Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

Gáti Balázs

A személyes adatok védelme a bűnügyi tudományokban az irányelvi szabályozás tükrében

Doktori értekezés tézisei

Témavezetők:
Prof. habil. Dr. Kőhalmi László tanszékvezető, egyetemi tanár
Dr. Tóth Dávid egyetemi adjunktus

Pécs, 2025

Tartalomjegyzék

I. Bevezetés

A globalizáció térnyerése és az információs technológia fejlődése jelentősen átalakította az adatvédelem területét, új kihívások elé állítva az Európai Uniót. Az Európai Bizottság 2012-ben kezdeményezett egy adatvédelmi reformot célzó javaslat csomagot, melynek célja az adatvédelem modernizálása volt a digitális kor igényeihez igazodva. Ennek eredményeképpen az Európai Parlament és a Tanács 2016 áprilisában elfogadta az új uniós adatvédelmi csomagot, amely két fő jogforrást tartalmaz: az általános adatvédelmi rendeletet és a bűnüldözési célú adatkezelésre vonatkozó irányelvet. [**(**EU) 2016/679, (EU) 2016/680]
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.(Eszteri,2018) 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. (Nagy, Mezei 2018)
Ennek érdekében az irányelv specifikus, differenciált szabályokat állít fel, amelyek meghatározzák a rendőrségi és igazságügyi adatkezeléseket, biztosítva az adatok szabad áramlását és a tagállamok közötti együttműködést. [(EU) 2016/680 Preambulum (10)] Ahogy a Rendeletet, úgy az Irányelvet is megelőzték a technikai-ipari forradalom jelentős változásai. (Szőke, 2014) Az Unió Biztonsági stratégiája hangsúlyozza, hogy az olyan új technológiák, mint a mesterséges intelligencia, hatékony eszközként használhatók a bűnözés elleni küzdelemben. (Eszteri, Péterfalvi 2022, Fantoly, Herke 2023) 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 nemcsak a gazdasági és technológiai területeken hozott forradalmi változásokat, hanem a bűnözési módszerekben is új dimenziókat nyitott meg (Schwab, 2016, Ambrus, 2022). 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 **(**Westermann, Joyce, Dupont, 2019, Nagy, 2020)**)**. Ebben a kölcsönhatásban értelmezhető az adatvédelem is. Szükségessé válhat a jelenlegi szabályozási gyakorlat felülvizsgálata, további pontosítása a büntetőjogi szankciókat, a nyomozást, vádeljárást, a büntetésvégrehajtást 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 (Kőhalmi, 2010, Eszteri, 2021) szempontjából. Az európai adatvédelmi

jogharmonizáció és 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 (Gál I., Tóth M. 2016, Jánosi 2022). Az egyes tagállamok jogfejlődése- és jogrendszere meghatározó az uniós jog átültetése területén.

Alapvető fontosságú, hogy hogyan járul hozzá az adatvédelmi reform a nemzetközi bűnözés elleni küzdelemhez a hazai és az egyes tagállami jogi szabályozás gyakorlata révén **(**Kőhalmi 2012, Bendik, 2020).

Ezen belül fontosnak tartom az Európai Bizottság által véleményezett és vizsgált gyakorlatot, és annak nemzeti jogba történő átültetését, amely irányadó a büntetőjogi szabályozás területén is **(**Gombos, 2017).

Globalizált világunkban a bűnözés, különösen a számítógépes bűnözés és más, a kibertérrel összefüggő bűncselekmények egyre inkább határokon átnyúló jellegűek. (Mezei 2020, Ambrus 2021) 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 (Simon, Gyaraki, 2020). 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. (Szíjártó, 2019) Ez az együttműködés, és különösen az elektronikus bizonyítékok gyűjtése és cseréje gyakran személyes adatok átadásával járnak, ezért alapvető fontosságúak a megfelelő adatvédelmi biztosítékok. Erre jó példa a Budapesti Egyezmény 2. Kiegészítő jegyzőkönyve, mely az elektronikus bizonyítékok határon túli továbbításának szabályozása mellett külön fejezetet szentel az adatvédelmi biztosítékoknak. (Sorbán, 2019)

Az ilyen biztosítékok hozzájárulnak a bűnüldöző hatóságok közötti bizalomépítéshez is, gyorsabb és hatékonyabb információcserét biztosítanak, és erősítik a jogbiztonságot a büntetőeljárásokban **(**Szendrei, 2019). 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 (Sorbán, 2016, Krasznay, 2021)

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 **(**Péterfalvi, Bendik, Tóásó 2019**,** Somssich, 2020)

Másrészt az informatika rohamos fejlődésének köszönhetően az egyes deliktumok elkövetése a kibertéren keresztül - az esetek túlnyomó többségében a személyes adatok sérelmével egyidejűleg - valósul meg. A digitális technológiák fejlődése és az online térben történő adatgyűjtés exponenciális növekedése új kihívásokat jelentenek a személyes adatok védelme területén **(**Eszteri, 2021, Kis Kelemen, 2022).

A személyes adatok védelme nemcsak az egyének jogainak garantálását szolgálja, hanem fontos eszköz a számítógépes bűncselekmények elleni küzdelemben is. A Fehér Könyv és a Mesterséges Intelligencia törvénytervezet példái annak, hogy az adatvédelmi kérdések egyre inkább integrálódnak a jogi szabályozásba a technológia fejlődésével párhuzamosan. (COM (2020)65 final, COM(2021) 206 final).

Az adatvédelmi intézkedések közvetetten segíthetnek megakadályozni a kibertámadásokat (Brown 2020). Az adatvédelmi szabályok lehetővé teszik a hatóságok számára, hogy hatékonyabban és gyorsabban nyomozzanak az online bűncselekmények ügyében (Taylor 2017).
A megfelelő adatvédelmi intézkedések nemcsak az egyének személyes adatainak védelmét szolgálják hagyományos környezetben, hanem hozzájárulnak a digitális környezetben való biztonság és stabilitás biztosításához (Csiszár 2019, Fenyvesi 2019, Gyaraki 2022)

I.2. A kutatás célja

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

Hipotéziseim az alábbiak szerint fogalmaztam 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 a szankciókat illetően.

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. 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 az egyes részeknél a logikai és kritikai elemzéssel kiegészítve.

II. Az eredmények bemutatása

A disszertáció bevezető részében az adatvédelem fogalmával kapcsolatos elméleti megfontolások, az adatvédelmi jog fejlődésének főbb állomásai, és a személyes adatok védelmének aktuális jogi szabályozása kerültek bemutatásra. Az értekezés további részeiben a 2016/680/EU irányelv - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv és jogharmonizációja bemutatása után, a bűnügyi célú adatkezelésekkel kapcsolatos probléma felvetés kapcsán bemutattam a nyomozás-, a vádeljárás-, a büntetés-végrehajtás jogszabályi hátterét, továbbá a személyes adatok védelméhez kapcsolódó büntetési szankciókat meghatározó kódexünk szabályozását is. A digitális térben elkövetett bűncselekmények és az adatvédelem közötti összefüggéseket részletesen elemeztem, különös hangsúlyt fektetve a személyes adatok védelmének jelentőségére.

II.1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése

A II. fejezetben az adatvédelem fogalmának és történetének rövid áttekintése után bemutattam a vonatkozó aktuális uniós szabályozást és annak intézményrendszerét. Az adatvédelem fogalmát illetően, annak gyakorlati szempontú megközelítését tartottam

fontosnak, figyelembe véve az értekezés során vizsgált szempontokat. Ennek megfelelően a személyes adatok védelme – véleményem szerint gyakorlati szempontból - nem más, mint, a természetes személyek jogainak és szabadságainak védelme a természetes személyek személyes adataihoz fűződő önrendelkezési jog gyakorlási körülményeinek meghatározása által, - valamint a természetes személyek személyes adatait kezelő adatkezelőkre vonatkozó adatkezelési feltételek szabályozása által.
Ennek értelmében mind az adatkezelő, mind az adatkezeléssel érintett természetes személy rendelkezési joggal bírnak az érintett személyes adatai felett. Míg az adatkezelő által történő rendelkezési jog jogszerűségét, másnéven jogalapját a vonatkozó szabályozásban, úgy, mint a GDPR-ban, valamint a LED-ben foglalt jogalapok valamelyike biztosítja, addig az érintett személyes adataival információs önrendelkezési joga keretében saját maga rendelkezik. Azaz az adatkezelés feltételeit, a személyes adatok feletti rendelkezési jog gyakorlásának feltételeit az érintetten kívüli személyek, vagyis az adatkezelők vonatkozásában valamely „adatvédelmi" jogszabály vonatkozó rendelkezése határozza meg.
A rendelkezési jognak vannak korlátai mindkét irányból. Az adatkezelés mint fogalom maga is jogszabály által szabályozott rendelkezési jogosultság az érintett személyes adatai felett. [GDPR 4. cikk. (2.)] Az adatkezelő által végzett adatkezeléseknek, vagyis a személyes adatokon végrehajtott valamely műveleteknek vannak bizonyos korlátai.
Ha elméleti síkon egy mérleg két serpenyőjébe helyeznénk az érintett személyes adatait érintő rendelkezési jogosultságokat adatkezelői, valamint érintett oldalról egyaránt, akkor általános következtetésként elmondható lenne, hogy a személyes adatokkal kapcsolatos rendelkezési jogosultságoknak több jogszabályi korlátja van adatkezelői oldalon, mint érintetti oldalon. Az érintett saját személyes adatai feletti önrendelkezési jogának is vannak korlátai, amelyek klasszikus értelemben nem az úgynevezett „adatvédelmi szabályozás" részét képezik, hanem egyéb jogi normák által és etikai elvek által meghatározottak.
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.
Ezzel a harmadik generációs szabályozás által is megjelenített adatkezelői szempontú megközelítéssel (Szőke 2013) vizsgáltam a jogszabályok által meghatározott illetékes hatóságok szerepét, úgymint a nyomozó hatóságok, bíróságok és a büntetés-végrehajtás szerveit.

II.2. A kutatással elérni kívánt célok bemutatása, a hipotézisek megválaszolása

A III. fejezetben a bűnügyi adatvédelmi irányelvet ennek tagállami jogharmonizációját, és a szabályozással kapcsolatos szakirodalmi álláspontokat és az egyes értelmezési kérdéseket illetően EUB ítélkezési gyakorlatát ismertettem. A jogirodalomban az irányelv számos

értelmezése és bemutatása lelhető fel. **(**Sajfert, Quintel 2017, Oswald 2018, Nagy, Mezei 2018, Eszteri 2018, Leiser,Custers 2019, Quezada-Tavárez, et al. 2019, Lynskey 2019, Winter 2020, Bolognini 2020, Drechsler 2020, Naudts, 2020, Eszteri 2021)
Áttekintettem az Európai Bizottságnak a bűnüldözésben érvényesítendő adatvédelemről szóló irányelve alkalmazásáról és működéséről szóló jelentéseit, valamint az Állampolgári Jogi, Bel- és Igazságügyi Bizottság (LIBE) megbízásából készült tanulmányt, amely a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv végrehajtásának kritikai értékelését tartalmazta **(**Vogiatzoglou, 2022). A jogharmonizációs értékeléséről szóló átfogó jelentések áttekintése mellett, a magyar, a német, a francia és a svéd jogba történő átültetés példáin keresztül ismertettem az egyes nemzeti jogszabályokba történő gyakorlatot, beleértve az adott nemzeti jogrendszerek adatvédelmi történetéhez kapcsolódó összefüggéseket.
A tagállami jogharmonizációs gyakorlatok összehasonlító vizsgálatánál, az adatvédelmi szabályozás területén 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.

1.Hipotézis

Az uniós jogharmonizáció és a nemzeti jogrendszerek vonatkozásában feltételeztem, 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.

Általánosságban elmondható, hogy a jogharmonizáció kereteit az adott tagállam jogrendszerének szabályai adják, azok történeti kialakulásának és hierarchiájának megfelelően. (Palánkai 2019)
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 a módosító törvény tartalmazta. A svéd jogalkotás annyiban különbözik, hogy a korábbi adatvédelmi rendeleteket hatályon kívül helyezve új jogszabály megalkotásával biztosította az általános adatvédelmi rendelet közvetlen érvényesülését, és külön törvény keretében implementálta a bűnügyi irányelvet is, megfelelően a korábbi jogi szabályozásának.

Megállapítottam, hogy a tagállamok között vannak eltérések a bűnügyi irányelv átültetésében. 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 irányelv hatályát illetően alapvetően két szempont az irányadó, a személyi (illetékes hatóság) és a tárgyi hatály (bűncselekmény fogalma), melyek együttesen határozzák meg az egységes megközelítést. [(EU) 2016/680, 2. cikk (1) és (12)–(14) preambulumbekezdés)]

A magyar joggyakorlatban az Infotv. kiterjesztette a törvény hatályát a nemzetbiztonsági-és honvédelmi célú adatkezelésekre is, *„az Infotv. előírásainak teljességét rendelte el alkalmazni”* (Infotv. 2. § (3) bekezdés)

A német adatvédelmi törvény az (EU) 2016/680 irányelv hatályával kapcsolatban egyértelműen megjelöli az irányelv szerinti bűnügyi adatkezelési célt, és a törvény hatályát a „ *(...) büntetőjogi vagy közigazgatási szankciók végrehajtására illetékes állami szervek által végzett adatkezelésre”* rendeli alkalmazni.(BDSG 45.§) Arról is rendelkezik, hogy ez a hatály a szövetségi adatvédelmi biztosra és hivatalára is vonatkozik. Alkalmazható azokra a közigazgatási szabálysértésekre is, amely nem minősülnek büntetőjogi szabálysértésnek és csak pénzbírság formájában kiszabott közigazgatási szankciókkal sújthatók [BDSG 11. § (1). 8.]
A német törvény hatálya így eltér a bűncselekmény szűkebb értelmezését alkalmazó országokban megfigyelhető joggyakorlattól, amelyek a hasonló közigazgatási szankciókat esetleg nem tekintik a LED végrehajtása alá tartozónak.

A francia 78-17 számú törvény a 87. cikkben határozza meg az irányelv szerinti hatályt. A 87. cikk külön kitér a hatóságok GDPR szerinti célú adatkezeléseire is. A 2018. júniusi törvényben még szerepelt a nemzetbiztonság védelme az adatkezelés céljai között, a jelenleg hatályos törvényben már nem szerepel.

A svéd bűnügyi adatokról szóló törvény meghatározza a törvény célját, és az illetékes hatóságokat a hatályt illetően. (SFS 2018:1177 1.ch.2.§) A törvény nem vonatkozik a nemzetbiztonsági vonatkozású személyes adatok biztonsági rendőrség általi kezelésére, illetve arra az esetre, ha a rendőrség nemzetbiztonsági feladatot vett át a biztonsági rendőrségtől. A törvény nem vonatkozik továbbá a személyes adatok fegyveres erők általi kezeléséről szóló törvényre, illetve fegyveres műveletekkel kapcsolatos törvény által meghatározott adatkezelésekre sem.

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. 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 87.cikk), valamint a svéd (SFS 2018:1177, 2. ch 1-3. §, és 11-14.§) adatvédelmi törvények biztosítják ezt. Jogalapok tekintetében a hozzájárulást, mint jogalapot, a német, francia, svéd és a magyar 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. 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. Eltérés még a LED- től, hogy a német adatvédelmi törvény nem tesz kifejezett említést a közös adatkezelésre vonatkozó kapcsolattartási pont kijelölésének kötelezettségéről, így a LED 21. cikk szerinti követelménye látszólag teljesen hiányzik a nemzeti jogi keretből.

Megállapítottam, hogy a tagállamok között eltérések vannak a bűnügyi irányelv átültetésében, a bűnüldözési célú adatkezelések uniós szabályozása ugyanakkor egyrészt nem rendeleti formában, hanem irányelvi megfogalmazás keretei között jött létre, ami tág mérlegelési jogkört biztosított a tagállamok részére. 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 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 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, az Európai Bizottság, az Adatvédelmi Testület iránymutatásai, a folyamatban lévő EUB döntések által nyújtott iránymutatások és támogatások hatékony alkalmazása.
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.

2.Hipotézis

A személyes adatok védelme területén a büntetőeljárás, valamint a büntetés-végrehajtás jogszabályi feltételei adatvédelmi szempontból megfelelőek, azonban a jelenlegi jogszabályok alapján létrejött gyakorlatok a büntetőeljárás- és végrehajtási folyamatok területén nem mindig biztosítják az érintettek egyes kategóriáinak teljes körű védelmét, így további szabályozásra vagy megoldásokra van szükség a védelem megerősítéséhez.

A büntetőeljárások alapvető célja a bűncselekmények felderítése, az elkövetők felelősségre vonása és a jogellenes cselekményekből eredő károk orvoslása, miközben az alapvető jogokat, a magánélet védelmét is tiszteletben kell tartani (Kőhalmi 2013).
A IV. fejezetben az adatvédelmi szabályoknak való megfelelést az eljárás különböző szakaszaiban, a Büntetőeljáráról szóló törvény szabályozását figyelembe véve vizsgáltam. (Király 2000, Fenyvesi, Herke, Tremmel 2004, Nyíri 2018, Herke 2018, Fantoly, Budaházi 2019).
Részletesen áttekintettem, hogyan határozzák meg a jogszabályok a gyanúsítottak tanúk, vádlottak és sértettek személyes adatainak kezelését, valamint milyen potenciális problémákat vetnek fel az eljárás során. (Hesz, Kőhalmi 2009, Pálvölgyi 2014, Németh 2019, Róth 2021, Mándi 2023) Kiemelt figyelmet fordítottam a tárgyalás nyilvánosságának és a zárt tárgyalásnak az adatvédelemmel kapcsolatos kihívásaira, valamint az ügyiratok zárt kezelésének problémáira. Bemutattam a tárgyalás nyilvánosságának elvéből és a természetes személyek adatainak védelméről szóló jogszabályokból eredő lehetséges konfliktusokat. (Cséka 2007, Petrik 2009, Erdei 2011, Navratil 2011, Varga 2018, Németh 2019, Kőhalmi 2023, Márki 2023).

Adatvédelmi aggályok a tárgyalási jegyzék kifüggesztése, a tárgyalás nyilvánossága vagy zárt tárgyalás elrendelése, valamint az 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 elengedtethetetlenül szüksége időszakra korlátozódik. Másrészt a bűnügyi adatkezelés során figyelembe kell venni az érintettek kategóriáit, mivel ez meghatározza az alkalmazandó adatvédelmi szabályozásból adódó jogokat és korlátokat.
Az Infotv. rendelkezései alapján a bíróság az adatkezelő szerepét tölti be a vádeljárás során, tehát az érintetti jogok és korlátozások tekintetében rendelkezhet. [Infotv. 7.§ (1) a) –d)], és [Infotv. 7.§ (4)]
Véleményem szerint a bíróság mérlegelési jogkörét figyelembe véve, amennyiben az eljáró bíró úgy ítéli meg, hogy valamely - az eljárásban felsorolt egyéni kategóriák szerinti megkülönböztetés alapján - személyes adat védelméhez az elengedhetetlenül szükséges, a Be. szerinti „erkölcsi okból” [Be. 436.§. (4) a)] elrendelheti a zárt tárgyalást. (Mándi 2023)

De lege ferenda javaslatom ezzel kapcsolatban a Be. taxatív felsorolásainak ilyen irányú módosítása. [Be. 436.§. (4) c)]. A 436. szakasz (4) bekezdése c) pontjának - „*minősített adat és egyéb védett adat védelme érdekében*” kiegészítését javasolnám az alábbiak szerint: - „*minősített adat és egyéb védett adat védelme érdekében, valamint olyan személyes adat esetében melynek védelméhez az elengedhetetlenül szükséges különös tekintettel az érintettek kategóriái közötti különbségtételre.”*

Felmerül a kérdés az **„**az elengedhetetlenül szükséges**”** meghatározás értelmezését illetően.

A Be. használja ezt a kifejezést, a személyes adatok zárt kezelése esetében a személyes adatot az áldozat 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 (Mándi 2023, Németh 2023) 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 után sikeresen reintegrálódjanak a társadalomba, a büntetett előéletből adódó hátrányok nélkül. Ezzel összefüggésben az online térben közzétett bírósági tárgyalásokról szóló tudósítások esetében megjelenő személyes adatok, mint az elítéltek neve, a bűncselekmények és a kiszabott büntetések, hosszú távon is hozzáférhetővé válnak, (Németh 2019, Kőhalmi 2023, Márki 2023) 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 (Havasiné 2017, Márki 2023, Kőhalmi 2023).
Véleményem szerint a sajtónyilvánossággal kapcsolatban egyensúlyt kell biztosítani a közvélemény tájékoztatásának jogos igénye és az egyének magánszférája, személyes adatokhoz való jogának védelme között. A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény, hangsúlyozza, hogy a sajtószabadság gyakorlása nem eredményezheti bűncselekmény elkövetését vagy annak felhívását, nem sértheti a közízlést, továbbá nem sértheti harmadik fél személyhez fűződő jogait. (2010. évi CIV. törvény)
A médiatartalom-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 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.

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 rendszerek használatát a büntésvégrehajtásban. Az AI alapú rendszerek adatvédelmi problémái közé tartozik a személyes adatok bizalmas kezelése, az adatok szükségtelen gyűjtése és tárolása, valamint a diszkrimináció lehetősége (Schmehl 2020, Mezei 2022, Eszteri, Péterfalvi 2022, Herke 2023). Az 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. Adatkezeléskor csak hiteles, megbízható forrásból származó adatok használata lehetséges, készen állva a nemzetközi bűnügyi vonatkozásokkal kapcsolatos AI-adatigénylések támogatására. (Nagy, 2021).
A büntetésvégrehajtás 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 büntetésvégrehajtás 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.

3.Hipotézis

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.

Megállapítható, hogy a GDPR és a LED szabályozásai, melyek a személyes adatok védelmét hivatottak biztosítani, alapvetően hozzájárulnak a kiberbiztonsághoz is. (Porcedda 2012, Bederna,2018, Moore, Anderson 2019, Wicki-Birchler 2020, Schreiber 2021, Hirvonen 2022)

Ezzel kapcsolatban az alábbi pontokban foglaltam össze a legfontosabb tényezőket.

1. Proaktív védelem: A GDPR előírja az adatvédelmi intézkedések beépítését az információs rendszerek tervezési fázisában (beépített adatvédelem elve), valamint az adatvédelmi intézkedések folyamatos fenntartását az adatok kezelésének egész folyamata során. Ez magában foglalja a titkosítást, a hozzáférés-szabályozást, az adatok integritásának és biztonságának fenntartását. Ezek az intézkedések jelentősen csökkenthetik a kiberbűnözők által kihasználható kockázatokat, például jogosulatlan hozzáférését adatainkhoz, vagy az adatlopást. (GDPR, Preambulum (8), 47. cikk d))
2. Adatkezelési elvek: A GDPR és a LED az adatminimalizálás elvét is előírja, amely szerint csak a feltétlenül szükséges adatok gyűjthetők és tárolhatók, és csak meghatározott, világos és jogszerű célokra. Ez az elv csökkenti a kiberbűnözők számára elérhető érzékeny információk mennyiségét, ezzel minimalizálva az adatokkal visszaélés kockázatát. [GDPR, 5. cikk c)]
3. Adatvédelmi hatásvizsgálat: A GDPR előírja az adatvédelmi hatásvizsgálat elvégzését magas kockázatot jelentő adatkezelési műveletek esetén, mint például nagy mennyiségű személyes adat feldolgozása vagy különösen érzékeny adatok kezelése. Ez lehetővé teszi az adatkezelési tevékenységek kockázatainak azonosítását és kezelését, így proaktív védelmet nyújthat a kiberfenyegetésekkel szemben. (GDPR, 35. cikk)

4. Hozzáférés-vezérlés és felhasználói jogosultságok Mind a GDPR, mind a LED szigorú követelményeket állapít meg a személyes adatokhoz való hozzáférés kezelésére. A szervezeteknek gondosan kell szabályozniuk, hogy ki férhet hozzá az adatokhoz, ezzel csökkentve a jogosulatlan hozzáférés kockázatát. (GDPR, Preambulum (73), 15. cikk)
5. Incidenskezelés és értesítés: A GDPR kötelezővé teszi az adatvédelmi incidensek, például adatsértések nyilvánosságra hozatalát és jelentését az illetékes hatóságoknak, valamint érintett egyének értesítését, ha az incidens valószínűleg magas kockázatot jelent az érintettek jogaira és szabadságaira. Ez hatással lehet a kibertámadások okozta károk enyhítésére. [GDPR, Preambulum (49), (85) – (88), 33. cikk.]

Az (EU) 2022/2555 irányelve (NIS2) számos kötelezettséget ró a tagállamokra a kiberbiztonság területén, ezek egy része speciális adatvédelmi követelményeket is meghatároz, összhangban a GDPR-ral. Ez magában foglal néhány olyan előírást is, ahol az adatvédelmi és kiberbiztonsági követelmények átfedik és kapcsolódnak egymáshoz, úgy, mint a biztonsági intézkedések, adatvédelmi szabályzatok, az auditok, ellenőrzések, az incidensek, az adatfeldolgozói szerződések, és az adatkezelési tájékoztatók területén.

A NIS Irányelvet a GDPR kiegészítő jogszabályként lehet tekinteni, amely megfelelő biztonsági kötelezettségeket és új bejelentési kötelezettségeket vezet be bizonyos iparágakban és digitális szolgáltatásnyújtók számára.(Cole, Schmitz 2019).

A 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 jelentős szerepe van a kiberbűnözés elleni küzdelemben, így a harmadik hipotézisemet elfogadom.

4.Hipozézis

A személyes adatokkal kapcsolatos bűncselekmények büntetőjogi tényállásai és az ehhez szorosan kapcsolódó információs rendszer elleni bűncselekmények tényállásai megfelelnek az uniós keretrendszernek, azonban nem mindig fedik le teljes körűen a digitális térben elkövetett személyes adatokkal kapcsolatos bűncselekményeket a szankciókat illetően.

Az adatvédelem, mint az egyén alapvető joga, információs önrendelkezés jogaként került meghatározásra az Alkotmánybíróság 15/1991. (IV. 13.) AB határozatában, származtatva azt, az emberi méltósághoz való jogból és a személyes adatok védelmének jogából. Az Alaptörvény VI. cikkének (2) bekezdése ezt a jogot, mint alapvető jogot rögzíti, biztosítva mindenki számára a személyes adataik védelméhez való jogot (Eszteri, Péterfalvi 2017). A Büntető Törvénykönyv

XXI. fejezete, amely az emberi méltóság és egyes alapvető jogok elleni bűncselekményeket tárgyalja, szabályozza a személyes adatokkal kapcsolatos visszaélés bűncselekményét. A személyes adattal való visszaélés jogi megfogalmazása a Büntető Törvénykönyv úgynevezett keret diszpozíciói közé esik. 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 **(**Belovics és mts.2014, Péterfalvi, Eszteri, 2017)
A büntetőjogi keretet elsősorban a GDPR szabályai töltik meg tartalommal, amennyiben az adott adatkezelési tevékenységre a GDPR tárgyi hatálya kiterjed. Azokban az esetekben, amikor az adatkezelés a GDPR 2. cikk (2)-(4) bekezdései alapján kívül esik a rendelet hatálya alól, az adatkezelési normákat subszidiáriusan az Infotv. határozza meg**. (**Jóri 2018**)** Abban az esetben, ha a személyes adatok kezelése bűnüldözési, nemzetbiztonsági, vagy honvédelmi célból történik, az Infotv. előírásait kell alkalmazni.

A Büntető Törvénykönyv 219.§-a határozza meg a személyes adattal való visszaélés bűncselekményének jogi definícióját. A bűncselekmény passzív alanyát elkövetési tárgyát illetően a szakirodalom nem képvisel egységes állaspontot. A személyes adat fogalmát a GDPR és az Infotv. határozza meg, lényegi eleme az érintettel kapcsolatba hozható bármely információ.[Infotv. 3.§ (10)] Ennek alapján Szomora álláspontjával értek egyet, (Szomora 2014,2019) amely szerint a személyes adatok nem tekinthetők a bűncselekmény tárgyának, különös tekintettel arra, hogy azok igazságtartalmuktól függetlenül kapcsolatba hozhatók az adott személlyel.
Az elkövetési alakzatok elsősorban a GDPR által felsorolt elvek, úgymint a jogszerűség, a célhoz kötöttség és az adattakarékosság adatvédelmi elvének megfelelő érvényesülését hivatottak biztosítani. [GDPR 5. cikk (1) a)–c)]
A tényállással kapcsolatban ismertettem a szakirodalom álláspontját a személyes adattal kapcsolatos „azonosított vagy azonosítható” fogalmakat illetően, (Pók,2019, Czapáry, Szőke 2022) tekintettel arra, hogy meghatározza a személyes adat fogalmának értelmezését.
A meghatározás jelentőségét mutatja, hogy egy Kúriai döntés jelentős szakmai vitákat váltott ki, az értelmezést illetően, amelynek kapcsán az azonosított, az azonosíthatóság, és a személyes adatra vonatkoztatható fogalmak értelmezési problémája merült fel. (BH 2019.272)
Egy adat vagy információ akkor tekinthető személyre vonatkozónak, ha legalább egy az alábbi három kritérium közül teljesül: tartalom, cél vagy eredmény. (Pók,2019) Az információ akkor vonatkozik egy személyre, ha közvetlenül az adott személyre utal, függetlenül attól, hogy az adatkezelő vagy bármely harmadik fél milyen célból kezelte, vagy milyen hatást gyakorol az információ az érintettre. (WP 136, 4/2007) Felvetődik a kérdés ezzel kapcsolatban, hogy bizonyos esetben, az adatkezelőnek technikailag meglenne a lehetősége, de nem áll szándékában az azonosítás. Ezt a helyzetet úgy kell megítélni, hogy nem kizárólag az adatkezelő ezzel kapcsolatos szándéka számít, hanem az, hogy az ügy összes körülménye alapján észszerűen feltételezhető-e, hogy az adatokat az érintett azonosítására fogja használni. (Czapáry, Szőke 2022)
Egy személyt „azonosítottnak” tekinthetünk, ha kiemelkedik egy csoport többi tagjából. (WP 136, 4/2007) Azonosítható” egy személy akkor, ha lehetséges az azonosítása, még ha ez eddig nem is történt meg. Ennek a képességnek a megléte határozza meg, hogy az információ ebből a szempontból releváns –e. (Pók 2019) Ezzel kapcsolatban felmerül, hogy a személyes adattal

való visszaélés jogi tényállása nem nyújt megfelelő védelmet bizonyos helyzetekben, mint például a tömeges és a teljes személyiségprofilozás, a kiskorúak védelme, valamint a deepfake jelenségek esetén.(Miskolczi, Szathmáry 2019).
Fontos különbséget tenni az érintett azonosítása vagy azonosíthatósága és a személyazonossága között. Az előbbi esetben az adatok lehetővé teszik az érintett különválasztását környezetétől vagy az ott lévő többi személytől, míg a személyazonosság meghatározása azt teszi lehetővé, hogy pontosan ki azonosítható az adott egyén.(Pók 2019)
A személyes adatok fogalmának és büntetőjogi védelmének értelmezése fontos.
Miközben a GDPR közvetlenül hatályos és alkalmazandó az Európai Unió tagállamaiban, nem írja elő a személyes adatok védelmét a büntetőjog keretein belül. Ezzel együtt, a GDPR kiemeli, hogy az EU tagállamainak jogukban áll büntetőjogi szankciókat előírni a rendelet sérelme esetén. [EU 2016/679 Preambulum (149)] A Magyar Büntető Törvénykönyv (2012. évi C. törvény) nem ad explicit definíciót a személyes adatokra, hanem az „Az Európai Unió jogának betartása" fejezetben, utalás történik azok szabályozására,[465.§ (2) d)], az ennek végrehajtásához szükséges intézkedéseket megállapítására.(Btk.219.§)

A tiltott adatszerzés és az információs rendszer elleni bűncselekmények kapcsán az információs rendszer vagy adat megsértése (Btk.423) kapcsán, az adatok hozzáférhetetlenné tételével kapcsolatban a külső fizikai hozzáférhetetlenség kérdése, merült fel. (Szathmáry 2022). 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.
Álláspontom szerint a tágabb értelmezést kell elfogadni ebben az esetben. Ennek megfelelően a „fizikai külső" tényezők biztosítását, és az informatikai rendszer működőképességének biztosítását is szükségesnek tartom az alábbi indoklás alapján: Az adatok hozzáférhetősége ma már adatbiztonsági kérdés. Az adatbiztonsági intézkedések alapján az adatkezelő vagy az adatfeldolgozó megfelelő műszaki és szervezési intézkedéseket tesz. [Infotv. a 25/I §. (1).] Biztosítja „*az adathordozók (...) eltávolításának megakadályozását,* [Infotv. 25/I.L.(3)b)] valamint hogy „ *üzemzavar esetén az adatkezelő rendszer helyreállítható legyen*"[Infotv. 25/I.L.(3)i)] „valamint azt, hogy az adatkezelő rendszer működőképes legyen"[Infotv. 25/I.L.(3)j)]. Mindezek alapján véleményem szerint a fizikai tényezők által, és a rendszer működésének egyéb módon történő akadályoztatásait is a tényállás részeinek kellene tekinteni.

Az információbiztonság elleni cselekmények nemcsak a közvetlenül védett információs rendszert érintik, hanem annak szélesebb környezetében, a rendszerelemeken keresztül is megvalósulhatnak. Az információs rendszer biztonságát közvetlenül érintő támadások tipikusan az információs rendszer vagy adat megsértése (Btk.423. §.) tényállás alá esnek, míg a közvetett vagy előkészítő jellegű tevékenységek, mint például a social engineering vagy a jelszavak és egyéb azonosítók megszerzésére irányuló adathalászat, amelyek az információs

rendszert kezelő személyeket célozzák, az információs rendszer védelmét biztosító technikai intézkedések kijátszása (Btk.424. §) szerint minősülhetnek.

A jelenleg hatályos Büntető Törvénykönyv szabályozása a személyes adatok védelme és az információs rendszerekkel kapcsolatos tényállások tekintetében összhangban áll az uniós előírásokkal. Ezeket a kereteket az Általános Adatvédelmi Rendelet és a Bűnügyi Adatvédelmi Irányelv alapján az Infotv. határozza meg. A Btk. rendelkezik 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.

III. Az értekezés eredményeinek hasznosíthatósága

III. 1. A jogelmélet számára hasznosítható eredmények

- Rövid áttekintést nyújtottam az adatvédelem fogalmával kapcsolatosan, annak kialakulásáról, a fogalom evolúciójáról és elméleteiről.
- Az adatvédelem fogalmát illetően, annak gyakorlati szempontú megközelítésű definícióját alkottam meg.
- Röviden áttekintettem az adatvédelmi jog fejlődésének főbb állomásait, a történeti fejlődést meghatározó gazdasági-társadalmi változásokat.
- Ismertettem a személyes adatok védelmének aktuális jogi szabályozását, és intézményrendszerét.
- Ismertettem az EU 2016/680 irányelvét - a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelvet.
- Összehasonlító elemzéssel vizsgáltam az Irányelv jogharmonizációját a magyar, a svéd, a német- és francia jogalkotásba, az adott jogszabályok rövid bemutatásával.
- Bemutattam a magyar büntetőeljárás- és büntetés-végrehajtás jogszabályi hátterét, kiemelve az adatvédelemmel összefüggő szabályokat.
- Bemutattam a személyes adatok védelméhez kapcsolódó büntetési szankciókat meghatározó kódexünk szabályozását is.
- Röviden ismertettem a kiberbűnözés hátterét, kapcsolatát az adatvédelemmel.

- A digitális térben elkövetett bűncselekmények és az adatvédelem közötti összefüggéseket részletesen elemeztem, különös hangsúlyt fektetve a személyes adatok védelmének jelentőségére.

.

III. 2. A jogalkotás számára hasznosítható eredmények

- De lege ferenda javaslatot fogalmaztam meg a 2017. évi XC. törvény a büntetőeljárásról szóló törvénnyel kapcsolatban. (Be.) Adatvédelmi aggályok esetében a zárt tárgyalás elrendelését a Be. nem tartalmazta. Álláspontom szerint a bíróság mérlegelési jogkörét figyelembe véve, amennyiben az eljáró bíró úgy ítéli meg, olyan személyes adat esetében melynek védelméhez az elengedhetetlenül szükséges, a .Be. 436.§. (4) c bekezdés módosítása esetén, a bíró elrendelhetne zárt tárgyalást.
  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.”*

III. 3. A jogalkalmazás számára hasznosítható eredmények

- Felhívtam a figyelmet a büntetőeljárás és a büntetésvégrehajtás jogszabályainak adatvédelmi szempontú vizsgálata során, annak gyakorlati szempontú megvalósulása esetén lehetséges kollízíókra és adatvédelmi aggályokra. A tárgyalás során 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 aktuális törvényi szabályozás a megoldást magában hordozza, azonban az ágazati jogszabályokat és a végrehajtási jogszabályokat is egyeztetni és vizsgálni szükséges az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)megfelelő rendelkezéseivel.
- A jogszabályi háttér tekintetében nem csak a törvényi szabályozás, hanem rendeletek, utasítások, szabályzatok is tartalmaznak adatvédelmi előírásokat az egyes területeknek megfelelően. A jogszabályok hierachiájában az azonos szintű törvények – mint például a 2013. évi CCXL. (Bvtv.) és az 1997. évi XLVII. törvény (Eüaktv.) - ellentmondásait a jogalap meghatározása oldhatja fel.
- Felhívtam a figyelmet arra, hogy az adatkezelő szervek, - jelen esetben a büntető igazságszolgáltatásban eljáró 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. Summary

The thesis provides a comprehensive overview of the EU and national legislation on the protection of personal data in the context of the Law Enforcement Directive.
It also analyses in detail the challenges of transposing the Directive into national law and the regulatory issues related to criminal procedure, law enforcement and sanctions. From the perspective of data security and cybercrime protection, it highlights the legal and practical aspects of misuse of personal data and offences against information systems.
The research highlights the importance of the practical application of legislation and the need for harmonisation and uniform interpretation of the law. The final conclusions of the study suggest that close cooperation between the EU and Member States, exchange of best practices and continuous review of the data protection framework are essential to achieve a coherent European data protection regime.

V. A szerző publikációs jegyzéke

Gáti, B. „A gazdasági válság hatásai a személyes adatok védelmére és annak büntetőjogi aspektusaira.” In Válságok és büntetőjog: Fiatal büntetőjogászok első konferenciája, szerk. M. Nagy és D. Ripszám, 67–92. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2023.

Gáti, B. “Data Protection Aspects of the Use of Facial Recognition Systems for Law Enforcement.” In Law Between Creation and Interpretation, edited by D. Ćeranić, S. Ivanović, R. Lale, and S. Aličić, vol. 3, 306–327. East Sarajevo, Bosnia and Herzegovina: Faculty of Law, University of East Sarajevo, 2023.

Tóth, D., and B. Gáti. “The Common Law Approaches to Identity Theft: Implications for Hungarian Law Reform.” Problemy Prawa Karnego 7(1): 1–13, 2023.

Gáti, B. „The Main Types of Cybercrime during the COVID-19 Pandemic.” In III. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai, szerk. Á. L. Bendes, Sz. Diósi, Zs. Gáspár, B. Gáti és N. Projics, 13–39. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, 2022.

Gáti, B. "Some Aspects of Data Protection in Criminal Justice." JURA 28, no. 3: 25–41, 2022.

Gáti, B. „Adequacy Aspects of Police and Judicial Cooperation in Criminal Matters in EU Legislation.” In Válság, technológia és jog: Konferenciakötet, szerk. Zs. Bujtár, Zs. Gáspár, B.

Breszkovics, Sz. Ázsoth, A. R. Szívós, B. Ferencz és M. Martin, 78–89. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2022.

Gáti, B. „A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései.” In FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI: KONFERENCIAKÖTET, szerk. Zs. Bujtár, Zs. Gáspár, Cs. Szilovics, B. Breszkovics, B. Ferencz, Sz. Ázsoth és M. Martin, 59–78. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2022.

Gáti, B. „A Schrems II. ítélet lehetséges hatásai a nemzetközi jogalkotásra.” In Az internet és a közösségi média jogi kihívásai – Konferenciakötet, szerk. D. Tóth, 18–35. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, 2022.

Gáti, B. „Certain Privacy Related Aspects of Cybercrime and Digital Forensics.” In Biztonság és jog: Konferenciakötet, szerk. L. Kőhalmi, G. Kulcsár, D. Tóth, B. Gáti és E. Sándor, 19–48. Pécs, Hungary: PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, 2022.

Gáti, B. „Az adatvédelmi szabályozás aktuális tendenciái a büntető igazságszolgáltatás területén.” In IV. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai, szerk. Á. L. Bendes, Zs. Gáspár, B. Gáti, N. Projics és D. Tóth, 42–61. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2022.

Gáti, B. „Az adatvédelmi jog fejlődésének főbb állomásai.” Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai 23(1): 153–168, 2022. https://doi.org/10.46942/SIDM.2022.1.153-168.

Gáti, B. “Some Data Protection Issues of the EU Regulation of Artificial Intelligence.” In Contradictions of the Contemporary Law, vol. 2, 588–605. Sarajevo, Bosnia and Herzegovina: Копикомерц, Источно Сарајево, 2022.

Gáti, B. „Possible Links between Digitalization, Cybercrime, and the COVID-19 Pandemic.” Büntetőjogi Szemle 10, különszám: 23–33, 2021.

Gáti, B. „Az adatvédelem számítástechnikai bűnözéssel összefüggő aktuális kérdései – Adatvédelmi kérdések a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv Tervezetével kapcsolatban.” In PhD Tanulmányok 15., szerk. L. Kőhalmi, 23–58. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, 2021.

Gáti, B. “Some Aspects of Data Protection in Criminal Justice.” In 10th Jubilee Interdisciplinary Doctoral Conference: Book of Abstracts, edited by L. F. Kajos, C. Bali, Zs. Preisz, P. Polgár, A. Glázer-Kniesz, Á. Tislér, and R. Szabó, 128. Pécs, Hungary: Pécsi Tudományegyetem Doktorandusz Önkormányzat, 2021.

Gáti, B. “Transformation of the Digital World and Cybercrime During Covid-19 Pandemic.” In Dreptul Crizei: Crizele Dreptului, 56–74. Timișoara, Romania: Universitatea de Vest din Timișoara, Facultatea de Drept, 2021.

Gáti, B. „Major Legal and Economic Aspects of Digitalization in the EU with Special Attention to Recent Developments on Data Protection.” In Gazdaság és pénzügyek a 21. században II., szerk. Cs. Szilovics, Zs. Bujtár, B. Ferencz, B. Breszkovics és A. R. Szívós, 139–154. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2020.

Gáti, B. „A Kiberbűnözés Jellegzetességei és a COVID-19 járvány kapcsolata a statisztikák tükrében.” In Rendészet a rendkívüli helyzetekben: húsz éves a Szent László napi konferencia, szerk. Gy. Gaál és Z. Hautzinger, 111–120. Pécs, Hungary: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2021.

Tóth, D., and B. Gáti. „Risk Analysis of Certain Economic Crimes.” In Gazdaság és pénzügyek a 21. században II., szerk. Cs. Szilovics, Zs. Bujtár, B. Ferencz és A. R. Szívós, 170–181. Pécs, Hungary: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2020.

Az értekezés témaköréhez nem kapcsolódó közlemények:

Tóth, D., and B. Gáti. “Comparative Law Analysis of the Regulation of Stamp Forgery.” Police Studies: The Periodical of the Police Scientific Council 2(1–2): 56–78, 2022.

Tóth, D., és B. Gáti. „Összehasonlító jogi elemzés a bélyeghamisítás szabályozásáról.” Rendőrségi Tanulmányok 5 (3): 121–144, 2022.

Szerkesztett kötetek:

Bendes, Á. L., Gáspár, Zs., Gáti, B., Projics, N., Ripszám, D., és Tóth, D., szerk. V. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai. 214 p. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, 2023. ISBN: 9789636261405.

Bendes, Á. L., Gáspár, Zs., Gáti, B., Projics, N., és Tóth, D., szerk. IV. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai. n.p. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, 2022. ISBN: 9789634299912.

Bendes, Á. L., Diósi, Sz., Gáspár, Zs., Gáti, B., Projics, N., és Tóth, D., szerk. III. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai. 188 p. Pécs, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola, 2022. ISBN: 9789634299141.

Kőhalmi, L., Kulcsár, G., Tóth, D., Gáti, B., és Sándor, E., szerk. Biztonság és jog: Konferenciakötet. Pécs, Magyarország: PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, 2022.

VI. Irodalomjegyzék

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.