [731]
Hazánkban a büntetés végrehajtásban használnak AI alapú eszközöket. Herke szerint különösen óvatosak vagyunk a mesterséges intelligencia igazságszolgáltatásban betöltött szerepének értékelésében.[732] Ezzel kapcsolatos kételyeit fejti ki Lynskey is, kérdésessé téve a prediktív

[730] 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))."

[731] Herke Csongor. (2023.) "Mesterséges intelligencia a büntetőjogi döntéshozatalban." *Jogtudományi Közlöny* 78, (4) pp. 165-176.

[732] Ibid. p.165.

technológiák rendészeti alkalmazását,[733] mellyel nem értek egyet, a megoldást a megfelelő adatvédelmi keretek kidolgozásában látom.

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 hátteret biztosítva.

A SAFE rendszer egy mobiltelefon méretű, Near Field Communication (továbbiakban NFC) alapú információs készülék[734], amit a büntetés-végrehajtási szervezet használ. Célja a gyors és egyszerű adatlekérés, amely a Fogvatartotti Alapnyilvántartásból[735] 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 rendszerben az offline adatok is elérhetők, mivel WiFi vagy APN technológián keresztül kapcsolódik a központi szerverhez.[736]

A SAFE főbb funkciói:

- Információszolgáltatás a büntetés-végrehajtási intézményben elhelyezett fogvatartottakról, beleértve a következő adatokat: természetes személyazonosító adatok, fénykép, bv. jogviszonyra vonatkozó információk (fogvatartás jellege, jogcíme, időtartama), valamint kiemelt figyelmet igénylő adatok (pl.: magas biztonsági kockázat, szuicid veszélyeztetettség).
- Az engedéllyel birtokolható technikai eszközök nyilvántartása, illetve a fogvatartott bűntársainak azonosítása helyben és országosan.
- A fogvatartottak azonosítása az NFC chipek SAFE eszközzel történő leolvasásával, illetve NFC kártya vagy karkötő használatával.

---

[733] Lynskey, Orla. „Büntetőjogi profilalkotás és uniós adatvédelmi törvény: bizonytalan védelem a prediktív rendfenntartással szemben.” *International Journal of Law in Context* 15, no. 2 (2019): 162–76. https://doi.org/10.1017/S1744552319000090.

[734] A Near Field Communication (NFC**)** egy olyan új, rövid távú (kis hatósugarú), vezeték nélküli kapcsolódási technológia, amely főleg mobileszközök használatára alkalmas, érintkezés nélküli összeköttetési és felismerési technológiákból fejlődött ki. http://www.sarkany.hu/index.dw?mit=133&almenu=97

[735] Büntetés-végrehajtási Szervezet Fogvatartotti Alap Nyilvántartás (FANY)

[736] Hinkel Tamás. 2020. "A mesterséges intelligencia térhódítása a büntetésvégrehajtásban." *Börtönügyi Szemle*, (4), pp. 13-29.

- A fogvatartottak tartózkodási helyének meghatározása (pl. zárkába helyezés, szabadlevegőn tartózkodás, látogatás, munkahely), akár csoportosan is.
- Zárka és ágy kijelölése a fogvatartottak számára.[737]

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 papírmentesen, hatékonyabban tudja ellátni feladatait, teljes figyelmét az őrzési feladatra összpontosítva.[738 ,739]

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

[737] Büntetés-Végrehajtási Biztonsági Ismeretek, 2020.
https://bv.gov.hu/sites/default/files/Biztons%C3%A1gi%20jegyzet%202020.08.10. pdf, (hozzáférés,2023.02.20)

[738] Hinkel Tamás. (2020.) "A mesterséges intelligencia térhódítása a büntetésvégrehajtásban." p.16.

[739] Schmehl 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

adatok hozzáférhetőségét és elemzésének hatékonyságát.[740] A 24 órás adatszolgáltatás modul egységesíti az adatrögzítést, megkönnyítve az adatszolgáltatást és a tovább jelentést.[741]

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.[742]

A büntetés-végrehajtási AI 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 AI alapú rendszerek adatvédelmi problémái közé tartozik a személyes adatok bizalmas kezelése, az adatok szükségtelen gyűjtése és tárolása, valamint a diszkrimináció lehetősége[743] az adatelemzés során.[744] 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 mindezeken kívül kulcselemnek tartja a rendszer megismerhetőségét, azon belül is az alkalmazott logikáról való tájékoztatást tartja az egyik legfontosabbnak.[745]

---

[740] 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 űrlapon keresztül, előre meghatározott válaszokat adva rögzíthetik az eseményeket, csökkentve ezzel a jelentéstétel időigényét. A rendszer automatizált kimutatásokat és táblázatokat generál a tiltott tárgyakról, elősegítve az elemző-értékelő munkát. Ez a fejlesztés javítani fogja az információáramlást és megkönnyíti az adatkezelést a büntetés-végrehajtási szervekben.

[741] Hinkel Tamás. "A mesterséges intelligencia térhódítása a büntetésvégrehajtásban," pp. 17-20.

[742] Ibid. Hinkel Tamás p.20

[743] Mezei Kitti. (2022.) "Diszkrimináció az algoritmusok korában." *Magyar Jog*, (6), pp. 336-337.

[744] 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.

[745] Ibid. p.118.

Az AI alkalmazása adatokra támaszkodik, melyek kezelésének adatvédelmi normáknak kell megfelelnie. Szükséges az adatok védelme az EU[746] 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 AI-adatigénylések támogatására.[747]

V. Az adatvédelem és a kiberbűnözés kapcsolata

A gyors technológiai fejlődés és a hálózati infrastruktúrák expanziója következtében a kiberbűnözés, mint a számítástechnika negatív következménye, korunk egyik jelentős globális problémájává vált. *„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.”*[748]
A modern technológiai fejlesztések alkalmazásával az információs technológia eszközein keresztül számos bűncselekmény megvalósítása válik lehetővé, így a kiberbiztonság a modern ember és társadalom számára elengedhetetlen alapkövetelménnyé vált.[749] A digitális forradalom dinamikus növekedést eredményezett a technológiai fejlődésben. Ez a jelenség nem

[746] 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.

[747] 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.

[748] 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, 179. Budapest, Magyarország: Ludovika Egyetemi Kiadó.

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

csak a technológia terén mutatkozott meg, hanem kihatással volt a számítástechnikai bűncselekményekre is.[750,751,752,753,754]

A statisztikai adatok szerint a kibertámadások számának növekedése a világhálón tárolt adatok mennyiségével arányosan növekszik, 2025-re a világ 200 zettabájtnyi adatot fog tárolni.[755]

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.[756]

V.1. A kiberbűnözés fogalma

A számítógépes bűnözés fogalmának meghatározása nem egységes, számos definiálása ismert a szakirodalomban, gyakran szinonimaként használják az informatikai bűnözéssel.[757]

---

[750] 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.

[751]Datareportal. (2019). "Digital 2019: Global Digital Overview." Retrieved from https://datareportal.com/reports/digital-2019-global-digital-overview.

[752] 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

[753] Wall, David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.

[754] Holt, Thomas J., Bossler, Adam M., and Seigfried-Spellar, Kathryn C. (2022). *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. London: Routledge.

[755] 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

[756] Statista. "Annual cost of cybercrime worldwide 2017-2028." 2023. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[757] Kiss, Tibor. "Kiberbűnözés." In *Alkalmazott Kriminológia*, szerkesztette Barabás A. Tünde, p.445.

„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”

A kiberbűnözést több szerző, mint Jonathan Clough[758], Peter Grabosky[759] és Susan W. Brenner, [760]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.[761]. A magyar szakirodalomban számos szerző vizsgálta az informatikai bűnözés fogalmát, köztük Polt Péter, Pusztai László, Nagy Zoltán András.[762] Később Parti Katalin és Kiss Tibor,[763] Szathmáry Zoltán,[764] valamint Szabó Imre[765] is kifejtették saját értelmezéseiket, melyek összhangban vannak a nemzetközi szakirodalom definícióival.

Alapvetően kétféle értelemben használatos, egyrészt ezen értve a számítógéppel, mint eszközzel elkövetett cselekményeket[766], másrészt azokat az informatikai bűncselekményeket, amelyeket az információs rendszer, a hálózatok, illetve adattartalom ellen követnek el.

A "tiszta" 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 kapcsolatosak. (IKT eszközök) Például a számítógépes adathalászat vagy a rosszindulatú kártevőkkel való fertőzés "tiszta" kiberbűncselekményeknek számítanak.[767]

---

[758] Clough, J. (2015.) *Principles of Cybercrime*. Cambridge: Cambridge University Press, pp.10-11.

[759] Grabosky, Peter. (2016.) *Cybercrime*. Oxford: Oxford University Press, pp. 8-9.

[760] Brenner, W. S. (2010.) *Cybercrime – Criminal Threats from Cyberspace*. Santa Barbara: Praeger, pp.39-47.

[761] Grabosky, Peter. (2001.) "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2: pp.243-249.

[762] Sieber, U. (1993.) "A számítógépes bűnözés és más bűncselekmények az információtechnológia területén." *Magyar Jog*, no. 2: pp.105–109.

[763] 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.

[764] 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.

[765] Szabó I. (2008.) "Informatikai bűncselekmények." In *Az informatikai jog nagy kézikönyve*, szerk. Dósa I., Budapest: Complex pp.547.

[766] Tóth Dávid és Nagy Zoltán András. (2015.) "Computer related economic crimes in Hungary." *Journal of Eastern-European Criminal Law*, no. 2: pp. 165-174.

[767] 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.

A kiberbűncselekmények 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.[768]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.[769]

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.[770]

A kiberbűnözés 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 elkövethetők.[771] 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.

---

[768] Knoops, Bert-Jaap. (2011). "The Internet and its Opportunities for Cybercrime." *Tilburg Law School Legal Studies Research Paper Series*, 9, p. 739.

[769] Ambrus, István. *Digitalizáció és büntetőjog*. Budapest: Wolters Kluwer, 2021, p.290.

[770] Grund, Borbála. (2021). "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról." *MTA LAW WORKING PAPERS*, 20212, 1-37.p.37

[771] 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.

V.2. A kiberbűncselekmények jellegzetességei

V.2.1 Hacking és adathalász jellegű bűncselekménye

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. „hekkelhetőség",[772] 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, okostelevíziókat 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.[773]

A hacking-jellegű cselekmények mögötti motivációk között szerepel az információhoz való hozzáférés, az adat megváltoztatása vagy törlése, valamint az információs rendszer használata.[774]

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

---

[772] Furnell, Steven. (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 belépes. 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.

[773] 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.

[774] Momsen, Carlsten. "Relevance of Data Security and Data Protection in Companies from the Perspective of Criminal Law." In *Handbook Industry 4.0*, edited ed.Walter Frenz, 57–74. Berlin, Heidelberg: Springer, 2022. https://doi.org/10.1007/978-3-662-64448-5_3.

követően az elkövetők gyakran nem saját céljaikra használják fel ezeket, hanem tovább értékesítik azokat a Darknet fórumokon.[775,776]

V.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) [777] 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.[778]

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-támadásokat[779] is felhasználnak zsarolási célokra, ahol az elkövetők a célpont weboldalának vagy hálózatának leállításával, vagy annak működésének megzavarásával fenyegetnek. Ezek a támadások különösen veszélyesek lehetnek, hiszen jelentős anyagi és reputációs károkat okozhatnak a cégeknek vagy szervezeteknek.[780]

---

[775] Bartlett, Jamie. (2014). *The Dark Net: Inside the Digital Underworld*. London: Heinemann p.303

[776] Mezei Kitti. (2020). "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre." *Állam- és Jogtudomány* 61,(4), p.70.

[777] Bart Custers, Jan-Jaap Oerlemans, and 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.

[778] McGuire, Mike., and Dowling, Samanta. (2013). Cyber-dependent crimes. In *Cybercrime: A review of the evidence* (Research Report 75, Chapter 1). Law, Computer Science.

[779] 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.

[780] 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

Ezek a modern zsarolási módszerek rávilágítanak az információs rendszerek és az online adatok védelmének fontosságára.

V.2.3. A személyiséglopás jelensége, mint a kiberbűncselekmények sajátos együtt állása

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. Ezek a tényállások a következő fejezetben kerülnek részletes elemzésre.

A személyiséglopás az információtechnológia rohamos fejlődésével párhuzamosan globális szinten nőtt. Az ENISA az adatok elleni támadások közül kiemeli 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 (Federal Trade Comission - 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.[781]A jelenség nem kötődik specifikusan a fejlett technológiákban élenjárró földrészekhez.[782]

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,

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).

[781] ENISA, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[782] Cassim, Fawzia. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?. *Potchefstroom Electronic Law Journal (PELJ)*, *18*(2), 69-110.https://doi.org/10.4314/PELJ.V18I2.02

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.[783]

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.[784]

Kahn és Roberds definíciójukban az identitáslopást a más személyes adatok csalási szándékkal történő felhasználásaként határozzák meg.[785] Farina azonosításában a csalásra koncentrál: „*Egy személy személyes adatainak csalárd célból való felhasználása.*"[786] Biegelman – aki a témáról kézikönyvet írt – szerint az identitáslopás az emberek jóhírnevének és hírnevének anyagi előny szerzése céljából történő megszerzése.[787]

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. [788]

Amennyiben a különböző fogalmi meghatározásokat összehangoljuk, a következő közös elemek azonosíthatók minden definícióban: az elkövetés tárgya, amely az identitáshoz kapcsolódó információkat foglalja magában. A bűntetendő cselekmény, amely magában foglalhatja az információk megszerzését, felhasználását és kereskedelmét, valamint az alanyi

---

[783] Arnold, Tom. (2022). "The Early Prediction of Internet Identity Theft and Its Global Impact on Cybersecurity." *Journal of Cybersecurity Research,* 20 (2) p. 32.

[784] Tóth, Dávid, „Az identitáslopás kriminológiai sajátosságai" p. 207.

[785] Kahn, Charles M., and William Roberds. "Credit and Identity Theft." *Journal of Monetary Economics* 55 (2008): p. 251. Idézi: Tóth, Dávid, Ibid. p. 208

[786] 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

[787] 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

[788] US Code 18. fejezet, 1028.§ Idézi: Tóth, Dávid, Ibid. p. 208

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 magánélet fenyegettsége előfeltétele az személyes adatok elleni bűncselekmény bekövetkezésének.[789]

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 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 értékként jelenik meg az adathoz 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. [790]

A fentieken 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 rágalmazás (Btk. 226. §), ahol a személyes adatokhoz kapcsolódó rágalmazó 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

[789] Petrović, Dragana B. "Privacy and Protection of Personal Data – Criminal Law Aspect." *Strani pravni život* 66, no. 4 (2022): 469-486. https://doi.org/10.56461/SPZ_22407KJ.

[790] 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 Ćeranić, Dimitrije; Ivanović, Svjetlana; Lale, Radislav; Aličić, Samir, pp. 233-246. East Sarajevo, Bosnia-Herzegovina: Faculty of Law, University of East Sarajevo.

használata (Btk. 393. §), illetve az információs rendszeren keresztüli csalás, amennyiben az elkövető anyagi kárt okoz (Btk. 375. §).[791,792,793]

A hamis vád esete, amikor az elkövető más személy okmányait és személyes adatait felhasználva igazolja saját azonosságát. [794] Emellett a személyes adatok bűncselekmény tárgyai lehetnek olyan esetekben is, amikor titkosított információkról vagy a nemzeti vagyont képező nyilvános nyilvántartásokkal és jegyzékekkel kapcsolatban (Btk. XXV. fejezet), történik bűnelkövetés.[795]

A GDPR értelmében a személyes adatok védelme alapvető jog. A GDPR által az adatkezelők számára előírt ún. beépített adatvédelem elve[796] jelentik a legnagyobb prevenciós erőt 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 identitáslopás mint jelenség átfogó jellegű abban az értelemben is, hogy az online térben történt elkövetési módok által - phising, smishing, wi-phising, skimming, hacking- több a következő fejezetben leírt büntetőjogi tényállást megvalósítanak. [797]

---

[791] Tóth Dávid, ”A bankkártyával kapcsolatos bűncselekmények prevenciós eszközei”, PEME XV. PhD – konferenciakötet (eds. I. Koncz, I. Szova), Professzorok az Európai Magyarországért Egyesület, Budapest 2017, pp. 182–192.

[792] 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.

[793] Gál, István L.”A pénz–és bélyegforgalom biztonsága elleni bűncselekmények,” Új Btk. kommeV/ntár: 7. kötet, Különös rész, (ed. P. Polt), Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest 2013, 193–224.

[794] BH 2014.234.II., Idézi Tóth, Dávid,” Személyiséglopás az interneten” *Büntetőjogi Szemle 2020/1. szám*, (2020), 116-117.

[795] Miskolczi Barna., Szathmáry Zoltán , "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.

[796] GDRP 35. cikk

[797] Tóth Dávid. (2020). "Személyiséglopás az interneten." *Büntetőjogi Szemle*, 2020/1. szám, 116-117.

V.2.4 Jogszabályi háttér [798]

A kiberbűncselekmények 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)[799], amely 2004-ben lépett hatályba. Ez volt első nemzetközi szerződés, amely kifejezetten a számítógépes bűnözésre összpontosított.[800]

Ide sorolhatók továbbá a számítástechnikai bűnözés elleni küzdelem területén a nemzetközi együttműködéssekkel kapcsolatos kezdeményezések – az ENSZ, az OECD, az Európai Unió és a G8-ak által – ehhez kapcsolódó egyezmények, illetve ajánlások.[801,802,803,804,805] Az első fontos nemzetközi jogi dokumentum a Gazdasági Együttműködési és Fejlesztési Szervezet

---

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

[799] Council of Europe. 2001. "Convention on Cybercrime." *European Treaty Series – No. 185*. https://rm.coe.int/1680081561. (hozzáférés, 2023.02.20)

[800]A 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 (hozzáférés, 2023.02.20)

[801] 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. (hozzáférés, 01.06.2019).

[802] 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).

[803] 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. (hozzáférés, 01.06.2019).

[804] 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. (hozzáférés,01.06.2019).

[805] 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. (hozzáférés, 01.06.2019).

(OECD) által kibocsátott 1986-os jelentés volt.[806,807] A következő fontos dokumentum az Európa Tanács 1989-es ajánlása,[808] az Európa Tanács 1995-ben adott ki egy újabb ajánlást, amely többek között az információs technológiával kapcsolatos büntető eljárásjogi problémákat gyűjtötte egybe.[809]

2005-ben került elfogadásra az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat.[810] A kerethatározat büntetőjogi intézkedéseket, szankciókat és információcserére vonatkozó eljárásokat is tartalmaz.

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).[811]

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.[812,813]

Az (EU) 2016/1148 irányelv (Network and Information Systems,NIS),[814] 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.[815]

---

[806] 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.

[807] 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.

[808] Recommendation No. R (89) 9 to Member States on Computer-Related Crime., Accessed June 1, 2019. https://rm.coe.int/09000016804f1094.

[809] Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology. https://rm.coe.int/16804f6e76. Accessed [01.06.2019].

[810] A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról." *Hivatalos Lap* L 69/67,

[811] 460/2004/EK Rendelet, Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. *Hivatalos Lap* L 77 (13 március 2004).

[812] 2013/40/EU Irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

[813] Nagy Zoltán András.(2020) "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor, Budapest: Dialóg Campus. p.49.

[814] 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).

[815] (EU) 2016/1148 1. cikk (1)

Az Európa Tanács 2017-ben bízta meg az Egyezmény Bizottságát a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv[816] tervezetének megalkotására, elsősorban az elektronikus bizonyítékok, a számítógépen tárolt adatok büntetőeljárás során történő hozzáférésével 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.

A 2016-ban bevezetett uniós kiberbiztonsági szabályokat a 2023-ban hatályba lépett (EU) 2022/2555 irányelv (NIS2) módosította.[817] 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.

---

[816]"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.

[817] 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. (...)”

V.3. Személyes adatok, mint a kiberbűncselekmények elkövetési tárgyai

Az Európai Parlament és Tanács 2013/40/EU irányelve[818], 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.[819] Ennek eredményeként az illetéktelen személyek egyre könnyebben szerezhetik meg a személyes adatokat, például malware, phishing és egyéb módszerek segítségével.

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.[820] 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.[821] 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. Ezen kívül 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

---

[818] 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.

[819] Ibid., (EU) 2013/40/, Preambulum (14)

[820] 1/2012. számú BJE-határozat. Idézi: Mezei Kitti "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre"

[821] 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.

adatalany számára gyakran követhetetlen lehet. Minél több eszköz kapcsolódik a hálózatba, annál több adat gyűjthető az egyes személyekről, ami alapján részletes személyiségprofilok is készülhetnek.[822]

Klasszikusnak mondható a személyes adatokat ért támadás tekintetében a már tárgyalt identitáslopás jelensége.

V.3.1. A személyes adatok védelmének szerepe a kiberbűnözés elleni küzdelemben

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 legjobb gyakorlatok" és szabályozások is hozzájárulnak az adatvédelmi normák megerősítéséhez, ezzel a kiberbűnözés csökkentéséhez, mivel meghatározott keretet biztosítanak az adatok kezelésére és védelmére.[823,824]

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.[825]

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

---

[822] Ibid., p. 411.

[823] Moore, Tyler. and Anderson, Ross. (2019). "Rethinking Information Security to Improve Data Privacy," European Journal of Information Systems, 28(5), pp.687-694.

[824] European Union Agency for Cybersecurity (ENISA). (2020). *Threat Landscape for Cybersecurity in the Context of GDPR*. European Union Agency for Cybersecurity.

[825] Cate, Fred, and Rachel Dockery. "Data Privacy and Security Law." In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish. *Oxford Handbooks*. Oxford: Oxford Academic, 2021. Online edition, December 8, 2021. https://doi.org/10.1093/oxfordhb/9780198800682.013.20.

tartozik a „beépített adatvédelem” elvének alkalmazása és az adatvédelmi hatásvizsgálat elvégzése, amennyiben a meghatározott feltételek teljesülnek. [826]

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 (lásd. 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.[827]

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. [828]

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

---

[826] 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

[827] 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.

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- periferikus modellben értelmezzük (Alekszij jogelméleti megközelítés)

[828] 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.

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 összegfoglaló tanulmány is vizsgálta, hogy az általános adatvédelmi rendelet bevezetése milyen hatással volt a szervezetekre kiberbiztonsági eredményeiket illetően.[829] A felmérés összefüggés keresett a NIS irányelvvel is. Megállapították, hogy a GDPR hatására a szervezetek jelentősen javítottak 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.[830]

Az adatvédelmi szabályozás szerepét a kiberbiztonság területén az alábbiakban összegezhetjük:

---

[829] 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

[830] Hirvonen, Pauliina. (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.

- 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.[831] 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 hozzáférését adatainkhoz, vagy az adatlopást.
- Adatkezelési elvek: A GDPR és a LED az adatminimalizálás elvét[832] 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.
- 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.[833] 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.[834] 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.[835] Ez hatással lehet a kibertámadások okozta károk enyhítésére.

V.3.2. Az (EU) 2022/2555 Irányelve (NIS 2) és az adatvédelem kapcsolódási pontjai

[831] (EU) 2016/679, Preambulum (8), 47. cikk d)

[832] (EU) 2016/679, 5. cikk c)

[833] (EU) 2016/679, 35. cikk

[834] (EU) 2016/679, Preambulum (73), 15V/V/. cikk

[835] (EU) 2016/679, Preambulum (49),(85) – (88), 33. cikk

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. törvény[836] 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 be bizonyos iparágakban és digitális szolgáltatásnyújtók számára.[837]A tanulmány egyúttal az átfedésekből adódó problémákat is jelzi, ilyen például az incidens bejelentési kötelezettség.

Bár elméletben elkülöníthetők 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.[838]

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.

[836] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

[837] 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). hozzáférés: at SSRN: https://ssrn.com/abstract=3512093 or http://dx.doi.org/10.2139/ssrn.3512093.

[838] Ibid.,17.p

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,[839] amelyek együttesen erősítik az adatvédelmi és kiberbiztonsági keretet.

- 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.[840]
- 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.[841]
- 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

[839] A NIS 2 előírásai magukban foglalják az információs rendszerek és adatok biztonsági besorolását, információbiztonsági szabályzatok kialakítását, eseménykezelést, ellátási lánc biztonságának garantálását, 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.

[840] (EU) 2022/2555, 32. cikk (2) b)

[841] EU) 2022/2555, Preambulum (102)

kockázatait. A nemzeti implementációk követelményei szerint az elektronikus információs rendszerek üzemeltetésében részt vevőknek is meg kell felelniük ezeknek az előírásoknak.[842]

- 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 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 jogalapjára.[843]

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.[844] Ezek az alapelvek különösen fontosak a kiberbűnözés viszonylatában, mivel az adatvédelmi intézkedések és az adatbiztonsági protokollok, [845] 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 kiberbiztonságért felelős hatóságok jogosultak arra, hogy kibervédelmi incidens esetén az érintett szervezetek szolgáltatásait igénybe vevő személyeket tájékoztassák

[842] EU) 2022/2555, Preambulum (85)

[843] (EU) 2022/2555, Preambulum (51)

[844] (EU) 2016/679 5. cikk

[845] EU) 2016/679 25. cikk (2)

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 és kiberbiztonsági incidensek kezelésére vonatkozó eljárások integrálását, valamint a kiberbiztonsági és adatvédelmi intézkedések hatékonyságának folyamatos értékelését.

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.[846]

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.[847] A GDPR személyes adat fogalmát a következőképpen 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*”[848]

[846] Görög, Márta, Menyhárd, Attila., & Koltay, András. (2017). "A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül." ELTE ÁJK, Budapest, 406.

[847] Infotv. 3.§ 2.

[848] GDPR. 4. cikk,

A meghatározás jelentőségét mutatja, hogy egy Kúriai döntés jelentős szakmai vitákat váltott ki, az értelmezést illetően.[849]

A Büntető Törvénykönyv XXI. fejezete, amely az emberi méltóság és egyes alapvető jogok elleni bűncselekményeket tárgyalja, szabályozza a személyes adatokkal való visszaélés bűncselekményét.

VI.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 keret rendelkezései közé esik. A büntetőjogi keretet elsősorban a GDPR szabályai töltik meg tartalommal, amennyiben az adott adatkezelési tevékenységre a GDPR tárgyi hatálya kiterjed.[850]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.[851]

A keret diszpozíciók 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.[852] A külső norma megsértése tehát nem minden esetben jelent egyben bűncselekmény elkövetését, csak akkor, ha azt a Büntető Törvénykönyvben meghatározott módon sértik meg.

---

[849] BH 2019.272

[850] 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.

[851] Jóri András. (2018). "IV. fejezet. A rendelet hatálya." In *A GDPR magyarázata*, szerk. Jóri András, 118. Budapest: HVG-ORAC Lap- és Könyvkiadó, p. 118

[852] Belovics Ervin, Gellér Balázs, Nagy Ferenc, és Tóth Mihály. *Büntetőjog I., Általános rész*. HVG-ORAC. 2014. 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.

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 érdeksérelmet okozva*
a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
b) az adatok biztonságát szolgáló intézkedést elmulasztja,
vétség 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 bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.”

VI.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.

VI.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.[853]. Számos szerző képviseli ezt az álláspontot. [854] ,[855],[856] Ezt a véleményt osztja Gál Andor is, aki kiemeli, hogy csak a természetes személyre vonatkozó adat lehet az elkövetés tárgya [857], így bűncselekmény nem követhető el szervezet (jogi személy, személyösszesség) vagy elhunyt személy adatával összefüggésben.[858] Lényegesnek tartja az adott személye vonatkozó bármely információ meglétét ebben az összefüggésben.

Ezzel ellentétes 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*."[859] A személyes adat fogalmát a GDPR [860] és az Infotv.[861] 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.

---

[853] Péterfalvi Attila – Eszteri Dániel: „A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata" p..458

[854] Békés, Ádám. (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..

[855] Belovics, Ervin. (2021). "Az emberi méltóság és az egyes alapvető jogok elleni bűncselekmények." In *Büntetőjog II. Különös Rész*, szerk. E. Belovics E., 280. Budapest: HVG-ORAC

[856] ' Horváth Tibor. (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

[857] 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

[858] 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.

[859] Szomora ,Zsolt. (2013). "Btk. XXI. fejezet." In *Kommentár a Büntető Törvénykönyvhöz*, szerk. Karsai Krisztina, Budapest: Complex.p.459.

[860] GDPR 4. cikk 2

[861] Infotv. 3. § 10.

Az első alakzat szerinti elkövetési magatartás a jogosulatlan vagy céltól eltérő adatkezelés,[862] amely aktív magatartást jelent. Az adatkezelés a GDPR és az Infotv. alapján azon tevékenységek összessége, amelyek a személyes adatok bármiféle kezelését magukban foglalják.[863] 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 kötött[864], ha az adatkezelés nem megfelelő céllal történik, akkor megfelelő jogalap esetén is jogszerűtlen, és tényállásszerűvé válik.

A második alakzat szerinti elkövetési magatartás a mulasztás[865], amely az adatok biztonságát szolgáló intézkedés elmulasztásával valósul meg.[866] 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 szolgálják. 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.[867]

A felvázolt lehetséges elkövetési magatartások további két alternatív tényállási elem megvalósulása esetén vezetnek büntetendőséghez. Egyrészt a magatartásoknak vagy jelentős

---

[862] Btk. 219. § (1) a)

[863] GDPR 4. cikk 2. pontja és az Infotv. 3. § 10. pontja szerinti 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”

[864] GDPR 6. cikk és Infotv. 4. §:

[865] Btk. 219. § (1) b) pont

[866] GDPR 32. cikk és Infotv. 25/I. §- a szerinti a „megfelelő technikai és szervezési intézkedések”

[867] GDPR 5. cikk (1) bek. a)–c) pont.

érdeksérelmet kell okozniuk, vagy – érdeksérelem hiányában – haszonszerzési célból kell azokat kifejteni.

„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.).”[868]

A haszonszerzési 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 haszonszerzési célból, tehát anyagi haszonszerzésre törekedve sérti meg az elkövető. Nem szükséges, hogy az elérni kívánt hasznot realizálja is.[869]. A jelentős érdeksérelem okozásával megvalósuló személyes adattal visszaélés eredmény-bűncselekmény, amely akkor válik befejezetté, amikor az érdeksérelem ténylegesen bekövetkezik. Ugyanakkor, amennyiben a cselekményt haszonszerzési szándék motiválja, a bűncselekmény akkor is megvalósul, ha a jelentős érdeksérelem tényleges bekövetkezése elmarad.

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 haszonszerzésre 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.[870]

A bűncselekmény harmadik alakzata a tájékoztatási kötelezettség megszegésével valósul meg.[871] 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 eredetére, kezelésük céljára, jogalapjára, időtartamára, az adatfeldolgozó adataira, az

---

[868] 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, p.445.

[869] Péterfalvi Attila, Eszteri Dániel. „A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata” p. 459.

[870] Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." p.445.

[871] Btk. 219. § (2)

adatkezelési műveletekre, és ha történt adattovábbítás, annak jogalapjára és címzettjére vonatkozó információkat.

Az érintett kérelmére a tájékoztatást legfeljebb huszonöt napon belül írásban vagy elektronikus úton meg kell adni[872], 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.[873]

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 aktusaiban foglalt előírásokat megsértve nem ad megfelelő tájékoztatást az érintett személy hozzáférési jogának gyakorlásához, és ezzel súlyosan sérti más személyek érdekeit.[874]

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.[875]

VI.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

[872] GDPR 13–14. cikk és az Infotv. 15–16.

[873] Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények.„ p. 445.

[874] „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.

[875] „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

bűnügyi személyes adatra követik el.[876] Minősített esetet képez, ha a személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.[877]

A hivatalos személyként elkövetett személyes adattal visszaélés speciális tényállás a hivatali visszaéléshez képest.[878] 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.[879]

Ha azonban a hivatalos személy a személyes adattal nem jogtalan haszonszerzés 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 visszaélés[880] szerinti bűncselekmény igen[881]

VI.1.4. Rendbeliség

A bűncselekmény rendbelisége az érintett személyek számától függ, kivéve a (2) bekezdés[882] szerinti alakzatot, amely több sértett esetén is törvényi egységet képez.

---

[876] 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 érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat

[877] Btk. 459. § (1) bekezdés 11. pont

[878] Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." p. 446.

[879] 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 bűntettét 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 érdeksérelem vagy haszonszerzési célzat bizonyítandó, hanem a hivatalos személy által a jogtalan adatkezeléssel szerzett jogtalan előny vagy okozott jogtalanhátrány. Lásd.: Péterfalvi- Eszteri p. 417.

[880] Btk. 305. §

[881] BH2013. 146., BH2015. 296

[882] 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

A személyes adattal kapcsolatban a már hivatkozott Kúriai döntés - BH 2019.272 - kapcsán, az azonosított, az azonosíthatóság, és a személyes adatra vonatkoztatható fogalmak értelemzési problémája merült fel, melynek jelentősége a büntetőjogi megítélés szempontjából fontos. Lényeges ebből a szempontból, hogy milyen információkat tekintünk egy adott személyre „vonatkozónak". Egy adat vagy információ akkor tekinthető személyre vonatkozónak, ha legalább egy az alábbi három kritérium közül teljesül: tartalom, cél vagy eredmény.[883] 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.[884]

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.[885]

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.[886,887]

---

gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti."

[883] Pók, László, (2019) "5 kínzó kérdés a Kúria személyes adatokra vonatkozó döntése alapján." gdpr.blog.hu.

[884] 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

[885] WP.29 4/2007. sz. vélemény, 13. o Idézi: Ibid. Pók László

[886] Miskolczi Barna, Szathmáry Zoltán. (2019). *Büntetőjogi kérdések az információk korában*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., 140-141.

[887] Szathmáry, Zoltán (2019). "A mesterséges intelligencia hatása a büntetőjogi felelősségre." *Ügyészek Lapja*, 26 (3), pp. 37-46.

A Kúria ítéletének[888] elemzése során két lényeges pont merül fel: az egyik, hogy az adatok, melyek álnéven kerülnek átadásra egy szervnek, valójában konkrét személyekre vonatkoznak, 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 közvetetten 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.[889]

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.[890]

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

[888] 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.

[889] BH 2019.272 Ítélet: 19. pont, Idézi: Pók, László: "5 kínzó kérdés a Kúria személyes adatokra vonatkozó döntése alapján."

[890] Czapári, Dóra, Szőke, Gergely László.(2022) "Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása." *JURA* 28, (4) 24-48. p.30.

egyén. Ez egy további lépés, amely nem közvetlenül az adat személyes jellegének megállapításához kapcsolódik. Az eset részletes elemzésével Pók László szolgál.[891]
A személyes adatokkal történő visszaélések esetében további jogesetek, bírósági ítéletek és döntések, valamint példák tekintetében hivatkozom Gyaraki Réka elemzéseire.[892]
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.[893]
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 rendeletre, 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.[894]

VI.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 és tényállási elemek

A bűncselekmény jogi tárgya a sértettnek a magántitka megőrzéséhez fűződő személyiségi joga.

---

[891] Ibid., Pók László

[892] Gyaraki Réka (2023). "Az adatokkal kapcsolatos visszaélések és az információs rendszerben tárolt adatok sértetlensége." In *A kibernyomozói munka büntetőjogi sajátosságai*, szerk. Kovács Zoltán, 90. Budapest, p.90

[893] EU 2016/679 Preambulum (149)

[894] 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.

A magántitok megsértésének bűntette 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.[895] A magántitok jogellenes nyilvánosságra hozatala kiterjedhet a személyi, családi, gazdasági státuszra, egészségi állapotra vagy bármely egyéni szokásra, ami egyébként nem lenne nyilvános.[896]

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 bűntettében 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.[897]

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

[895] 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. §).

[896] BH.2004. 170 f

[897] Btk. 219. § (4)

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 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.

VI.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.[898]

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.[899]

[898] Btk.195. §.

[899] Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények” p. 454.

VI.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, rágalmazás bűncselekménye[900] is megállapítható.

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 kezelőszemély, az adatkezelés biztonságát szolgáló intézkedéseket elmulasztja, akkor a személyes adattal visszaélés cselekménye valósul meg,[901] 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.[902]

Különleges személyes adat esetén szintén a személyes adattal visszaélés tényállása valósul meg.[903] A magántitok megsértését a NAIH hatósági eljárás során vizsgálta egy kérelmezés kapcsán, és a GDPR alapján adatvédelmi bírságot állapított meg.[904] Az eset kapcsán

[900] Btk. 229. §

[901] Btk. 219. § (1) bekezdés b)

[902] Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények" p.454.

[903] Btk. 219. § (3)

[904] 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.

büntetőeljárás is zajlott. A párhuzamos eljárás lehetőségére mind a GDPR[905], mind az Infotv.[906] lehetőséget ad.

VI.3. Levéltitok megsértése

224. § (*1) Aki*

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 közmegbízatás felhasználásával követik el.

(3) A büntetés

a)két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény,

b) bűntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős érdeksérelmet okoz."

VI.3.1. Jogi tárgy és tényállási elemek

A bűncselekmény jogi tárgya a személyiségi jogok általános kategóriájába tartozó az magánélet sérthetetlenségének joga és az hirdetett emberi méltósághoz való jog. A jogvédelem a magánszemélyekre, a jogi személyekre, illetve a hatóságokra és a hivatalos személyekre egyaránt vonatkozik.

---

[905] 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.

[906] 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 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 bármely 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 Btűrlapk. 224. szakasza (1) bekezdés b) pontjában kerül meghatározásra, mely az elektronikus hírközlő hálózaton keresztül továbbított közleményeket célozza meg, az információs rendszereket is beleértve.[907]

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.[908]

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 e 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.[909]

VI.3.3. Stádiumok és tettesség

[907] Btk. 459. § (1) bekezdés 15. pont

[908] Szomora, Zsolt. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények”p.456.

[909] Btk. 459. § (1) bekezdés 15. pont

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.

VI.3.4. Minősített esetek

Amennyiben a cselekményt a tettes a foglalkozásával vagy közmegbízatásának 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 készteti, hogy egy levelet átadjon a tartalmának megismerése céljából, szintén ide tartozik. További minősítő körülmény, ha a cselekmény jelentős érdeksérelmet okoz. Ebben az összefüggésben a Btk. 9. szakasza alapján a tettes gondatlansága is elegendő ahhoz, hogy a jelentős érdeksérelem kritériuma teljesüljön.

VI.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.[910]

VI.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, rágalmazás 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.szakasza (2) bekezdés alapján.

VI.4. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

Az informatikai bűncselekmények saját fejezetet kaptak a Büntető Törvénykönyvben, az Európai Unió 2013/40 irányelvének [911] 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

[910] Be. 43. § (2), 200–206/A. §

[911] 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.

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 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.[912]

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.

VI.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 történteket 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 kifürkész, és az észlelteket technikai eszközzel rögzíti, (…)

[912] Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I., *Infokommunkácó és Jog,* 2022/2. (79.), pp. 6-10

422/A. *§ (1) Aki pilóta nélküli légi jármű jogosulatlan használatával más lakását, egyéb helyiségét, vagy ezekhez tartozó bekerített helyet megfigyeli és az ott történteket 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 átkutatja mások lakását, helyiségét vagy azokhoz tartozó területet, technikai eszköz segítségével megfigyeli, rögzíti az ott történteket, 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.

VI.4.1.1. Jogi tárgy

A bűncselekmény jogi tárgya a személyes adat, magántitok, gazdasági titok, üzleti titok védelme.

VI.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).[913] 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.[914]

Az első alapeset közül elkövetési magatartásai, a titkos helyiségek átkutatása, technikai eszközökkel történő megfigyelés, zárt küldemények jogosulatlan felbontása, elektronikus

[913] 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

[914] Ibid., p. 911.

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.[915] Ebben az esetben a törvény célja ezeknek a személyeknek a 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 megkezdi 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.

VI.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.

[915] 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.

VI.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, bűnszövetségben jelentős érdeksérelmet 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.[916]

VI.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,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő”.

[916] 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.

(3) A büntetés bűntett 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."

VI.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 „hackinget" mint eszközcselekményt.[917] 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. [918] Az elektronikus adatok fogalma a digitális bizonyítékok fogalmának megfeleltethető, annak megfelelően határozza meg azt a büntetőeljárásról szóló törvény is.[919]

VI.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. Jellemzően a hacking, DDoS- és a malware-támadások az információs rendszer vagy adat megsértése körébe tartozó

[917] Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.

[918]Nagy Zoltán. "A kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerkesztette Kiss Tibor. Budapest: Dialóg Campus, 2020.p.51.

[919] Máté István Zsolt. (2018). "Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe." *Belügyi Szemle, 2018, 66, (*7-8), pp. 36-54.

cselekmények.[920] Adatintegritás sértése, az információs rendszerben tárolt adatok jogosulatlan megváltoztatásával történhet. Ennek jogi tárgya, kiegészül, az az adatok tartalmától függően azok által képviselt értékkel.[921]

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.[922]

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 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.[923]

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. [924] 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

[920] Nagy Zoltán. "A kiberbűncselekmények szabályozása."p.51.

[921] Nagy, Zoltán András. "A számítógépes környezetben elkövetett bűncselekmények új szabályozásáról. Háttér és elemzés." *Ügyészek Lapja*, 2014/3-4. sz., p.32.

[922] Kúria BHAR.I.537/2017/5. sz. határozata és BH2017. 392.

[923] Grund, Borbála.(2021) "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról." p.15.

[924] Nagy Zoltán. "A kiberbűncselekmények szabályozása." p. 51.

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. [925]

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 és ennek következtében az adatbevitelre, ebben az esetben a rendszer működésének akadályozása kérdéses lehet. [926]

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.[927]

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

[925] Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.

[926] Ibid.,

[927] Szabó Imre. 2008. "Informatikai bűncselekmények."p.612.

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.[928]

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 megsértő törlése, vagy hozzáférhetetlenné tétele az Irányelv 5. cikkének, mint „adatot érintő jogellenes beavatkozás" a magyar szabályozásba történő átültetésének feleltethető meg.[929]

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.

[928] Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I.

[929] Grund, Borbála. "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról."p.15.

Jelenleg a számitógépes rendszerek mechanikus - technikai védelmét ez tényállás nem tartalmazza, azt a rongálás törvényi tényállása adja.[930]

VI.4.2.3 Minősített esetek és rendbeliség

Ha a cselekmény jelentős számú információs rendszert érint, és jelentő érdeksérelem következik be, vagy ha bűncselekmény egy közérdekű üzem információs rendszerét érinti.[931]

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.

VI.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, megszerez, vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja,

vétség 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.

---

[930] 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

[931] 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

VI.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 károkozói 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.

VI.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, úgymint 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.[932]

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.[933]

[932] Nagy Zoltán. "A kiberbűncselekmények szabályozása." p.56.

[933] Ibid. p. 56

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 botnetek 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.[934] Befejezett a bűncselekmény az elkövetési magatartások bármelyikének tanúsításával. A bűncselekmény elkövetője tettesként bárki lehet.[935]

VI.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 készítő tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

VI.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.[936]

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, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.”*

[934] Szathmáry Zoltán: (2023) "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése II.", *Infokommunikáció és Jog*, 2023/1. (80.), pp. 11-13.

[935] Karsai, Krisztina. "Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." p. 918.

[936] 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.

(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.

(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül."

VI.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.[937]

A tényállás szerkezete szerint a bűncselekmény két fő alakzatot különböztet meg.

Az egyik a károkozó adatvisszaélés,[938] ami az információs rendszerbe jogtalanul bevitelt, a rendszerben kezelt adatok jogosulatlan módosítását, törlését, vagy hozzáférhetetlenné tételét,

[937] Ambrus István.(2021) "Vagyon elleni kriminális cselekmények a modernizálódó kiskereskedelemben." *Ügyészek Lapja* 27, no. 1-2 ISSN 1217-7059.

[938] Btk. 375. § (1)–(4) bekezdés

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. [939] 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.[940]

VI.4.4.2 Elkövetési tárgy és a bűncselekményi alakzat elkövetési magatartásai

Az információs rendszer vagy annak bármely eleme, valamint az információs rendszer szempontjából releváns adat.[941]

Magukban foglalják az adatok jogosulatlan bevitelét a rendszerbe, az információs rendszerben tárolt adatok módosítását, törlését vagy hozzáférhetetlenné tételét, illetve bármely más olyan 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.[942]
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.

---

[939] Btk. 375. § (5)–(6)

[940] 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.

[941] Btk. 459. § (1) bekezdés 15.

[942] Szomora, Zsolt. "A vagyon elleni bűncselekmények." p 811.

VI.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.[943]

VI.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 cselekmény megvalósulásának helye (pl. a terminál vagy szerver fizikai helye) vagy a bekövetkezett kár helye, mindkettő megalapozhatja a magyar Btk. területi hatályát.[944]

VI.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.

VI.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)

[943] Ibid., 811.o

[944] Btk. 3.§

bekezdése által meghatározott bűncselekmény kategóriájába, tehát nem minősül bűncselekménynek.[945]

VI.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 érinti [946]. 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.[947]

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.

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) bankszámla-tulajdonos, 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

[945] Szomora, Zsolt. "A vagyon elleni bűncselekmények." p. 812.

[946] Btk. 459. § (1) bekezdés 20.

[947] Btk. 375. § (6)

meg, vagy érintéses fizetéskor, ahol bizonyos összeghatár alatt nem szükséges PIN-kód bevitel.[948]

Az elektronikus készpénz-helyettesítő fizetési eszközzel való visszaélés bűncselekményének alapja a kár bekövetkezése. Ezen bűncselekmény befejezettként 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 eszköz hamisságát. A bűncselekmény általában jogtalan haszonszerzési szándékkal követik el, de ez nem kötelező elem, így eshetőleges 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 tekinthetőek 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. Ezen kívül, ha a fizetési eszköz használatával egyidejűleg több

[948] 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.

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.[949]

Összefoglalva a jelenleg hatályos Büntető Törvénykönyv szabályozása a személyes adatok védelme és az információs rendszerekkel kapcsolatos tényállások tekintetében összhangban áll az uniós jogi előírásokkal. A keretrendszert 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 ismertettem a szakirodalmi álláspontokat, különös tekintettel, a személyes adatokkal való visszaélésre vonatkozó tényállásra. A GDPR és az Infotv. szerint a személyes adat minden olyan információ, amely egy természetes személlyel kapcsolatba hozható A bírói gyakorlatban azonban vitatott kérdés, hogy az azonosíthatóság milyen kritériumok alapján határozható meg. A BH 2019.272 számú kúriai döntés (jelentős szakmai vitát váltott ki, különösen az „azonosított” és „azonosítható” fogalmak kapcsán.

Az azonosított személy az, akit egyértelműen be lehet azonosítani egy adott információ alapján, míg az azonosítható személy esetében már az a lehetőség is elegendő, hogy a rendelkezésre álló adatok felhasználásával azonosításra kerülhet. A személyes adatokat érintő bűncselekmények esetében ez a megkülönböztetés meghatározza a büntetőjogi tényállás alkalmazhatóságát.

A személyes adattal visszaélés tényállása, bizonyos bűncselekmények, például a tömeges profilalkotás vagy deepfake manipulációk esetében nem nyújt egyértelmű szabályozást.

A digitális térben elkövetett adatvédelmi bűncselekmények szorosan összefonódnak az információs rendszerek elleni bűncselekményekkel. A Btk. 423–424. §-ai szabályozzák az információs rendszer és adat megsértését, valamint az információs rendszer védelmét biztosító

[949] Szathmáry Zoltán: "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése II.

technikai intézkedések kijátszását. E tényállások egyaránt alkalmazhatók adathalász támadásokra, jogosulatlan hozzáférésekre és az információs rendszerekbe való behatolásokra. Azonban felmerülő jogértelmezési probléma, hogy a Btk. nem rendelkezik egyértelműen a szociális manipulációval elkövetett támadások (social engineering) vagy a deepfake-technológia által generált visszaélések büntetőjogi megítéléséről.

A kutatás során vizsgáltam az adatbiztonság fogalmának büntetőjogi relevanciáját is. A hatályos Infotv. szerint az adatkezelő és az adatfeldolgozó köteles olyan technikai és szervezési intézkedéseket hozni, amelyek biztosítják az adatok biztonságát. A Btk. 423. §-a szerinti tényállás, amely az információs rendszerek akadályozását szabályozza, nem korlátozódik kizárólag az informatikai műveletekre, hanem fizikai beavatkozásokat is magában foglalhat, például egy szerverterem hűtőrendszerének megrongálását. Ez alátámasztja, hogy az információs rendszerek elleni támadásokat szélesebb körben kell értelmezni, mint pusztán szoftveres beavatkozásokat. Jelenleg ez a Btk. 371. §, azaz a rongálás tényállásához kapcsolható.

Megállapítható, hogy a személyes adatokkal kapcsolatos bűncselekmények és az információs rendszerek elleni támadások tényállásai összességében megfelelnek az uniós keretrendszernek. A GDPR Preambulum 149. pontja ugyan nem ír elő közvetlen büntetőjogi szankciókat, azonban lehetőséget biztosít arra, hogy a tagállamok büntetőjogi eszközökkel is biztosítsák az adatvédelmi normák betartását Azonban bizonyos új típusú bűncselekmények esetében szabályozási hiányosságok tapasztalhatók, úgy, mint a deepfake-technológiával kapcsolatos visszaélések, a tömeges személyiségprofilozás és biometrikus adatkezeléssel kapcsolatos visszaélések és a szociális manipulációs technikák (social engineering) és az adathalászat egyes formáinak eltérő jogi megítélése terén.

Álláspontom szerint a bírói ítélkezési gyakorlat döntő szerepet fog játszani az információs rendszer elleni bűncselekményekkel kapcsolatos pontos jogértelmezés kialakításában.

VII. Összefoglalás - Eredmények

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. Ezt követően részletesen bemutattam a 2016/680/EU irányelv tartalmát és annak nemzeti jogba történő átültetésének sajátosságait Magyarország, Németország, Franciaország és Svédország jogrendszerében.

A bűnügyi célú adatkezelések kapcsán feltárt problémakörök elemzése során kitértem a nyomozás, a vádeljárás és a büntetés-végrehajtás adatkezelési vonatkozásaira, továbbá áttekintettem a személyes adatok védelmének megsértéséhez kapcsolódó büntetőjogi szankciókat szabályozó jogszabályi kereteket. Elemeztem továbbá, a digitális térben elkövetett bűncselekmények és az adatvédelem közötti összefüggéseket, különös hangsúlyt fektetve a személyes adatok védelmének jelentőségére.

VII.1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése

Az adatvédelem fogalmát illetően, annak gyakorlati szempontú megközelítését tartottam fontosnak, figyelembe véve az értekezés során vizsgált szempontokat.
Ennek megfelelően a személyes adatok védelmét gyakorlati szempontú megközelítéssel definiáltam. A személyes adatok védelme ebben a megközelítésben 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.
Ezzel a harmadik generációs szabályozás által is megjelenített adatkezelői szempontú megközelítéssel vizsgáltam a jogszabályok által meghatározott illetékes hatóságok szerepét, úgy, mint a nyomozó hatóságok, bíróságok és a büntetés-végrehajtás szerveit.

VII.2 Első hipotézisemmel kapcsolatos eredmények áttekintése - A Bűnügyi Adatvédelmi Irányelv jogharmonizációja

Ismertettem a bűnügyi adatvédelmi irányelvet ennek tagállami jogharmonizációját, a szabályozással kapcsolatos szakirodalmi álláspontokat és az egyes értelmezési kérdéseket illetően EUB ítélkezési gyakorlatát. A jogirodalomban az irányelv számos értelmezése és bemutatása lelhető fel.[950]
Áttekintettem az Európai Bizottságnak a bűnüldözésben érvényesítendő adatvédelemről szóló irányelve alkalmazásáról és működéséről szóló jelentéseit, valamint az Állampolgári Jogi, Bel- és Igazságügyi Bizottság megbízásából készült tanulmányt, amely a bűnüldözésben

[950] Lásd: 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

érvényesítendő adatvédelemről szóló irányelv végrehajtásának kritikai értékelését tartalmazta.[951] 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.

VII.2.1. Az egyes tagállami átültések 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.[952]

A magyar szabályozás ezen elvek mentén, az információszabadságról 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, biztosítva egyrészt a GDPR közvetlen érvényesülését, másrészt az irányelvi szabályozás átültetését. Az Infotv. megtartotta a korábbi magyar szabályozás alaptörvény által meghatározott, uniós jog által nem szabályozott területének e törvény általi szabályozását.

Németországban, hat évvel a hesseni 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, és egyúttal implementálták az EU 2016/680 rendeletét.

Franciaország a jogharmonizáció során 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 Módosító törvénnyel - Loi n° 2018-

[951] Lásd: Vogiatzoglou, 2022

[952] Lásd: Palánkai, 2019

493 – együttesen ültette át a francia jogba a bűnügyi adatvédelmi irányelvet és egyben határozta meg általános adatvédelmi rendelet közvetlen hatályosulását direkt hivatkozásokkal. 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 irányelvét 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 GDPR közvetlenül hatályosul, az irányelv átültetésnek szabályait módosító törvény tartalmazta. 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.

VII.2.2 Az egyes nemzeti szabályozások összehasonlítása az Irányelv alapján

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 megfelelőségi értékelés szerint a tagállamok az irányelv bevezetésekor vagy módosították meglévő adatvédelmi törvényeiket, vagy azokat hatályon kívül helyezve, új, horizontális adatvédelmi jogszabályokkal helyettesítették.

Az összehasonlítás során megállapítható eltérések a tagállami gyakorlatban általában többlettartalmak, vagy kiegészítések, melyek a korábbi jogszabályaikban is szerepeltek.

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 az EU) 2016/680, 2. cikk (1) és (12)–(14) preambulumbekezdés alapján.

Ami az Infotv. hatályát illeti, a korábbi magyar szabályozásnak megfelelően „*a törvény szabályai továbbra is az Alaptörvény VI. cikkében biztosított mindkét alapjog, a személyes adatok védelméhez fűződő jog (információs önrendelkezési jog) és a közérdekű adatok megismeréséhez és terjesztéséhez fűződő jog (információszabadság) érvényesüléséhez szükséges rendelkezéseket rögzítik a magyar joghatóság alá tartozó személyesadat- és közérdekűadatkezelések vonatkozásában*".[953]

A magyar joggyakorlatban tehát, az Infotv. kiterjesztette a törvény hatályát a nemzetbiztonsági- és honvédelmi célú adatkezelésekre is, Infotv. 2. § (3) bekezdése szerint *„az Infotv. előírásainak teljességét rendelte el alkalmazni"*

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- es 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

[953] Lásd. Sziklay,2018

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.

Álláspontom szerint – és ez jól látható a magyar jogirodalomban az Infotv. hatályának értelmezésekor - ezek a többlettartalmak nem ellentétesek az irányelvvel, ha a szabályozást megtartva kiegészítik azt.

A hatály tekintetében a GDPR-tól való elhatárolás sem egyértelmű - a Bizottság jelentése szerint - elsősorban egyes közigazgatási egységek nem bűnüldözési célú, például pénzügyi információs adatkezelését is az irányelv hatálya alá sorolják.

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 Integritásvédelmi 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. A NAIH bírósági pert indíthat [Infotv. 64. szakasza (1)], a német BfDi is rendelkezik a GDPR 58. cikk (5) bekezdésében említett hatáskörökkel. (BDSG 16.§.) A francia CNIL haladéktalanul tájékoztatja meghatározott feltételek esetén az ügyészséget [Loi, n°78-17 8.

cikk. f)] a büntetőeljárási törvénykönyv (Code de procédure pénale) 40. cikkében foglalt minden olyan bűncselekményről vagy szabálysértésről, amelyről tudomást szerzett, és előterjesztheti észrevételeit a büntetőeljárásban. A svéd IMY - nek bár szankciós jogkörrel rendelkezik, nincs perindítási eljárási képessége. (SFS 2018:1177 5. ch.7.-8.§)

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 8.7. 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 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.§), (Informatiq. 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 információtípusokat, amelyeket a naplóknak tartalmazniuk kell. A magyar, a német, a francia és svéd szabályozás is rögzíti ezeket. [Infotv.25/E.§ és 25/F.§], (BDSG 76.§), (Informatiq. 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.[954] 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 nemzeti jogszabályok vizsgálatakor. A bűnüldözési célú adatkezelések uniós szabályozása ugyanakkor egyrészt nem rendeleti formában, hanem irányelvi megfogalmazás keretei között jött létre, ami tág mérlegelési jogkört biztosított a tagállamok részére saját nemzeti jogszabályaik kialakítására. Másrészt, a tagállami átültetés vizsgálata során az általam vizsgált országok gyakorlatában egyértelműen megállapítható, hogy a történeti jogfejlődésük hagyományai, az adatvédelmi korábbi jogszabályaik és az alaptörvényeik szabályozása a meghatározó az átültetés gyakorlatában, és az eltérések oka ebben keresendő.

Egyes eltérések esetén - mint például az érintetti joggal kapcsolatosan a hozzáférési jog értelmezése esetén Franciaország gyakorlatában – kérdéses az összhang a LED-l, vagy a közös kapcsolattartási pont németországi hiányzó szabályozása esetében, mivel az eltérő értelmezés például a nemzetközi adattovábbítások esetén megfelelőségi problémát jelenthet.

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

[954] Lásd: Dimitrova, De Hert, 2018

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
A kritikus területeken azonban a megfelelőséget illetően az EDPS, és az EDPB szabályozás ad iránymutatást, vagy kötelező érvényű szabályozást. A többlettartalmak esetében, ahogy az a hatály esetében is látható, a megfelelőség biztosított.

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, úgy, mint a személyes adatok különleges kategóriái, valamint az automatizált döntéshozatal kérdésköre. Az EDPB és EDPS által kialakított gyakorlat és a kötelező érvényű döntések képesek a technikai fejlődés által megkívánt kiegészítéseket a szabályozási folyamatba „kívülről” beépíteni. Ennek alapján első hipotézisemet elfogadom.

VII.3 Második hipotézisemmel kapcsolatos eredmények áttekintése - Bűncselekményekhez kapcsolódó személyes adatok védelme a büntetőeljárás és a büntetés-végrehajtás során

VII.3.1 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.[955]
Elemeztem a bűncselekményekhez kapcsolódó személyes adatok védelmét a büntetőeljárás során, különös tekintettel az érintettek kategóriáinak megkülönböztetésére.

[955] Lásd: Kőhalmi,2013

Az adatvédelmi szabályoknak való megfelelést az eljárás különböző szakaszaiban, a Büntetőeljárásról szóló törvény szabályozását figyelembe véve vizsgáltam.[956] (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.

Kiemelt figyelmet fordítottam a tárgyalás nyilvánosságának és a zárt tárgyalásnak az adatvédelemmel kapcsolatos kihívásaira, valamint az ügyiratok zártan történő kezelésének problémáira. Bemutattam a tárgyalás nyilvánosságának elvéből és a természetes személyek adatainak védelméről szóló jogszabályokból eredő lehetséges konfliktusokat.[957]

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.

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 szükséges 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)].

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 – a személyes adat védelméhez az elengedhetetlenül szükséges, a Be. szerinti „erkölcsi okból” [Be. 436.§. (4) a)] elrendelheti a zárt tárgyalást.[958]

[956] Lásd: Hesz, Kőhalmi 2009, Pálvölgyi 2014, Németh 2019, Róth 2021, Mándi 2023

[957] Lásd: Cséka 2007, Petrik 2009, Erdei 2011, Navratil 2011, Varga 2018, Németh 2019, Kőhalmi 2023, Márki 2023

[958] Lásd: Mándi,2023

Tekintettel arra, hogy az erkölcsi okra való hivatkozás általában nem fedi le az adatvédelem fogalomkörét, 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 segítés 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 véleményem szerint az eljárás ügyszámának önmagában történő kifüggesztése biztosíthatja az érintettek személyes adatainak védelmét.[959] 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).

Ehhez kapcsolható a sajtónyilvánosság kérdése is. A bírósági eljárások során kialakított ítéletek nyilvános kihirdetése egyrészről a társadalmi normák érvényesítését szolgálja az elkövetőkkel szemben, másrészről 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

[959] Lásd: Mándi 2023, Németh,2023

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, [960] ami figyelmen kívül hagyja az elítéltek jogát a büntetett előélethez 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.[961]

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-szolgáltatónak meg kell őriznie az emberi méltóságot a közvetített tartalmakban.[2010. évi CIV.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

[960] Lásd: Németh 2019, Kőhalmi 2023, Márki 2023

[961] Lásd: Havasiné 2017, Márki 2023, Kőhalmi 2023

médiatartalmak alapvető szabályairól szóló törvény általános elveivel. Képi-és hangeszközök használata esetére is vonatkoztatható ez megállapítás.
A fentiek alapján a második hipotézisem büntetőeljárással kapcsolatos részét elfogadom.

VII.3.2. A bűncselekményekhez kapcsolódó személyes adatok védelme a büntetés-végrehajtás során

A büntetésvégrehajtás adatvédelmi vonatkozásaival kapcsolatban részletesen bemutattam a vonatkozó jogszabályok adatkezeléssel kapcsolatos rendelkezéseit, a 2013. évi CCXL. törvény (Bvtv.) alapján, a 2013. évi CCXL. törvény (Bvtv.) alapján, és a 2009. évi XLVII. törvény (Bnytv)alapján.
Vizsgáltam a mesterséges intelligencia alapú adatkezelések problémáit a büntés-végrehajtásban. A büntetés-végrehajtásban egyre nagyobb szerepet kapnak az MI-alapú rendszerek, amelyek új adatvédelmi kockázatokat vetnek fel, úgy, mint a személyes adatok bizalmas kezelése, az adatok szükségtelen gyűjtése és tárolása, valamint a diszkrimináció lehetősége

VII.3.2.1 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 büntetés-végrehajtás 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 büntetés-végrehajtás során a rendőrség is jogosult az érintettek adatainak kezelésére, tekintettel arra, hogy az általuk foganatosított 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.] Bizonyos esetekben 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.§)

VII.3.2.2 A fogvatartottak személyes adatainak védelme a 1995. évi CVII. (Bvsztvv.) 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 fogva tartás körülményeinek, biztonságának biztosítása, a fogvatartottak társadalmi reintegrációjának elősegítése, munkaerő-piaci reintegrációjuk, egészségügyi ellátásuk, logisztikai menedzselésük, valamint az adatkezelésük szabályozása és felügyelete. [Bvsztv4.§.g)] A Bvsztv. rendelkezik a fogvatartottak és kapcsolattartóik nyilvántartásáról, a sértett és kapcsolattartóik nyilvántartásáról.(Bvsztv. 28. § - 29.§)
A büntetés-végrehajtási rendszeren belül a személyes adatok integritásának megőrzése kiemelt fontosságú, melyen belül hangsúlyt kapott a nemzetközi adattovábbítás kérdése. [Bvsztv. 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. [Bvsztv.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"* [Bvsztv.29/A.(4)]. Az adattovábbítás nem érintheti a sértettel kapcsolatos adatokat.[Bvsztv. 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.§).

VII.3.2.3. Mesterséges intelligencia alapú rendszerek a büntésvégrehajtásban

Ismertettem a büntésvégrehajtásban hazánkban használatos mesterséges intelligencia alapú rendszereket.[962] Ezzel kapcsolatban felhívtam a figyelmet arra, hogy az AI alapú rendszerek, mint a SAFE, Navigator és KIOSZK, adatvédelmi kihívásokat vetnek fel, különösen a személyes adatok nagy mennyiségű kezelése és azok biztonsága kapcsán. Az AI alapú rendszerek adatvédelmi problémái közé tartozik a személyes adatok bizalmas kezelése, az adatok szükségtelen gyűjtése és tárolása, valamint a diszkrimináció lehetősége [963].

Az AI 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.[964] Adatkezeléskor csak hiteles, megbízható forrásból

[962] Lásd: Hinkel, 2020

[963] Lásd: Schmehl, 2020, Mezei 2022, Eszteri, Péterfalvi 2022, Herke 2023

[964] Marquenie, Thomas, and Katherine Quezada-Tavárez. "Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing." In *Security Technologies and Social Implications*, szerkesztette Garik Markarian, Ruža Karlović, Holger Nitsch, és Krishna Chandramouli, 32–60. Hoboken, NJ: Wiley, 2022. https://doi.org/10.1002/9781119834175.ch2.

származó adatok használata lehetséges, készen állva a nemzetközi bűnügyi vonatkozásokkal kapcsolatos AI-adatigénylések támogatására.[965]

A büntetés-végrehajtás területén a személyes adatok kezelésével kapcsolatos jogi keretek véleményem szerint megfelelő védelmet biztosítanak az érintettek személyes adatait illetően, a GDPR és az Infotv. szabályainak az ágazati jogszabályok megfelelnek. 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.

Az adatvédelmi jog megsértéseinek vizsgálata során számos esetben tapasztalható, hogy a jogellenes adatkezelés oka gyakran az adatkezelés jogalapjának hiánya, az arányosság és a szükségesség elveinek megsértése. (NAIH 2020,2021,2022 éves beszámolók).Ezek a problémák számos területeken jelentkeznek, kezdve a büntetőeljárások és a büntetés-végrehajtás során keletkezett adatok jogosulatlan hozzáférésétől az egészségügyi adatok kezeléséig. Az adatbiztonság kérdése szintén kiemelt figyelmet érdemel, hiszen az adatkezelés során a technikai és szervezési intézkedések elégtelensége jelentős kockázatot jelenthet az érintettek személyes adatainak védelmére. Az esetek elemzése rávilágít arra, hogy az adatvédelmi elvek és jogok érvényesítése kulcsfontosságú a jogellenes adatkezelések megelőzése érdekében. Az adatkezelőknek biztosítaniuk kell az adatkezelés jogalapját, tiszteletben kell tartaniuk az arányosság és a szükségesség elveit, valamint megfelelő adatbiztonsági intézkedéseket kell hozniuk. Ezen túlmenően, az érintettek jogainak tiszteletben tartása – mint az adathoz való hozzáférés, a tájékoztatáshoz való jog és a jogorvoslati lehetőségek – elengedhetetlen a jogellenes adatkezelések elkerülése érdekében.

A fentiek alapján a második hipotézisem büntetés-végrehajtásra vonatkozó részét elfogadom.

VII.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.[966]

[965] Lásd: Nagy, Z. 2021

[966] Lásd: Porcedda 2012, Bederna,2018, Moore, Anderson 2019, Wicki-Birchler 2020, Schreiber 2021, Hirvonen 2022

A GDPR és a LED szabályozásai mellett a kiberbiztonság megerősítésében kiemelt szerepet játszik az (EU) 2022/2555 irányelv (NIS2) is, amely a hálózati és információs rendszerek biztonságának növelése érdekében további követelményeket támaszt a tagállamok és az érintett szervezetek számára. A kiberbiztonsági és adatvédelmi követelmények egyre inkább összefonódnak, különösen a biztonsági intézkedések, az incidenskezelési eljárások, valamint a digitális infrastruktúrákat érintő auditok és ellenőrzések tekintetében. Az adatvédelmi szabályozás kiberbiztonságot erősítő hatásai az alábbiakban foglalhatók össze:

1. Proaktív védelem és beépített adatvédelem elve: A GDPR a beépített és alapértelmezett adatvédelem elvét (privacy by design and by default) alkalmazza, amely megköveteli, hogy az adatvédelmi szempontokat már az információs rendszerek tervezési fázisában figyelembe vegyék. Ennek érdekében a következő intézkedések kiemelten fontosak:
    - Titkosítás alkalmazása az adatok tárolása és továbbítása során.
    - Hozzáférés-szabályozás és a legkevesebb jogosultság elve (least privilege principle) alkalmazása.
    - Az adatok integritásának biztosítása a jogosulatlan módosítások vagy manipulációk ellen.

    Ezek az intézkedések csökkentik a jogosulatlan hozzáférés és az adatlopás kockázatát, ezzel erősítve a személyes adatok biztonságát (GDPR, Preambulum (8), 47. cikk d)).
2. Adatminimalizálás és célhoz kötött adatkezelés: A GDPR és a LED az adatminimalizálás elvét is előírja, amely kimondja, hogy csak a feltétlenül szükséges adatok gyűjthetők és tárolhatók, és azokat csak meghatározott, világos és jogszerű célokra lehet felhasználni. Ez az elv különösen fontos a nagyszabású adatszivárgások és adatlopások megelőzése szempontjából. (GDPR, 5. cikk c).
3. Adatvédelmi hatásvizsgálatok és kockázatelemzés: A GDPR kötelező adatvédelmi hatásvizsgálatot (DPIA) ír elő minden olyan adatkezelés esetén, amely magas kockázatot jelenthet az érintettek jogaira és szabadságaira. Ez különösen igaz, nagy mennyiségű személyes adat kezelése esetén, különleges kategóriájú adatok (pl. egészségügyi adatok, biometrikus adatok) feldolgozásakor és az automatizált döntéshozatali rendszerek és profilalkotás alkalmazása során.

    Az adatvédelmi hatásvizsgálat lehetővé teszi a kiberbiztonsági kockázatok előzetes azonosítását és kezelését, ezáltal megelőzve a potenciális adatvédelmi incidenseket. (GDPR, 35. cikk).

4. Hozzáférés-vezérlés és felhasználói jogosultságok kezelése: Mind a GDPR, mind a LED szigorú követelményeket állapít meg a személyes adatokhoz való hozzáférés kezelésére:
    - Az adatokhoz való hozzáférést korlátozni kell azokra a személyekre, akiknek az munkaköri feladataik ellátásához szükséges.
    - Többszintű azonosítás és hitelesítés alkalmazása az adatok védelme érdekében.

    A megfelelő hozzáférés-kezelés csökkenti a belső visszaélések és a külső jogosulatlan behatolások kockázatát. (GDPR, Preambulum (73), 15. cikk).
5. Incidenskezelési kötelezettségek és értesítési protokollok: A GDPR kötelezővé teszi, hogy az adatkezelők és adatfeldolgozók minden adatvédelmi incidenst megfelelő módon kezeljenek és bejelentsenek az illetékes hatóságoknak: Az adatvédelmi incidenseket 72 órán belül be kell jelenteni az illetékes adatvédelmi hatóságnak. Ha az incidens magas kockázatot jelent az érintettekre nézve, akkor őket is tájékoztatni kell.
    Ez az előírás hatékony eszközt biztosít a kibertámadások által okozott károk enyhítésére és az érintettek védelmére. (GDPR, Preambulum (49), (85) – (88), 33. cikk).

A GDPR és a NIS2 Irányelv kapcsolata: A NIS2 Irányelv számos olyan kiberbiztonsági követelményt ír elő, amelyek összhangban állnak a GDPR előírásaival:

- Biztonsági intézkedések és auditok végrehajtása.
- Incidenskezelési protokollok kialakítása és gyors válaszlépések biztosítása.
- Adatkezelési szabályzatok és szerződések felülvizsgálata az adatbiztonság érdekében.

A NIS2 Irányelv a GDPR kiegészítő szabályozásának is tekinthető, amely új kötelezettségeket vezet be a digitális szolgáltatók és kritikus infrastruktúrák számára.[967] A GDPR és a NIS2 együttes alkalmazása integrált kiberbiztonsági és adatvédelmi rendszert hoz létre, amely hatékonyabb védelmet nyújt az egyre növekvő kibertámadásokkal szemben.

Megállapítható, hogy az adatvédelmi jogszabályok jelentős szerepet játszanak a kiberbűnözés elleni küzdelemben. A GDPR és a LED előírásai nemcsak az adatkezelés jogszerűségét biztosítják, hanem a személyes adatok védelmén keresztül közvetlenül hozzájárulnak az internetes bűncselekmények kockázatának csökkentéséhez is.

[967] Lásd: Cole, Schmitz 2019

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 viszonylatában, 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 hoztak a szervezetek incidenskezelési folyamataiban. A NIS 2 Irányelv ebben az értelemben kiegészíti az adatvédelmi szabályokat.
A fentiek alapján megállapítható, hogy az adatvédelmi jogszabályoknak fontos szerepe van a kiberbűnözés elleni küzdelemben, így a harmadik hipotézisemet elfogadom.

VII.5. Negyedik hipotézisemmel kapcsolatos eredmények áttekintése - A személyes adatokkal kapcsolatos és az információs rendszerrel kapcsolatos bűncselekmények

VII.5.1. Személyes adatokkal kapcsolatos tényállások

A személyes adatok védelme alapvető jog, amely az információs önrendelkezés jogából ered, és az emberi méltóság védelmén alapul. Az Alkotmánybíróság 15/1991. (IV. 13.) határozata, valamint az Alaptörvény VI. cikkének (2) bekezdése is elismeri ezt a jogot, amely mindenki számára biztosítja személyes adatainak védelmét[968] A személyes adatok védelme azonban nemcsak alapjogi kérdés, hanem büntetőjogi is, amely a visszaélésekkel szemben nyújt védelmet.

A személyes adatokkal való visszaélés bűncselekményét a Büntető Törvénykönyv (Btk.) XXI. fejezete szabályozza, az emberi méltóság elleni bűncselekmények között. A visszaélés tényállása úgynevezett keret diszpozíció, vagyis a büntetőjogi megfogalmazás a GDPR (általános adatvédelmi rendelet) és más külső jogszabályok elveire épül.[969]. Ha a személyes adatokat a GDPR előírásainak megsértésével kezelik, az büntetőjogi felelősséget

[968] Lásd: Eszteri, Péterfalvi, 2017

[969] Lásd: Belovics et al., 2014; Péterfalvi, Eszteri, 2017

vonhat maga után, míg ha a GDPR nem alkalmazható, például nemzetbiztonsági célból történő adatkezelésnél, akkor az Infotv. szabályai érvényesek.[970]

A Btk. 219. § a személyes adattal való visszaélést szabályozza. A bűncselekménynek sem passzív alanya, sem elkövetési tárgya nincs, tekintettel arra, hogy a személyes adat eszmei kategória. E jogi megközelítés szerint, mellyel egyetértek, a személyes adat elvont fogalom, amelynek tárgya az érintettre közvetlenül vagy közvetetten vonatkozó információ, azaz a személyes adat. Így nem tekinthető a bűncselekmény tárgyának, különös tekintettel arra, hogy azok igazságtartalmuktól függetlenül kapcsolatba hozhatók az adott személlyel[971]. Más szerzők szerint viszont a személyes adat maga is lehet a bűncselekmény tárgya, ha annak kezelése jogellenesen történik.[972]

A személyes adatok kezelésére vonatkozó alapelveket a GDPR és az Infotv. rögzíti, amelyek között kiemelt szerepű a jogszerűség, a célhoz kötöttség és az adattakarékosság. A személyes adatokkal való visszaélés három elkövetési formája: (1) jogosulatlan vagy céltól eltérő adatkezelés, amely aktív elkövetési magatartásként jelenik meg; (2) a biztonsági intézkedések elmulasztása, amely mulasztással valósul meg; és (3) a tájékoztatási kötelezettség megszegése, amely utóbbi kettő, kizárólag a jogszerű adatkezelőket terheli (GDPR 32. cikk; Infotv. 25/I. §; GDPR 13–14. cikk; Infotv. 15–16. §). 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 aktusaiban foglalt előírásokat megsértve nem ad megfelelő tájékoztatást az érintett személy hozzáférési jogának gyakorlásához, [Btk.219 (2)] és ezzel súlyosan sérti más személyek érdekeit.[973]

A személyes adat fogalmának meghatározásához elengedhetetlen az „azonosított vagy azonosítható személy” értelmezése. E fogalom az adatokat olyan személyekhez köti, akik valamilyen módon azonosíthatók, ami a személyes adatok jogi védelmének alapját képezi. Az adat akkor személyre vonatkozó, ha legalább egy szempont a következő háromból – tartalom, cél vagy eredmény – kapcsolódik az érintetthez.[974].Az azonosíthatóság kérdésénél nemcsak az adatkezelő szándéka fontos, hanem az is, hogy az ügy minden körülménye alapján feltételezhető-e az azonosítás valószínűsége.[975]

---

[970] Lásd: Jóri, 2018

[971] Lásd: Szomora 2014,2019

[972] Lásd: Békés, 2016; Péterfalvi, Eszteri, 2017; Horváth, 2020; Gál A., 2020; Belovics, 2021

[973] Lásd: Gál A. 2020

[974] Lásd: Pók, 2019

[975] Lásd: Czapáry, Szőke, 2022

A személyes adat fogalmának büntetőjogi értelmezése különösen fontos az új technológiák, például a tömeges profilalkotás, kiskorúak védelme vagy deepfake alkalmazások esetén, ahol a személyes adattal való visszaélés jogi tényállása gyakran nem nyújt elegendő védelmet.[976]
Az azonosíthatóság különbséget jelent az érintett elkülöníthetősége és konkrét személyazonossága között. Előbbi az érintett megkülönböztetését jelenti a környezetétől, míg az utóbbi esetében pontosan meghatározható, ki az adott személy.
Noha a GDPR közvetlenül alkalmazandó az Európai Unióban, nem ír elő kötelező büntetőjogi védelmet a személyes adatokra vonatkozóan, de lehetőséget biztosít a tagállamoknak, hogy büntetőjogi szankciókat vezessenek be a rendelet megsértése esetére (EU 2016/679 Preambulum (149)). A magyar jogrendszerben a Btk. 465. § (2) d) pontja az EU jogának betartása keretében utal a személyes adatok védelmére, de nem ad konkrét definíciót a személyes adatfogalmát illetően.

A magántitok (Btk. 223. §) és a levéltitok megsértése (Btk. 224. §) szintén a személyes adatokhoz kapcsolódó bűncselekmények, amelyek a személyes adatok védelmén túl a magánszféra egyes részleteit is védelmezik. A magántitok megsértése a személyhez köthető, jogellenesen nyilvánosságra hozott információkra vonatkozik, amelyek az érintett érdekeit veszélyeztethetik (BH. 2004.170 f). A levéltitok megsértése pedig csak akkor kerül alkalmazásra, 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.

Összefoglalva, a Büntető Törvénykönyv - a GDPR mint keretjogszabály alapján - szabályozása óvja az érintettek alapvető jogait, különös tekintettel az emberi méltóságra és az információs önrendelkezésre. A modern technológiai kihívások – mint a tömeges profilalkotás vagy a deepfake – miatt azonban szükséges lehet a szabályozás továbbfejlesztése, hogy megfelelő védelmet biztosítson az érintetteknek.

VII.5.2.Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

Az informatikai bűncselekmények a Büntető Törvénykönyvben (Btk.) külön fejezetben kerültek szabályozásra, megfelelve az Európai Unió 2013/40 irányelvének, amely az információs rendszerek elleni támadásokra fókuszál. Az irányelv átültetése terminológiai változásokat hozott magával, mint például a „számítástechnikai rendszer” fogalom

[976] Lásd: Miskolczi, Szathmáry, 2019

„információs rendszer” terminológiára cserélését. Háttérjogszabályként érvényesül még, az Európai Tanács 2004. évi LXXIX. törvénnyel kihirdetett ún. Budapesti Egyezménye. Szükséges volt 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.[977]

A szabályozás alá tartozó cselekmények között szerepel a tiltott adatszerzés (Btk. 422. §), az információs rendszer vagy adat megsértése (Btk. 423. §), valamint a védelmi intézkedések kijátszása (Btk. 424. §), amellyel a Btk., a Tiltott adatszerzés és információs rendszer elleni bűncselekmények (XLIII. fejezet) címszó alatt foglalkozik.

Az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) külön tényállásként jelenik meg a vagyon elleni bűncselekmények körében, hangsúlyozva ezzel a digitális térben történő bűncselekmények súlyát és jelentőségét.

A tiltott adatszerzés jogi tárgya az egyének személyes adatai, magántitkai, üzleti és gazdasági titkai védelmét célozza. A jogszabály meghatározza az első alapeset elkövetési magatartásait, beleértve a titkos helyiségek átkutatását, a zárt küldemények jogosulatlan felbontását, valamint az elektronikus hírközlő hálózatokon keresztül továbbított adatok illetéktelen megszerzését és rögzítését. 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.[978]

Az elkövetés második alapesetében a célzat kiemelt szerepet kap, ahol a jogalkotó az információk jogosulatlan megszerzésének és felhasználásának lehetőségét a fedett nyomozók és titkosszolgálati együttműködők kilétének felderítése céljából szabályozza. A harmadik alapeset pedig az azonosított személyes adatok, magántitkok, üzleti és gazdasági titkok jogosulatlan továbbítását, felhasználását célozza meg. Ez a cselekmény különösen veszélyes, mivel az adatokat digitális vagy fizikai formában használhatják fel az elkövetők, akik gazdasági előnyök megszerzésére vagy mások érdekeinek sérelmére törekedhetnek, súlyosan sértve az

[977] Lásd: Szathmáry 2022

[978] Lásd: Karsai 2019

érintettek személyes adatokhoz és magánélethez való jogát, valamint fenyegetve az információs rendszerek integritását.[979]

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. §) magában foglalja az információs rendszerek zavartalan működésének és a bennük tárolt adatok hitelességének és bizalmasságának védelmét. Ide tartoznak a tipikus DDoS- és malware-támadások, ahol az elkövetési tárgy az információs rendszer és annak összetevői, például a számítógépek, programok és elektronikus adatok.[980]

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.[981] Álláspontom szerint a tágabb értelmezést kell elfogadni ebben az esetben.

Az elkövetési magatartások közül a második fordulat, az információs rendszer működésének jogosulatlan akadályozása [423. § (2) a)] a Btk. szövegében az Irányelv 4. cikkének átvételét tükrözi, mint „rendszert érintő jogellenes beavatkozás”. Ezzel szemben az adat törlése vagy hozzáférhetetlenné tétele [423. § (2) b)] az Irányelv 5. cikkének felel meg, amely „*adatot érintő jogellenes beavatkozásnak*” minősül.[982] Az adatok hozzáférhetetlenné tétele akkor áll fenn, amikor a jogosult személy nem tud az adatokhoz hozzáférni vagy azokat használni, például ransomware-támadások esetén. Ilyen esetekben az adatok ugyan megmaradnak, de a jogosult nem tudja őket elérni, mivel a hozzáférést technológiai úton akadályozzák meg.

[979] Lásd: Molnár 2016

[980] Lásd: Nagy 2020

[981] Lásd: Szathmáry 2022

[982] Lásd: Grund 2021

Azonban a „fizikai külső” tényezők biztosítását, és az informatikai rendszer működőképességének biztosítását is szükségesnek tartom, az alábbiak alapján: Az Infotv. előírásai szerint az adatkezelők kötelesek megfelelő műszaki és szervezési intézkedéseket alkalmazni, ideértve az adathordozók eltávolításának megakadályozását [Infotv. 25/I. § (3) b)], valamint a rendszer helyreállíthatóságának biztosítását üzemzavar esetén [Infotv. 25/I. § (3) i)], továbbá a működőképesség fenntartását [Infotv. 25/I. § (3) j)]. Ezek az elemek kiemelik, hogy a fizikai és mechanikus védelem nélkülözhetetlen a teljeskörű adatbiztonság megteremtéséhez, bár jelenleg a számítógépes rendszerek technikai védelmét a rongálás tényállása szabályozza. Mindezek alapján véleményem a fizikai tényezők által, és a rendszer működésének egyéb módon történő akadályoztatásait is a tényállás részeinek kellene tekinteni.

Az információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424. §) célja az információs rendszerek megbízhatóságának, hitelességének és titkosságának védelme. Az elkövetési tárgyak közé tartozik a bűncselekmények elkövetését elősegítő vagy lehetővé tevő eszközök és szakmai tudás, például jelszavak és számítástechnikai programok megszerzése és forgalmazása, akár a Darknet használatával, azaz a károkozói adatvisszaélés, (Btk. 375.§ /Btk 423.§). Az ilyen tevékenységeket bárki elkövetheti, aki szándékosan vesz részt ezekben.

Az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) a vagyon elleni bűncselekmények közé tartozik, és magában foglalja a jogtalan adatbevitelt, adatmódosítást, törlést vagy hozzáférhetetlenné tételt, amelyek jogtalan haszonszerzési célból történő kárt okoznak. Az információs rendszer felhasználásával elkövetett csalás ún. károkozó adatvisszaélés, és a készpénz-helyettesítési fizetési eszközzel visszaélés egyes alakzatainak összevonásával jött létre.[983] Jogi tárgya az információs rendszer vagy annak bármely eleme, valamint az információs rendszer szempontjából releváns adat.

Az elektronikus készpénz-helyettesítő fizetési eszközökkel való visszaélés, ideértve a hamis eszközök használatát, szintén ide tartozik, amennyiben az károkozó visszaélés[984]. Ez a tényállás kiegészíti a hagyományos csalás bűncselekményét, lehetővé téve, hogy az információs rendszerek útján elkövetett vagyoni károkozást, amely nem jár természetes személyek megtévesztésével, a büntetőjog szankcionálja.

Az információbiztonság elleni cselekmények nemcsak közvetlenül az információs rendszert érinthetik, hanem annak rendszerelemeit is. Az információs rendszer biztonságát közvetlenül

[983] Lásd: Szomora, 2012

[984] Lásd: Tóth D. 2019

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 minősülhetne.

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 is az uniós jogszabályoknak való megfelelésről. A GDPR Preambulum 149. pontja ugyan nem ír elő közvetlen büntetőjogi szankciókat, azonban lehetőséget biztosít arra, hogy a tagállamok büntetőjogi eszközökkel is biztosítsák az adatvédelmi normák betartását Az egyes szabályozási kérdésekkel kapcsolatban részletesen elemeztem a szakirodalmi álláspontokat, különös tekintettel, a személyes adatokkal való visszaélésre vonatkozó tényállására. Bizonyos új típusú bűncselekmények esetében szabályozási hiányosságok tapasztalhatók, úgy, mint a deepfake-technológiával kapcsolatos visszaélések, a tömeges személyiségprofilozás és biometrikus adatkezeléssel kapcsolatos visszaélések és a szociális manipulációs technikák (social engineering) és az adathalászat egyes formáinak eltérő jogi megítélése terén. Néhány értelmezési kérdést illetően a magyar jogirodalomban vannak eltérő vélemények, ezzel kapcsolatban álláspontomat indoklással együtt kifejtettem. Álláspontom szerint a bírói ítélkezési gyakorlat döntő szerepet fog játszani az információs rendszer elleni bűncselekményekkel kapcsolatos pontos jogértelmezés kialakításában.

A fentiek alapján hipotézisemet részben elfogadom, részben elutasítom.

VIII. Summary

The thesis offers an in-depth analysis of both EU and national legislation concerning the protection of personal data within the framework of the Law Enforcement Directive. It delves into the complexities of transposing the Directive into national legal systems, addressing regulatory challenges related to criminal procedures, law enforcement, and sanctions. Moreover, from the perspectives of data security and cybercrime prevention, the thesis emphasizes both legal and practical concerns surrounding the misuse of personal data and offenses against information systems.

In its introductory section, the thesis outlines theoretical foundations related to data protection, tracing the evolution of data protection law and presenting current legal frameworks safeguarding personal data. The development of data protection regulations is analyzed in the context of technological advancements and the growing significance of data in modern society. Subsequent sections provide a comprehensive analysis of Directive 2016/680/EU on the protection of personal data processed for law enforcement purposes and the harmonization process across EU Member States. The legal context surrounding investigations, prosecutions, and the enforcement of criminal law, along with national legislation governing criminal sanctions related to data protection, are explored in detail. The dissertation also scrutinizes the interconnections between digital crime and data protection, with particular focus on the significance of personal data security.

1. Practical Approach to Data Protection

Chapter II introduces the concept and historical development of data protection, followed by a detailed presentation of relevant EU legislation and its institutional framework. Data protection is approached from a practical perspective, emphasizing the safeguarding of individuals' rights and freedoms through the regulation of personal data processing conditions. This involves both the definition of self-determination rights concerning personal data and the establishment of regulatory requirements for data controllers processing such data.

Data controllers and data subjects both possess certain rights over personal data. The lawfulness of data processing activities conducted by controllers is ensured by legal instruments such as the GDPR (Regulation (EU) 2016/679, Article 6) and the Law Enforcement Directive (Directive (EU) 2016/680, Article 8), while data subjects exercise their rights through informational self-determination. The legal framework imposes restrictions on both parties, ensuring that data processing does not disproportionately infringe upon individual rights. The analysis extends to the principles of data minimization (Article 5(1)(c) GDPR), purpose limitation (Article 5(1)(b) GDPR), transparency (Article 12 GDPR), and accountability (Article 5(2) GDPR), which are critical for maintaining the balance between data processing needs and privacy rights.

For public authority data processing, including criminal data processing, the discretion of data controllers—such as law enforcement agencies—tends to prevail due to the "ultima ratio" principle of criminal law. This principle underscores the necessity of data processing activities being justified, proportionate, and strictly limited to what is essential for achieving legitimate

law enforcement objectives. The thesis examines the role and responsibilities of competent authorities, including investigative bodies, courts, and correctional institutions, as defined under third-generation data protection legislation (Szőke, 2013).

2. Research Objectives and Hypothesis Testing

Chapter III presents an analysis of the Law Enforcement Directive, its transposition into Member States' legal systems, and relevant case law from the Court of Justice of the European Union (CJEU). The chapter reviews extensive legal literature and critical analyses of the Directive's implementation (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).
Drawing on European Commission reports and studies from the LIBE Committee (Vogiatzoglou, 2022), the thesis evaluates the practical application of the Directive, focusing on Hungary, Germany, France, and Sweden. Comparative analysis highlights diverse transposition practices influenced by each country's historical and institutional data protection frameworks. Germany, Sweden, and France, as pioneers in data protection legislation, provide critical insights into the Directive's national implementation. The study also considers the impact of cultural, legal, and political differences on the interpretation and enforcement of data protection laws across these jurisdictions.

3. Key Hypotheses

Hypothesis 1: Divergences in EU Harmonization and National Legal Systems in the Field of Criminal Data Protection

In this research, I assumed that during the transposition of Directive (EU) 2016/680 by Member States, different legislative and legal practices may emerge, potentially affecting the uniformity of criminal data processing at the EU level. These divergences may arise from the specific characteristics of national legal systems, their historical development, and the data protection traditions of each Member State. The study analyzed legislative solutions in Hungary, Germany, France, and Sweden, focusing on the definition of the personal and material scope of the Directive, the purpose limitation of data processing, and the powers of supervisory authorities. Among the examined Member States, Hungary, Germany, and France implemented the Directive through amendments to their existing data protection regulations, while Sweden adopted a separate law to regulate criminal data processing.

Differences Observed in Defining the Scope of the Directive:

- Hungary: The Infotv. extends the rules of criminal data protection to data processing for national security and defense purposes, thus applying its full provisions (Infotv. Section 2(3)).
- Germany: The Federal Data Protection Act (BDSG) extends criminal data processing to include administrative offenses that do not qualify as crimes but are punishable by fines (BDSG Section 11(1), 8).
- France: Article 87 of Law No. 78-17 defines the scope of the Directive, though the 2018 amendment excluded data processing for national security purposes from its scope.
- Sweden: The Criminal Data Act (SFS 2018:1177) does not apply to data processing by the armed forces or to national security data processing handled by the police.

Divergences in the Powers of Supervisory Authorities:

- In Sweden, supervisory responsibilities are shared between the Integritetsskyddsmyndigheten (IMY) and the Swedish Security and Integrity Protection Commission.
- In Germany, state data protection officers oversee criminal data processing, while the Federal Commissioner for Data Protection (BfDi) is responsible for federal-level entities.
- In all four countries, supervisory authorities' powers to oversee data processing by judicial bodies are restricted [Hungary: Infotv. Section 38(2b), Germany: BDSG Section 9(2), France: Informatique et Libertés Article 19, Sweden: SFS 2018:1177, Chapter 5, Section 2].
-

Remedies and Rights of Data Subjects:

- Hungary, Germany, and France provide judicial remedies if supervisory authorities do not resolve complaints within three months [Infotv. Section 55(3), BDSG Section 20, Informatique et Libertés Article 108].
- In Sweden, judicial remedies are not available if the authority fails to decide within the set deadline.

The research concluded that the transposition of the Directive shows variations among the Member States. These differences primarily stem from the historical development of national

legal systems and do not always result in harmonization issues. Some divergences, such as Germany's extension of data protection to administrative offenses, reflect stricter national rules. However, inconsistencies, like France's restrictive interpretation of access rights, may limit data subjects' legal remedies. These discrepancies can particularly affect cross-border data transfers, where differing interpretations might hinder cooperation.
Based on the findings, further clarification of the Directive's implementation may be necessary, especially through enhanced cooperation between supervisory authorities and the sharing of best practices among Member States. While the Directive provides an adequate framework for criminal data protection, variations in national implementation can affect legal uniformity, warranting additional adjustments.

Hypothesis 2: Adequacy and Practical Challenges of Data Protection Regulation in Criminal Proceedings and Enforcement

I assumed that while the regulatory framework for personal data protection in criminal proceedings and enforcement is generally adequate, it may not provide comprehensive protection for certain categories of data subjects in practice. Consequently, further regulatory clarifications or practical solutions are necessary to strengthen data protection.
The primary goals of criminal proceedings are to detect crimes, hold perpetrators accountable, and remedy the harm caused by unlawful acts. Simultaneously, fundamental rights, including the right to privacy and data protection, must be upheld (Kőhalmi, 2013). Maintaining a balance between data protection and criminal proceedings presents significant legal challenges, particularly regarding the publicity of trials, handling personal data of suspects and victims, and the long-term accessibility of convicts' data.

*Assessment of Data Protection Compliance at Different Stages of Criminal Proceedings***:**

The compliance of criminal proceedings with data protection standards was examined based on the Criminal Procedure Act (Be.) and the Freedom of Information Act (Infotv.) (Kiralý 2000; Fenyvesi, Herke, Tremmel 2004; Nyíri 2018; Herke 2018; Fantoly, Budaházi 2019).
Key areas of analysis included:

- Processing of personal data of suspects, witnesses, defendants, and victims (Hesz, Kőhalmi 2009; Pálvölgyi 2014; Németh 2019; Róth 2021; Mándi 2023).

- Data protection concerns related to trial publicity and closed hearings (Cséka 2007; Petrik 2009; Erdei 2011; Navratil 2011; Varga 2018; Németh 2019; Kőhalmi 2023; Márki 2023).
- Public pronouncement of judgments and the accessibility of court records.

While legislation theoretically ensures adequate personal data protection, practical contradictions and gaps were identified, particularly concerning the protection of specific data subject categories.

Conflicts Between Trial Publicity and Data Protection:

- Public Display of Trial Schedules: Publicly listing personal data raises data protection concerns. Displaying only case numbers may suffice for data protection purposes (Mándi 2023; Németh 2023), as case numbers are considered personal data only if they can directly identify individuals (NAIH/2020/294/4).
- Ordering Closed Hearings: Be. Section 436(4)(a) allows judges to order closed hearings for moral reasons. I propose amending Section 436(4)(c) to include the protection of personal data where indispensable, considering the categories of data subjects involved.

Press Coverage and Data Protection of Convicts:

- Media coverage of trials serves public interest and maintains trust in the justice system. However, publicity must not infringe upon privacy rights.
- Public Pronouncement of Judgments**:** According to NAIH (NAIH-4418-5/2012/V), publicity should not entail unrestricted disclosure of personal data. Online court reports can affect the reintegration of convicts due to prolonged data accessibility (Németh 2019; Kőhalmi 2023; Márki 2023).

Balancing Freedom of the Press and Data Protection:

- The Press Freedom Act (Act CIV of 2010) mandates that media freedom must not violate personal rights. Media service providers should minimize published personal data, using initials or anonymization where possible.

Based on the above, I conclude that while the legal framework provides an adequate basis for data protection in criminal proceedings, practical issues necessitate regulatory refinements to ensure comprehensive protection for all data subject categories.

Data Protection Challenges in Penitentiary Systems:

In relation to data protection in penitentiary systems, this section provides a detailed overview of the relevant legal provisions concerning data management, based on Act CCXL of 2013 (Bvtv.), Act CCXL of 2013 (Bvtv.), and Act XLVII of 2009 (Bnytv).

The study examines the challenges of artificial intelligence (AI)-based data management in penitentiary environments. AI-based systems are increasingly used in correctional facilities, raising new data protection risks, such as the confidentiality of personal data, unnecessary data collection and storage, and the potential for discrimination (Schmehl 2020, Mezei 2022, Eszteri, Péterfalvi 2022, Herke 2023). The use of AI highlights the importance of conducting prior data protection impact assessments and using credible, reliable data (Nagy, 2021).

When analyzing data protection law violations, it was observed that unlawful data processing often results from the absence of a legal basis for data processing or violations of the principles of proportionality and necessity (NAIH Annual Reports 2020, 2021, 2022). These issues manifest across various areas, from unauthorized access to data generated in criminal proceedings and penitentiary systems to the handling of health data. Data security is also a critical concern, as inadequate technical and organizational measures pose significant risks to the protection of personal data.

The analysis of cases highlights that enforcing data protection principles and rights is essential to prevent unlawful data processing. Data controllers must ensure a legal basis for data processing, adhere to the principles of proportionality and necessity, and implement appropriate data security measures. Moreover, respecting data subjects' rights—such as the right of access, the right to information, and available legal remedies—is crucial to avoiding unlawful data processing.

Hypothesis 3: The Role of Data Protection Regulation in Cybersecurity and Personal Data Protection

The research hypothesized that the effective application of data protection regulations provides protection for natural persons' personal data against cyberattacks. By examining the interconnections between data protection and cybersecurity regulations, it was established that the GDPR and the Law Enforcement Directive (LED) not only guarantee the legality of data processing but also contribute directly to cybersecurity by enhancing the security of information

systems (Porcedda 2012, Bederna 2018, Moore, Anderson 2019, Wicki-Birchler 2020, Schreiber 2021, Hirvonen 2022).

In addition to the GDPR and LED, Directive (EU) 2022/2555 (NIS2) plays a key role in strengthening cybersecurity. NIS2 imposes additional requirements on Member States and relevant organizations to enhance the security of network and information systems. Cybersecurity and data protection requirements are increasingly intertwined, particularly concerning security measures, incident management procedures, and audits affecting digital infrastructures.

Key Data Protection Contributions to Cybersecurity

The research identified five key factors through which the GDPR and LED contribute to improving cybersecurity:

1. Proactive Protection and the Principle of Data Protection by Design:
   The GDPR mandates data protection by design and by default, requiring that data protection considerations be integrated into the design phase of information systems. Key measures include: Encryption for data storage and transmission, access control and the least privilege principle and ensuring data integrity to prevent unauthorized modifications.
   These measures reduce the risks of unauthorized access and data breaches, thereby enhancing the security of personal data (GDPR, Preamble (8), Article 47 (d)).
2. Data Minimization and Purpose Limitation:
   Both the GDPR and LED enforce the principle of data minimization, stipulating that only data strictly necessary for specific, legitimate purposes should be collected and stored. This principle reduces the amount of sensitive information available during cyberattacks, minimizing the risk of data misuse (GDPR, Article 5(c)).
3. Data Protection Impact Assessments (DPIA) and Risk Analysis:
   The GDPR requires DPIAs for data processing activities that pose high risks to individuals' rights and freedoms, particularly for large-scale processing, special categories of data, and automated decision-making systems. DPIAs help identify and mitigate cybersecurity risks, preventing potential data protection incidents (GDPR, Article 35).
4. Access Control and User Rights Management:
   The GDPR and LED impose strict access control requirements: Limiting data access to

individuals whose job functions require it, and implementing multi-factor authentication to protect sensitive data.

Proper access management reduces the risks of internal misuse and external unauthorized breaches (GDPR, Preamble (73), Article 15).

5. Incident Management and Notification Protocols:
   The GDPR mandates that data controllers and processors manage and report data breaches appropriately: Data breaches must be reported to the relevant authority within 72 hours and if the breach poses high risks to individuals, they must also be notified.

   These requirements provide an effective mechanism for mitigating damage from cyberattacks (GDPR, Preamble (49), (85)–(88), Article 33).

GDPR and NIS2 Directive Relationship

The NIS2 Directive introduces cybersecurity requirements aligned with the GDPR:

- Implementation of security measures and audits.
- Development of incident management protocols and rapid response mechanisms.
- Review of data processing policies and contracts to enhance data security.

NIS2 complements the GDPR by introducing new obligations for digital service providers and critical infrastructures (Cole, Schmitz 2019). The combined application of GDPR and NIS2 creates an integrated cybersecurity and data protection framework, offering robust protection against increasing cyber threats.

Based on the findings, it is clear that data protection regulations play a significant role in combating cybercrime. The GDPR and LED not only ensure the legality of data processing but also directly contribute to reducing the risks of cybercrime through the protection of personal data.

Hypothesis 4: Criminal Law Regulation of Personal Data Offenses and Information System Crimes

The research hypothesized that the criminal law provisions concerning personal data offenses and information system crimes generally align with the EU framework. However, they do not fully cover all personal data-related crimes in the digital space, particularly regarding sanctions.

It was found that Hungarian regulations are fundamentally consistent with EU legal frameworks. Nonetheless, certain digital crimes, such as mass profiling, deepfake-related abuses, and issues surrounding the online protection of minors, lack comprehensive criminal law regulation.

Foundations of Criminal Law Protection for Personal Data

Personal data protection is rooted in the right to informational self-determination, recognized as a fundamental right by the Constitutional Court's Decision 15/1991 (IV. 13.) AB and guaranteed under Article VI(2) of the Fundamental Law (Eszteri, Péterfalvi 2017).
The offense of misuse of personal data is regulated under Chapter XXI of the Criminal Code, which addresses crimes against human dignity and certain fundamental rights. Article 219 of the Criminal Code defines misuse of personal data, functioning as a framework provision supplemented by external regulations, particularly the GDPR and the Infotv. (Belovics et al. 2014, Péterfalvi, Eszteri 2017).
The goal of criminal law is to ensure data protection legality, purpose limitation, and data minimization (GDPR, Article 5(1)(a)-(c)). Violations of data processing rules can constitute criminal offenses if they breach obligations established by the GDPR or Infotv.

Interpretational Issues in Data Protection Crimes

The study highlighted interpretational challenges regarding the definition of personal data. According to the GDPR and Infotv., personal data includes any information relating to an identified or identifiable natural person [Infotv. Section 3(10)]. Judicial practice debates the criteria for identifiability, as reflected in a landmark decision by the Curia (BH 2019.272).

- Identified person: Clearly identifiable based on specific information.
- Identifiable person: Potentially identifiable using available data (Pók 2019).

In data-related crimes, this distinction affects the applicability of criminal law provisions. Current regulations lack clear provisions for crimes like mass profiling or deepfake abuses (Miskolczi, Szathmáry 2019).

Crimes Against Information Systems and Data Protection

Digital data-related crimes are closely linked to offenses against information systems. Articles 423–424 of the Criminal Code regulate breaches of information systems and circumvention of technical security measures.

Legal interpretation challenges arise concerning social engineering attacks and abuses involving deepfake technology. The analysis also addressed the criminal law relevance of data security, with the Infotv. mandating technical and organizational measures to ensure data security [Infotv. Section 25/I(1)].

Overall, while Hungarian criminal law aligns with the EU framework, gaps remain in regulating emerging digital crimes. The GDPR, while not imposing direct criminal sanctions, allows Member States to enforce data protection standards through criminal law [GDPR Preamble (149)].

Key Identified Gaps:

- Lack of explicit criminal provisions for deepfake-related abuses.
- Inadequate regulation of mass profiling and biometric data misuse.
- Inconsistent legal treatment of social engineering techniques and phishing variants.

4. Final Conclusions

The thesis concludes that while Directive 2016/680/EU provides a robust legal framework for protecting personal data in law enforcement contexts, disparities in national implementations necessitate ongoing efforts to harmonize practices. Enhanced cooperation among Member States, consistent CJEU case law, and dynamic regulatory adaptations are essential for achieving comprehensive data protection across the EU.

The research highlights the need for continuous monitoring and evaluation of data protection practices to ensure they remain effective in the face of evolving technological and legal landscapes. Recommendations include the establishment of stronger cross-border data protection mechanisms, increased support for national data protection authorities, and the promotion of best practices through EU-wide guidelines and training programs.

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. "Vagyon elleni kriminális cselekmények a modernizálódó kiskereskedelemben." Ügyészek Lapja 27, no. 1-2 (2021). ISSN 1217-7059.

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

Antal, Dániel. "A nyilvánosság és a büntetőeljárás." *Studia Iuvenum Iurisperitorium* 5 (2010): 217-271.

Arnold, Tom. "The Early Prediction of Internet Identity Theft and Its Global Impact on Cybersecurity." *Journal of Cybersecurity Research* 20, no. 2 (2022): 32.

Bäcker, Matthias., and Hornung, Gerrit. "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* 28, no. 6 (2012): 627-633.

Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld.* London: Heinemann, 2014.

Bederna, Zsolt. "Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai." *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata* 16, no. 3 (2018): 76-103.

Békés, Ádám. "Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények." In *A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja*, szerk. Polt P., Miskolczi B., Török T., és Gasz P. Budapest: Opten Informatikai Kft., 2016.

Belovics, Ervin, Gellér Balázs, Nagy Ferenc, és Tóth Mihály. *Büntetőjog I., Általános rész.* Budapest: HVG-ORAC, 2014.

Belovics, Ervin. "Az emberi méltóság és az egyes alapvető jogok elleni bűncselekmények." In *Büntetőjog II. Különös Rész*, szerk. Belovics E. Budapest: HVG-ORAC, 2021.

Bendik, Tamás. "A GDPR keletkezése és a magyar jogrendszerre gyakorolt hatása." 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, és Révész Balázs, 489-506. Budapest: Wolters Kluwer Hungary, 2021.

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: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), 2020.

Biegelman, Martin T. *Identity Theft Handbook: Detection, Prevention and Security.* Hoboken, NJ: John Wiley and Sons, 2009.

Black, Kyle D., Christina, B. Alam, Steven M. Bucher, Ashley J. Giannetti, Lauren D. Godfrey, and Justin D. Wear. “RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY.” *Tort Trial & Insurance Practice Law Journal* 54, no. 2 (2019): 403–34.

Bolognini, Luca. "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), January 10, 2020.

Brayne, Sarah. "The Criminal Law and Law Enforcement Implications of Big Data." *Annual Review of Law and Social Science* 14 (2018): 293–308

Brenner, W. Suzanne. *Cybercrime – Criminal Threats From Cyberspace.* Santa Barbara: Praeger, 2010.

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

Cassim, Fawzia. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?. *Potchefstroom Electronic Law Journal (PELJ)*, *18*(2), 69-110.

Caruana, Mireille M. (2017). “The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement.” *International Review of Law, Computers & Technology* 33 (3): 249–70.

Cate, Fred, and Rachel Dockery. "Data Privacy and Security Law." In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish. *Oxford Handbooks*. Oxford: Oxford Academic, 2021. Online edition, December 8, 2021.

Clough, Jonathan. *Principles of Cybercrime.* Cambridge: Cambridge University Press, 2015.

Cole, Mark D., and Sandra Schmitz. "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape." *University of Luxembourg Law Working Paper* No. -017 (2019).

Czapári, Dóra, és Gergely László Szőke. "Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása." *JURA* 28, no. 4 (2022): 24-48.

Cséka, Ervin, Zsanett Fantoly, István Hegedűs, Judit Kovács, és Vilmosné Maráz. *A büntetőeljárási jog alapvonalai. II.* Szeged: Bába Kiadó, 2007.

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

Custers, Bart, Jan-Jaap Oerlemans, and Ronald Pool. "Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies." *European Journal of Crime, Criminal Law and Criminal Justice* (2020): 121-152.

De Hert, Paul, and Vagelis Papakonstantinou. "The New Police and Criminal Justice Data Protection Directive: A First Analysis." *New Journal of European Criminal Law* 7, no. 1 (2016): 7–19

Dimitrova, Diana, and Paul De Hert. "The Right of Access under the Police Directive: Small Steps Forward." In *Privacy Technologies and Policy*, edited by M. Medina et al., 111-130. Lecture Notes in Computer Science. Springer International Publishing, 2018.

Drechsler, Laura. "Comparing LED and GDPR Adequacy: One Standard Two Systems." *Global Privacy Law Review* 1, no. 2 (2020): 93-103.

Dumitrescu, Mihaela-Sorina, and Mihaela-Emilia Marica. "Cybercrime in the Digital Era." In *New Trends in Sustainable Business and Consumption*, edited by Basic International Conference, 433-440. Bucharest: Editura ASE, 2019.

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 Attila Péterfalvi. "Amikor a gépeink tanulnak minket, avagy a mesterséges intelligencia alapú döntéshozatal és profilozás szabályozásának európai unió törekvéseiről." *Századvég* No. 1 (2022): 96.

Eszteri, Dániel. "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, és Révész Balázs, 489-506. Budapest: Wolters Kluwer Hungary, 2021.

Eszteri, Dániel. "A bűnügyi adatvédelmi irányelv." In *Magyarázat a GDPR-ról*, szerk. Buzás Péter, Péterfalvi Attila, és Révész Balázs, 385-401. Budapest: Wolters Kluwer Hungary, 2018.

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.

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

Faisal, Kamrul. "Journalism vs. Data Privacy: The GDPR Dilemma in Reporting Crimes." *Internet Policy Review* 11, no. 3 (2024).

Fantoly, Zsanett, és Budaházi Árpád. *Büntető eljárásjogi ismeretek I.* Budapest: Dialóg Campus Kiadó, 2019.

Fantoly, Zsanett, és Csongor Herke. "A mesterséges intelligencia a hatékonyabb büntetőeljárás szolgálatában." *Magyar Jog* 48, no. 4 (2023): 223-228.

Farina, Katie A. "Fraud Focus: The Fraudulent Use of Personal Information." *Journal of Financial Crime Prevention* 18, no. 3 (2021): 8.

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

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

Fried, Charles. "Privacy." *Yale Law Journal* 77 (1968): 475-493.

Furnell, Steven. "Hackers, Viruses and Malicious Software." In *Handbook of Internet Crime*, edited by Y. Jewkes and M. Yar, 43–45. Willan Publishing, 2010.

Gál, Andor. "A GDPR hatása a büntető anyagi jogra: a személyes adattal visszaélés tényállásának jövőjéről." In *A büntetőjog hazai rendszere megújításának koncepcionális céljai és hatásai*, szerk. Hollán M. és Mezei K., 133-146. Budapest: Társadalomtudományi Kutatóközpont Jogtudományi Intézet, 2020.

Gál, István László. "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: Ludovika Egyetemi Kiadó, 2021.

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

Gáti, Balázs. "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: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, 2021.

Gáti, Balázs. "Az adatvédelmi szabályozás aktuális tendenciái a büntető igazságszolgáltatás területén." In *IV. PhD konferencia kötet*, szerk. Bendes Ákos László, Gáspár Zsolt, Gáti Balázs, Projics Nárcisz, és Tóth Dávid, 42-61. Pécs: PTE-ÁJK, Doktori Iskola, 2022.

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

Gáti, Balázs. "A gazdasági válság hatásai a személyes adatok védelmére és annak büntetőjogi aspektusaira." In *Válságok és büntetőjog: Fiatal büntetőjogászok első konferenciája,* szerk.

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

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

Gáti, Balázs. "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, 2021.

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

Görög, Márta., Menyhárd, Attila., és Koltay, András. "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. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2 (2001): 243-249.

Grund, Borbála. "A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról." *MTA LAW WORKING PAPERS* 2 (2021): 1-37.

Gstrein, Oskar J., and Anne Beaulieu. "How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches." *Philosophy & Technology* 35, no. 1 (2022): 3

Gyaraki, Réka. "A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN-kód megadása sikeres vagy biztonságos az internet?" *Pécsi Határőr Tudományos Közlemények* XIII (2012): 237-238.

Gyaraki, Réka. "Az adatokkal kapcsolatos visszaélések és az információs rendszerben tárolt adatok sértetlensége." In *A kibernyomozói munka büntetőjogi sajátosságai*, szerk. Kovács Zoltán, 86-113. Budapest, 2023.

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

Háger, Tamás. "A nyilvánosság, mint a tisztességes eljárás egyik garanciája a büntetőperben." *Pro Futuro* 1 (2014): 46-61.

Havasiné Kulcsár, Petra. "A tárgyalás nyilvánossága, a tárgyalás nyilvánosságának korlátozása. A sajtó jelenléte a büntetőeljárásban: avagy a nyilvánosság fogságában." In *Büntetőjogi tanulmányok*, 18. köt., 51-81. Budapest, Magyarország: Matarka Kiadó, 2017.

Herke, Csongor. "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, 2021.

Herke, Csongor. *Magyar büntető eljárásjog.* Pécs: PTE Állam- és Jogtudományi Kar, 2021.

Herke, Csongor. *Büntető eljárásjog: Egyetemi jegyzet.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2018.

Herke, Csongor. "Mesterséges intelligencia a büntetőjogi döntéshozatalban." *Jogtudományi Közlöny* 78, no. 4 (2023): 165-176.

Hesz, Tibor, és Kőhalmi László. "A tanúvédelem a terhelt védőjének aspektusából." In *A tanú védelmének elméleti és gyakorlati kérdései*, szerk. Mészáros Bence, 97-107. Pécs: Pécsi Tudományegyetem, Gazdasági Büntetőjogi Kutatóintézet, 2009.

Hinkel, Tamás. "A mesterséges intelligencia térhódítása a büntetés-végrehajtásban." *Börtönügyi Szemle* no. 4 (2020): 13-29.

Hirvonen, Paulina. "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, 2022.

Holt, Thomas J., and Adam Bossler. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses.* Edited by Richard Wortley. London: Routledge, 2015. https://doi.org/10.4324/9781315775944.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction.* 3rd ed. London: Routledge, 2022.

Horváth, Tibor. "XXI. Fejezet az emberi méltóság és egyes alapvető jogok elleni bűncselekményekről." In *Magyar büntetőjog: különös rész*, szerk. Görgényi I. et al. Budapest: Wolters Kluwer Magyarország, 2020.

Gál, István László. "A pénz–és bélyegforgalom biztonsága elleni bűncselekmények." In *Új Btk. kommentár: 7. kötet, Különös rész*, szerk. Polt P., 193–224. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó, 2013.

Jánosi, Andrea. "Bűnüldözési célú adatkezelés – releváns EU jogforrások, az EU rendszereinek interoperabilitása." *Miskolci Jogi Szemle: A Miskolci Egyetem Állam- és Jogtudományi Karának Folyóirata* 17, no. 5 (2022): 151-161.

Jánosi, Andrea. "A Magyar bűnügyi nyilvántartási rendszer az Európai Unió által megfogalmazott elvárások tükrében." *Miskolci Jogi Szemle* 16, no. 5 (2022): 247-258.

Jóri, András. *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 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.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2009.

Kahn, Charles M., and William Roberds. "Credit and Identity Theft." *Journal of Monetary Economics* 55 (2008): 251-264.

Karsai, Krisztina. "Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerk. Karsai Krisztina, 989-996. Budapest, Magyarország: Wolters Kluwer, 2019.

Király, Tibor. *Büntetőeljárási jog.* Budapest: Osiris Kiadó, 2000.

Kis Kelemen, Bence. "Személyes adatok védelme fegyveres konfliktusokban." *Jogtudományi Közlöny* 77, no. 10 (2022): 395–402.

Kiss, Tibor. "Kiberbűnözés." In *Alkalmazott Kriminológia*, szerk. A. Tünde Barabás, 445-461.

Knoops, Bert-Jaap. "The Internet and its Opportunities for Cybercrime." *Tilburg Law School Legal Studies Research Paper Series* 9 (2010): 735-754.

Kohl, Uta. “THE RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW AND TWO WESTERN CULTURES OF PRIVACY.” *International and Comparative Law Quarterly*72, no. 3 (2023): 737–69.

Kokott, Juliane, and Christoph Sobotta. "The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR." *International Data Privacy Law* 4 (2013): 222-228.

Kondás, Katalin. "Biometria a börtönben." *Biztonságtudományi Szemle, OE* 3, no. 4 (2021): 1-10. ISSN 2676-9042. [Online]. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/185

Kondás, Katalin: „Adatok védelme a börtönökben.” In: Hadmérnök, NKE, XIII. évfolyam 1. szám 2018.

Kőhalmi, László. "A pénzhamisítással kapcsolatos bűncselekmények. A pénz büntetőjogi fogalma." In *Büntetőjog II. Különös Rész – Jogi Szakvizsga Segédkönyvek*, szerk. Balogh Ágnes, 411-417. Budapest–Pécs: Dialóg Campus Kiadó, 2005.

Kőhalmi, László. "Nyilvánosság és büntetőeljárás." In *Az internet és a közösségi média jogi kihívásai*, szerk. Tóth Dávid, 36-46. Konferenciakötet. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, 2022.

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

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

Kőhalmi, László. "The Human Rights in the Criminal Procedure." In *Europe of Founding Fathers: Investment in the Common Future,* edited by Magdalena Sitek, Gaetano Dammacco, Aleksandra Ukleja, and Marta Wojcicka, 397-407. Olsztyn, Poland: University of Warmia and Mazury, Faculty of Law and Administration, 2013.

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

Leiser, Mark and Bart Custers. "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680." *European Data Protection Law Review* 5, no. 3 (2019): 367-378.

Lynskey, Orla. "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection Against Predictive Policing." *International Journal of Law in Context* 15, no. 2 (2019): 162-176.

Majtényi, László. "Az információs jogok." In *Emberi jogok*, szerk. Halmai Gábor és Tóth Gábor Attila, 582-583. Budapest: Osiris, 2003.

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

Marquenie, Thomas. "The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework." *Computer Law & Security Review* 33, no. 3 (2017): 324–340

Marquenie, Thomas, and Katherine Quezada-Tavárez. "Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing." In *Security Technologies and Social Implications*, szerkesztette Garik Markarian, Ruža Karlović, Holger Nitsch, és Krishna Chandramouli, 32–60. Hoboken, NJ: Wiley, 2022.

Márki, Dávid. *Az igazságszolgáltatás nyilvánosságának alkotmányjogi vizsgálata: Alapjogi kollíziók a büntetőeljárás, a sajtó és a politika kereszttüzében.* Szeged, Magyarország: Iurisperitus Kiadó, 2023. https://publicatio.bibl.u-szeged.hu/27808/1/Marki_2023_07_05.pdf.

Matos, Sara. "Privacy and Data Protection in the Surveillance Society: The Case of the Prüm System." *Journal of Forensic and Legal Medicine* 66 (August 2019): 155–161.

Máté, István Zsolt. "Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe." *Belügyi Szemle* 66, no. 7-8 (2018): 36-54.

McDermott, Yvonne. (2017). Conceptualising the right to data protection in an era of Big Data.*Big Data & Society*,*4*(1).

McGuire, Mike., and Samantha, Dowling. "Cyber-dependent Crimes." In *Cyber Crime: A Review of the Evidence* (Research Report 75, Chapter 1), Law, Computer Science, 4-29, 2013.

Mezei, Kitti. "Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására." *JURA* 24, no. 1 (2018): 349-360.

Mezei, Kitti. "Szervezett bűnözés az interneten." In *A bűnügyi tudományok és az informatika*, 125-147. Budapest – Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019.

Mezei, Kitti. "A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre." *Állam- és Jogtudomány* 61, no. 4 (2020): 65-81.

Mezei, Kitti. "Diszkrimináció az algoritmusok korában." *Magyar Jog* no. 6 (2022): 336-337.

Mezei, Kitti. "A kiberbűnözés szabályozási kihívásai a büntetőjogban." 2023. https://real.mtak.hu/104974/1/Mezei_UL_201945.pdf.

Miskolczi, Barna, és Szathmáry Zoltán. *Büntetőjogi kérdések az információk korában.* Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., 2019.

Molnár, Gábor. "XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények." In *Magyar büntetőjog – Kommentár a gyakorlat számára*, szerk. Kónya Sándor, 971-972. Budapest: HVG-ORAC, 2016.

Momsen, Carlsten. "Relevance of Data Security and Data Protection in Companies from the Perspective of Criminal Law." In *Handbook Industry 4.0*, edited ed.Walter Frenz, 57–74. Berlin, Heidelberg: Springer, 2022.

Moore, Tyler., and Ross, Anderson. "Rethinking Information Security to Improve Data Privacy." *European Journal of Information Systems* 28, no. 5 (2019): 687-694.

Nagy Melánia and Ripszám Dóra, 67-92. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2023

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

Nagy, Zoltán András. "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerk. Kiss Tibor, 45-64. Budapest: Dialóg Campus, 2020.

Nagy, Zoltán András. *Bűncselekmények számítógépes környezetben.* Budapest: Ad Librum, 2009.

Nagy, Zoltán András. "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, 2021.

Nagy, Zoltán András. "Kiberbűncselekmények szabályozása." In *Kibervédelem a bűnügyi tudományokban*, szerk. Kiss Tibor. Budapest: Dialóg Campus, 2020.

Nagy, Zoltán András. "A számítógépes környezetben elkövetett bűncselekmények új szabályozásáról. Háttér és elemzés." *Ügyészek Lapja* 3-4 (2014): 31-45.

Nagy, Klára. "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*, szerk. Gaál Gyula és Hautzinger Zoltán, 81-88. Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2010.

Naudts, Lauren. "The Data Protection Impact Assessment for Law Enforcement Agencies (Adatvédelmi hatásvizsgálat a bűnüldöző szervek számára)." Lecture at the 12th International Communication Conference, Bucharest, Romania, June 15, 2018.

Navratil, Szonja. "Az igazságszolgáltatás nyilvánossága. Összehasonlító elemzés." In *A bírói függetlenség, a tisztességes eljárás és a politika*, szerk. Badó Attila. Budapest: Gondolat Kiadó, 2011.

Németh, Kata. "A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre." *Debreceni Jogi Műhely* 16, no. 1-2 (2019): 291-320.

Nyeste, Péter. "A bűnüldözési tevékenység során használt fontosabb nyilvántartások." In *A bűnügyi hírszerzés kézikönyve*, szerk. Sub Lege Libertas, 181-199. Budapest: Nordex Nonprofit Kft.; Dialóg Campus Kiadó, 2019. ISBN 978-615-5945-79-3 (print); 978-615-5945-84-7.
https://real.mtak.hu/128819/1/Web_PDF_A_bunugyi_hirszerzes_kezikonyve.pdf.

Nyiri, Sándor. "A nyomozóhatóságok és az ügyészség kapcsolata a büntetőeljárásról szóló törvényben." *Belügyi Szemle* 66, no. 6 (2018): 5-16.

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

Osztopáni, Krisztián. "Jogalapok." In *Magyarázat a GDPR-ról*, szerk. Péterfalvi Attila, Révész Balázs, és Buzás Péter. Budapest: Wolters Kluwer, 2018.

Palánkai, Tibor. "Integráció és kohézió az EU-ban." In *Tagállami integrációs modellek*, 27-50, 2019.

Pálvölgyi, Ákos. "A hírérték margóján: személyhez fűződő jogok védelméhez való jog a büntetőeljárásban különös tekintettel a személyes adatok védelmére." *Büntetőjog Szemle* no. 3 (2014): 41-45.

Parti, Katalin., és Kiss Tibor. "Az informatikai bűnözés." In *Kriminológia*, szerk. Borbíró A., Gönczöl K., Kerezsi K., és Lévay M., 491-493. Budapest: Wolters Kluwer, 2017.

Petrović, Dragana B. "Privacy and Protection of Personal Data – Criminal Law Aspect." *Strani pravni život* 66, no. 4 (2022): 469-486.

Péterfalvi, Attila, és 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, és Koltay András, 405-420. ELTE-ÁJK, Budapest, 2017.

Péterfalvi, Attila. "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), 2020.

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

Petrik, Ferenc. *Alkotmány a gyakorlatban, kommentár a gyakorlat számára.* Budapest: HVG-ORAC, 2009.

Porcedda, Maria Grazia. "Data Protection and the Prevention of Cybercrime - The EU as an Area of Security?" *EUI Working Papers LAW* No. 25 (2012). https://ssrn.com/abstract=2169340 or http://dx.doi.org/10.2139/ssrn.2169340.

Quezada-Tavárez, Katherine., Plixavra, Vogiatzoglou, and Sofie, Royer. "Legal Challenges in Bringing AI Evidence to the Criminal Courtroom." *New Jornal of European Criminal Law* 12, no. 4 (2021): 531-551.

Róth, Erika. "A digitalizáció és a terhelti jogok érvényesülése a büntetőeljárásban." *Miskolci Jogi Szemle* 16, no. 1, különszám (2021): 270-278.

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

Shutova, Albina A. "Patients' Personal Data, Including Biometrics, as Objects of Criminal Law Protection." *The International Journal of Law in Changing World* 1, no. 2 (2022): 45–58.

Schmehl, Gábor Dániel. "SMART eszközök és egyedi alkalmazások a magyar büntetés-végrehajtásban." *Börtönügyi Szemle* no. 4 (2020): 49-69. http://epa.niif.hu/02700/02705/00124/pdf/EPA02705_bortonugyi_szemle_2020_4.pdf.

Schreiber, Terry. *Data Protection and Cybersecurity Law.* Oxford: Oxford University Press, 2021.

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

Sieber, Ulrich. "A számítógépes bűnözés és más bűncselekmények az információtechnológia területén." *Magyar Jog* no. 2 (1993): 105-109.

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

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

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

Sorbán, Kinga. "A digitális bizonyíték a büntetőeljárásban." *Belügyi Szemle* 64, no. 11 (2016): 81-96.

Sorbán, Kinga. "Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában: Felelősség és kötelezettségek." *In Medias Res* VIII, no. 1 (2019): 84-101.

Szabó, Imre. "Informatikai bűncselekmények." In *Az informatikai jog nagy kézikönyve,* szerk. Dósa I.. Budapest: Complex, 2008.

Szabó, Máté Dániel. "Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival." *Információs Társadalom* no. 5 (2005): 44-54.

Szathmáry, Zoltán. "Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban." Doctoral dissertation, Pécsi Tudományegyetem ÁJK Doktori Iskolája Informatikai és Kommunikációs Jog Program, Budapest, 2012, 79-80.

Szathmáry, Zoltán. "A mesterséges intelligencia hatása a büntetőjogi felelősségre." *Ügyészek Lapja* 26, no. 3 (2019): 37-46.

Szathmáry, Zoltán. "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése I." *Infokommunikáció és Jog* 2 (2022): 6-10.

Szathmáry, Zoltán. "Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése II." *Infokommunikáció és Jog* 1 (80) (2023): 11-13.

Szendrei, Ferenc. "Bűnügyi Együttműködés." In *A Bűnügyi Hírszerzés Kézikönyve*, szerk. Szendrei Ferenc, 221-242. Budapest: Dialóg Campus Kiadó, 2019.

Szijártó, István. "Az Europol és az Eurojust szerepe a közös nyomozócsoportokban." *Ügyészek Lapja* 26, no. 6 (2019): 59-73.

Sziklay, Júlia, and Tamás Bendik. *Az adatvédelem hazai és európai uniós szabályozása és alapintézményei.* Budapest: NKE, 2018.

Szomora, Zsolt. "Btk. XXI. fejezet." In *Kommentár a Büntető Törvénykönyvhöz*, szerk. Karsai K. Budapest: Complex, 2013.

Szomora, Zsolt. "A vagyon elleni bűncselekmények." In *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, szerk. 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*, szerk. Karsai Krisztina, 492-531. Budapest, Magyarország: Wolters Kluwer, 2019.

Szőke, Gergely László. "Az adatvédelem szabályozásának történeti áttekintése." *Infokommunikáció és Jog* (2013): 107-112.

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*, edited by Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Alexander Prosser, Dona Scola, and Tamás Szádeczky, 301-311. Wien, Austria: Facultas Verlag, 2018.

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

Tóth, Dávid, és Zoltán András Nagy. "Computer Related Economic Crimes in Hungary." *Journal of Eastern-European Criminal Law* no. 2 (2015): 165-174.

Tóth, Dávid. "A bankkártyával kapcsolatos bűncselekmények prevenciós eszközei." In *PEME XV. PhD – konferenciakötet*, szerk. Koncz I. és Szova I., 182-192. Budapest: Professzorok az Európai Magyarországért Egyesület, 2017.

Tóth, Dávid. "A virtuális pénzekkel kapcsolatos visszaélések." In *Rendészet-Tudomány-Aktualitások. A rendészettudomány a fiatal kutatók szemével*, szerk. Baráth Emőke Noémi és

Mezei József, 242-250. Budapest: Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, 2019.

Tóth, Dávid. "Személyiséglopás az interneten." *Büntetőjogi Szemle* no. 1 (2020): 116-117.

Tóth, Dávid. "Az identitáslopás kriminológiai sajátosságai." In *A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői*, szerk. Gaál Gyula és Hautzinger Zoltán, 207-213. Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport.

Tóth, Dávid. "The Criminal Law Protection of Personal Data in Hungary." In *Collection of Papers "Law Between Creation and Interpretation" Vol. 3.*, edited by Dimitrije Ćeranić, Svjetlana Ivanović, Radislav Lale, and Samir Aličić, 233-246. East Sarajevo, Bosnia-Herzegovina: Faculty of Law, University of East Sarajevo, 2023.

Varga, Petra. "A nyilvánosság elvének érvényesülése a büntetőeljárásban." *Debreceni Jogi Műhely* XV, no. 1-2 (2018). DOI: 10.24169/DJM/2018/1-2/9.

Vogiatzoglou, Plixavra., 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 Louis Brandeis. "The Right to Privacy." *Harvard Law Review* IV, no. 5 (1890): 193-220. https://www.jstor.org/stable/1321160?seq=27.

Westermann, Hannes, Michael Joyce, and Benoit Dupont. *Artificial Intelligence in the Context of Crime and Criminal Justice.* Korean Institute of Criminology, 2018.

Wicki-Birchler, David. "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?" *International Cybersecurity Law Review* 1 (2020): 63-72. https://doi.org/10.1365/s43439-020-00012-5.

Winter, Heinrich, B., et al. *De verwerking van politiegegevens in vijf Europese landen.* Rijksuniversiteit Groningen - Pro facto, WODC rapport 3031, 2020.

Zhu, FangBing, és Zongyu Song. "Systematic Regulation of Personal Information Rights in the Era of Big Data." *SAGE Open* 12, no. 1 (2022): 1–12.

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

(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 bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi 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.

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

2013/40/EU Irányelve(2013. augusztus 12.): Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

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

2023.évi XXV.törvény,

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,

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

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.

A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról

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 átívelő áramlásáról,https://www.oecd.org/sti/ieconomy/15590228.pdf.

Az Európai Adatvédelmi Biztos Határozata (2020. május 15.) az európai adatvédelmi biztos eljárási szabályzatának elfogadásáról, 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

Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós 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.

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

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

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

Az Európai Parlament és a Tanács, 2004. Rendelete 460/2004/EK (2004. március 10.): Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról

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

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

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

Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata, 2012/C 326/01.
A 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.

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

Bundesgesetsblatt,.
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

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. Február 1970. URL: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf.

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

(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

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 - DSAnpUG-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 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.

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://svenskforfattningssamling.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 personalles

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertes, (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 lagöverträdelser 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.

Arkivlag (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 / Bírósági 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

BH2013. 146

BH2015. 29

BH2017. 392

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

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

Büntetés-végrehajtás Tudományos Tanácsa. Korszakváltás a büntetés-végrehajtásban: Útmutató a 2013. évi CCXL (Bv.) törvény megismeréséhez. Budapest, 2015. https://bm-tt.hu/wp-content/uploads/2022/02/Korszakvaltas_LO-RES.pdf.

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

European Union Agency for Cybersecurity (ENISA). *Threat Landscape for Cybersecurity in the Context of GDPR.* European Union Agency for Cybersecurity, 2020.

Európai Parlament. A személyes adatok védelme.
https://www.europarl.europa.eu/ftu/pdf/hu/FTU_4.2.8.pdf.

Integritetsskyddsmyndigheten,
https://www.imy.se

NAIH beszámoló a 2020. évi tevékenységről,
https://www.naih.hu/eves-beszamolok

NAIH beszámoló a 2021. évi tevékenységről
https://www.naih.hu/eves-beszamolok

NAIH beszámoló a 2022. évi tevékenységről
https://www.naih.hu/eves-beszamolok

Pók, László, (2019) 5 kínzó 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/ NAIH 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_en.pdf

01/2021. számú iránymutatás Az adatvédelmi incidensek bejelentésével kapcsolatos példákról, 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_controllerprocessor_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
infoszab_allasfoglalas_NAIH-2020-294-4 (5). pdf

NAIH-4418-5/2012/V, Állásfoglalás a bírósági tárgyalásokról készített MTI tudósítások során nyilvánosságra hozott személyes adatokról.
https://naih.hu/files/Adatvedelem-4418_V_2012-5-allasfoglalas-MTI.pdf

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