

Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

NEM VÉGLEGES VÁLTOZAT

Gáti Balázs

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

Doktori értekezés tézisei



Témavezetők:

Prof. habil. Dr. Kóhalmi László tanszékvezető, egyetemi tanár
Dr. Tóth Dávid egyetemi adjunktus

Pécs, 2024

Tartalomjegyzék

I. Bevezetés	3
1. A témaválasztás indoklása, aktualitása.....	3
2. A kutatás módszerei.....	5
3. A kutatás célja	5
II. Az eredmények bemutatása	6
1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése	6
2. A kutatással elérni kívánt célok bemutatása, a hipotézisek megválaszolása.....	7
III. Summary	14
IV. A szerző publikációs jegyzéke	15

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)

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 keretrendszer 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.

1. A témaválasztás indoklása, aktualitása

Témaválasztásom indoka, hogy a bűnügyi személyes adatok védelmének szabályozása, jogharmonizációja és gyakorlata az Európai Unió tagállamaiban eltérő lehet, ami kihívásokat és komplex jogi kérdéseket vet fel az adatvédelmi normák egységes értelmezése, ennek

következtében az adattovábbítás, a határokon átnyúló bűnügyi együttműködés (Kóhalmi, 2010, Eszteri 2021) szempontjából. Az európai adatvédelmi jogharmonizáció és az egyes tagállamok gyakorlatának összevetése rávilágíthat arra, hogy mely területeken szükséges további összehangolás vagy jogalkotási intézkedés, hogy a bűnüldözés és az adatvédelem közötti egység biztosított legyen az Unió területén (Gál I., Tóth M. 2016, Jánosi 2022).

Alapvető fontosságú, hogy hogyan járul hozzá az adatvédelmi reform a nemzetközi bűnözés elleni küzdelemhez a hazai és az egyes tagállami jogi szabályozás gyakorlata révén (Kóhalmi 2012, Bendik, 2020). Ezen belül fontosnak tartom az Európai Bizottság (továbbiakban Bizottság) által véleményezett és vizsgált gyakorlatot, és annak nemzeti jogba történő átültetését, amely irányadó a büntetőjogi szabályozás területén is (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, Gyarak, 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. (Szijártó, 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).

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. 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 biztosításában (Csiszár 2019, Fenyvesi 2019, Gyarakai 2022)

2. 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 részeken a logikai és kritikai elemzéssel kiegészítve.

3. 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. 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.

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.

1. Az adatvédelem fogalmának gyakorlati szempontú megközelítése

A II. fejezetben az adatvédelem fogalmának és történetének rövid áttekintése után bemutattam a vonatkozó aktuális uniós szabályozást és annak intézményrendszerét. Az adatvédelem fogalmát illetően, annak gyakorlati szempontú megközelítését tartottam fontosnak, figyelembe véve az értekezés során vizsgált szempontokat. Ennek megfelelően a személyes adatok védelme – véleményem szerint gyakorlati szempontból - nem más, mint, a természetes személyek jogainak és szabadságainak védelme a természetes személyek személyes adataihoz fűződő önrendelkezési jog gyakorlási körülményeinek meghatározása által, - valamint a természetes személyek személyes adatait kezelő adatkezelőkre vonatkozó adatkezelési feltételek szabályozása által.

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

A rendelkezési jognak vannak korlátai mindkét irányból. Az adatkezelés mint fogalom maga is jogszabály által szabályozott rendelkezési jogosultság az érintett személyes adatai felett. [GDPR 4.cikk. 2.).]. Az adatkezelő által végzett adatkezeléseknek, vagyis a személyes adatokon végrehajtott valamely műveleteknek vannak bizonyos korlátai. Ha elméleti síkon egy mérleg két serpenyőjébe helyeznénk az érintett személyes adatait érintő rendelkezési jogosultságokat adatkezelői, valamint érintett oldalról egyaránt, akkor általános következtetésként elmondható lenne, hogy a személyes adatokkal kapcsolatos rendelkezési jogosultságoknak több jogszabályi korlátja van adatkezelői oldalon, mint érintetti oldalon.

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

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

A hatósági típusú adatkezelések - ideértve a büntügyi típusú adatkezeléseket is - során jellemzően az előbbi mérleges példával ellentétben az adatkezelők rendelkezési jogosultsága van túlsúlyban. Ezen belül a büntügyi célú adatkezelések a büntetőjog ultima ratio elvet megtestesítő jellege okán jellemzően magukon hordozzák a hatósági jogosultságok többletét a hatósági eljáráson belül megvalósuló adatkezelések tekintetében.

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

A III. fejezetben a büntügyi 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.

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 büntügyi 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. A büntügyi adatvédelmi irányelv tagállami átültetése a magyar, a német, a francia- és a svéd nemzeti jogrendszerekbe az általános adatvédelmi rendelettel csaknem egyidőben történt.

A magyar, a német és a francia jogalkotó mindkét uniós jogszabályt egységesen, a nemzeti adatvédelmi szabályozás szerinti korábbi törvény keretében, módosító törvényjavaslattal ültette át, megtartva azok uniós szabályozással nem ellentétes rendelkezéseit. A svéd jogalkotás annyiban különbözik, hogy a korábbi adatvédelmi rendeleteket hatályon kívül helyezve új jogszabály megalkotásával alkalmazta az általános adatvédelmi rendeletet, és ugyanígy

implementálta a bűnügyi irányelvet is, megfelelően a korábbi jogi szabályozásnak, külön törvényi szabályozás keretei között.

Megállapítottam, hogy a tagállamok között vannak eltérések a bűnügyi irányelv átültetésében.

A hatályt illetően a közrend és a közbiztonság azok a fogalmak, melyekhez a tagállamok egy része a nemzetbiztonságot is köti, áttételesen a közrend megzavarására alkalmas bűncselekmények által. Ez láthatóan a magyar, a német és a korábbi francia joggyakorlatban is megjelent. A svéd adatvédelmi törvény hatálya pontosan követi az irányelvi szabályozást.

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 Integritésvédelmi Bizottság felügyeleti hatóság közösen látja el. A távközlési szolgáltatóknak csak a Svéd Posta és Távközlési Hatóság felé kell bejelenteniük a biztonsági eseményeket, azaz nem az IMY-nek, még akkor sem, ha az incidens személyes adatok megsértését is magában foglalja.

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 büntetőeljárás 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.§)

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.

A bűnüldözési célú adatkezelések uniós szabályozása nem rendeleti formában, hanem irányelvi megfogalmazás keretei között jött létre, ami tág mérlegelési jogkört biztosított a tagállamok részére. A "bűncselekmény", "közbiztonság" és "illetékes hatóság" fogalmak értelmezési különbségei jelentek meg, ami befolyásolja a hatály fogalmának értelmezését. Az eltérések abból is adódnak, hogy a LED nem ad egységes meghatározást ezekre a fogalmakra.

Véleményem szerint az irányelv végrehajtásának további pontosítása érdekében fontos a tagállamok közötti együttműködés erősítése, a legjobb gyakorlatok cseréje, az Európai Bizottság, az Adatvédelmi Testület iránymutatásai, a folyamatban lévő EUB döntések által nyújtott iránymutatások és támogatások hatékony alkalmazása. Emellett szükség lehet az irányelv felülvizsgálatára a fogalmak pontosítása szempontjából, valamint, hogy egyértelműbbé tegyék a személyes adatok különleges kategóriáinak feldolgozásával, valamint az automatizált döntéshozatallal kapcsolatos szabályozást.

Álláspontom szerint azonban jelenleg az Irányelv megfelelő keretrendszert biztosít a tagállamok számára, a fogalmak értelmezése tekintetében az EUB gyakorlata megfelelő útmutatást ad, úgy, mint a személyes adatok különleges kategóriái, valamint az automatizált döntéshozatal kérdésköre. Az EDPB által kialakított gyakorlat és a kötelező érvényű döntések képesek a technikai fejlődés által megkívánt kiegészítéseket a szabályozási folyamatba „kívülről” beépíteni.

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 IV. fejezetben az adatvédelmi szabályoknak való megfelelést az eljárás különböző szakaszaiban, a Büntetőeljárásról szóló törvény szabályozását figyelembe véve vizsgáltam. (Király 2000, Fenyvesi, Herke, Tremmel 2004, Nyíri 2018, Herke 2018, Fantoly, Budaházi 2019).

Részletesen áttekintettem, hogyan határozzák meg a jogszabályok a gyanúsítottak tanúk, vádlottak és sértettek személyes adatainak kezelését, valamint milyen potenciális problémákat vetnek fel az eljárás során. (Hesz, Köhalmi 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, Köhalmi 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 elengedhetetlenül szüksége időszakra korlátozódik. Másrészt a bűnügyi adatkezelés során figyelembe kell venni az érintettek kategóriáit, mivel ez meghatározza az alkalmazandó adatvédelmi szabályozásból adódó jogokat és korlátokat.

Az Infotv. rendelkezései alapján a bíróság az adatkezelő szerepét tölti be a vádeljárás során, tehát az érintetti jogok és korlátozások tekintetében rendelkezhet. [Infotv. 7.§ (1) a –d)], és [Infotv. 7.§ (4)]

Egyetértve Mándi felvetésével, a bíróság mérlegelési jogkörét figyelembe véve, amennyiben az eljáró bíró úgy ítéli meg, hogy valamely - az eljárásban felsorolt egyéni kategóriák szerinti megkülönböztetés alapján - személyes adat védelméhez az elengedhetetlenül szükséges, a Be. szerinti „erkölcsi okból” [Be. 436.§. (4) a)] elrendelheti a zárt tárgyalást. (Mándi 2023)

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

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

A Be. használja ezt a kifejezést, a személyes adatok zárt kezelése esetében a személyes adatot az áldozat segítség és pártfogói felügyelet ellátásához „elengedhetetlenül szükséges” mértékben lehet továbbítani. [Be. 99. § (5) b)] Használja továbbá a minősített adat felhasználása esetén, azaz a bíró és az ügyész „elengedhetetlenül szükséges” mértékben kezelhet minősített adatot feladatai végrehajtásához, [Be.104.§. (2)] Használja a különleges bánásmódot igénylő 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 egyetérték Mándi és Németh álláspontjával, amennyiben az eljárás ügyszámának önmagában történő kifüggesztése biztosíthatja az érintettek személyes adatainak védelmét. Az ügyszám csak akkor válik személyes adattá, ha az a természetes személlyel kapcsolatba hozható, és megismerhető, egyébként közérdekű adatnak minősül, ahogy ezt a NAIH is rögzíti állásfoglalásában. (NAIH/2020/294/4)

A tárgyalás nyilvánossága mellett a zártan történő eljárás esetében az ítélet nyilvános kihirdetésének problémája merült fel még adatvédelmi szempontból. Ezzel és az ehhez kapcsolódó sajtónyilvánosságával kapcsolatban a NAIH állásfoglalását tekintem irányadónak. (NAIH-4418-5/2012/V). Ennek megfelelően 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 adatok kezelhetők, a cél megvalósulásáig szükséges mértékben és ideig.

Véleményem szerint a sajtónyilvánossággal kapcsolatban egyensúlyt kell biztosítani a közvélemény tájékoztatásának jogos igénye és az egyének magánszférája, személyes adatokhoz való jogának védelme között. A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény, hangsúlyozza, hogy a sajtószabadság gyakorlása nem eredményezheti bűncselekmény elkövetését vagy annak felhívását, nem sértheti a közízlést, továbbá nem sértheti harmadik fél személyhez fűződő jogait. (2010. évi CIV. törvény)

A médiatartalom-szolgáltatóknak meg kell őriznie az emberi méltóságot a közvetített tartalmakban. [2010.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 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 (Bnytvtv) alapján.

A büntetésvégrehajtás területén a személyes adatok kezelésével kapcsolatos jogi keretek véleményem szerint szigorúak, a GDPR és az Infotv. szabályainak megfelelnek. Az adatkezelők felelőssége nagy, károkozás esetén kártérítésre és sérelemdíj fizetésére kötelezhetők. A bizonyítási teher az adatkezelőre hárul, aki köteles igazolni, hogy az adatkezelés jogszabályoknak megfelelt. Ismertettem a büntetésvégrehajtásban hazánkban használatos mesterséges intelligencia alapú rendszereket. Az MI alkalmazása adatokra támaszkodik, melyek kezelésének az uniós adatvédelmi normáknak kell megfelelnie. A rendszereknek tiszteletben kell tartaniuk az érintettek jogait, mint az adathoz való hozzáférés, helyesbítés, törlés, és az adatkezelés korlátozásának jogát. Az adatvédelmi szempontból kockázatos tevékenységek esetén előzetes adatvédelmi hatásvizsgálat elvégzése szükséges. Adatkezeléskor csak hiteles, megbízható forrásból származó adatok használata lehetséges.

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.

Megállapítottam, hogy a GDPR és a LED szabályozásai, melyek a személyes adatok védelmét hivatottak biztosítani, alapvetően hozzájárulnak a kiberbiztonsághoz is.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 hozzáférést 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 bűnüldözési irányelv és az általános adatvédelmi rendelet az Európai Unió két alapvető adatkezelésekre vonatkozó jogszabálya, amelyek az adatvédelem és az adatbiztonság területén hivatottak szabályozni az adatkezelési gyakorlatokat. A GDPR az adatkezelés alapelveire összpontosít, úgy, mint az adatminőség, az átláthatóság, az adatkezelés korlátozása, az adatbiztonság, és az elszámoltathatóság. Ezek az alapelvek különösen fontosak a kiberbűnözés kontextusában, mivel az adatvédelmi intézkedések és az adatbiztonsági protokollok közvetlenül befolyásolják a személyes adatokhoz történő jogosulatlan hozzáférés vagy azok illetéktelen felhasználásának kockázatát. A NIS 2 irányelvvel összhangban kialakuló új kibervédelmi és adatvédelmi előírások jelentős változásokat hoznak a szervezetek incidenskezelési folyamataiban. A NIS 2 Irányelv ebben az értelemben kiegészíti az adatvédelmi szabályokat.

4.Hipóézis

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 teljeskörűen a digitális térben elkövetett személyes adatokkal kapcsolatos bűncselekményeket a szankciókat illetően.

Az Alaptörvény VI. cikkének (2) bekezdése ezt a jogot, mint alapvető jogot rögzíti, biztosítva mindenki számára a személyes adataik védelméhez való jogot (Eszteri, Péterfalvi 2017). A Büntető Törvénykönyv XXI. fejezete, amely az emberi méltóság és egyes alapvető jogok elleni bűncselekményeket tárgyalja, szabályozza a személyes adatokkal kapcsolatos visszaélés bűncselekményét. A személyes adattal való visszaélés jogi megfogalmazása a Büntető Törvénykönyv úgynevezett keretdiszpozíciói közé esik. A keretdiszpozíciók sajátossága hogy a bűncselekmény Büntető Törvénykönyvben foglalt definíciója egy külső jogszabályra utal, és úgy rendelkezik, hogy a bűncselekmény a külső (extraneus) normának a Büntető Törvénykönyv által meghatározott módon történő megsértésével valósul meg (Belovics és mts.2014, Péterfalvi, Eszteri, 2017)

A 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 tárgyat illetően a szakirodalom nem képvisel egységes álláspontot. 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 ismertetem 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 tényállást illetően. Csoportból való azonosítás lehetősége ma már „technikai kérdés”. 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). Zárójelben jegyzem meg, a kérdést bonyolítja a mesterséges intelligencia alkalmazásának adatvédelmi szabályozása, amely különös „hangsúlyt” kap a bűnügyi tudományok területén.

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). Véleményével egyetértek, 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 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 az uniós jogszabályoknak való megfelelésről. Az egyes szabályozási kérdésekkel kapcsolatban részletesen elemeztem a szakirodalmi álláspontokat, különös tekintettel a személyes adatokkal való visszaélésre vonatkozó tényállásra. A bírói ítélezési gyakorlat döntő szerepet fog játszani az információs rendszer elleni bűncselekményekkel kapcsolatos pontos jogértelmezés kialakításában.

III. 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.

IV. A szerző publikációs jegyzéke

1. Gáti, Balázs. "A gazdasági válság hatásai a személyes adatok védelmére és annak büntetőjogi aspektusaira." In: Nagy, Melánia; Ripszám, Dóra (szerk.) "Válságok és büntetőjog" : F fiatal büntetőjogászok első konferenciája, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK) (2023) pp. 67-92.,"
2. Gáti, Balázs. 2023 "Data Protection Aspects of the Use of Facial Recognition Systems for Law Enforcement." In: Čeranić, Dimitrije; Ivanović, Svjetlana; Lale, Radislav; Aličić, Samir (szerk.) COLLECTION OF PAPERS "Law Between Creation and Interpretation" Vol. 3. = ЗБОРНИК РАДОВА „Право између стварања и тумачења“ Том 3. (Zbornik radova "Pravo između stvaranja i tumačenja" Tom 3.), East Sarajevo, Bosnia-Herzegovina : Faculty of Law, University of East Sarajevo (2023) 364 p. pp. 306-327.
3. Tóth, Dávid, Balázs Gáti. 2023. "The Common Law Approaches to Identity Theft: Implications for Hungarian Law Reform." Problemy Prawa Karnego 7 : 1 pp. 1-13. , 13 p. (2023)
4. Balázs, Gáti.. "The Main Types of Cybercrime during the COVID-19 Pandemic." In: Bendes, Ákos László (szerk.) ; Diósi, Szabolcs (szerk.) ; Gáspár, Zsolt (szerk.) ; Gáti, Balázs (szerk.) ; Projics, Nárcisz (szerk.) ; Tóth, Dávid (szerk.) III. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola (2022) , 188 p. ISBN: 9789634299141, 13–39.
5. Gáti, Balázs. "Some Aspects of Data Protection in Criminal Justice." JURA 3: 25.
6. Gáti, Balázs. "Adequacy Aspects of Police and Judicial Cooperation in Criminal Matters in EU Legislation." In: Bujtár, Zsolt; Gáspár, Zsolt; Breszkovics, Botond; Ázsoth, Szilvia; Szívós, Alexander Roland; Ferencz, Barnabás; Martin, Márton; Kálmán, Martin (szerk.) Válság, technológia és jog : Konferenciakötet - válogatott tanulmányok, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK) (2022) 107 p. pp. 78-89.
7. Gáti, Balázs. "A mesterséges intelligencia európai uniós szabályozásának egyes adatvédelmi kérdései." In: Bujtár, Zsolt; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond; Ferencz, Barnabás; Ázsoth, Szilvia; Szívós, Alexander Roland; Martin, Márton (szerk.) FINTECH – DEFI - KRIPTOESZKÖZÖK GAZDASÁGI ÉS JOGI LEHETŐSÉGEI ÉS KOCKÁZATAI : KONFERENCIAKÖTET – VÁLOGATOTT TANULMÁNYOK, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK) (2022) pp. 59-78. ,
8. Gáti, Balázs. "A Schrems II. ítélet lehetséges hatásai a nemzetközi jogalkotásra." In: Tóth, Dávid (szerk.) Az internet és a közösségi média jogi kihívásai – Konferenciakötet,

- Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés- végrehajtási Jogi Tanszék (2022) 142 p. pp. 18-35.
9. Gáti Balázs. “Certain Privacy Related Aspects of Cybercrime and Digital Forensics.” In: Kóhalmi, László; Kulcsár, Gabriella; Tóth, Dávid; Gáti, Balázs; Sándor, Enikő (szerk.) Biztonság és jog : Konferenciakötet, Pécs, Magyarország : PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék (2022) pp. 19-48..
 10. Gáti Balázs.. “Az adatvédelmi szabályozás aktuális tendenciái a büntető igazságszolgáltatás területén.” In Bendes, Ákos László (szerk.) ; Gáspár, Zsolt (szerk.) ; Gáti, Balázs (szerk.) ; Projics, Nárcisz (szerk.) ; Tóth, Dávid (szerk.) IV. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola (2022) ISBN: 9789634299912 , 42–61.
 11. Gáti Balázs.. “Az adatvédelmi jog fejlődésének főbb állomásai.” STUDIA IURISPRUDENTIAE DOCTORANDORUM MISKOLCIENSIVM-MISKOLCI DOKTORANDUSZOK JOGTUDOMÁNYI TANULMÁNYAI 23 (1): 153–168. doi:10.46942/SIDM.2022.1.153-168.
 12. Gáti. Balázs. 2021. Some Data Protection Issues of the EU Regulation of Artificial Intelligence. In: Collection of papers, “Contradictions of the Contemporary Law “, Vol. II, Szarajevó, Bosznia-Hercegovina : Копикомерц, Источно Сарајево (2022) pp. 588-605.
 13. Balázs, Gáti. 2021. “Possible Links between Digitalization, Cybercrime, and the COVID-19 Pandemic.” BÜNTETŐJOGI SZEMLE 10 (különszám): 23–33.
 14. Gáti Balázs.2021. “Az adatvédelem számítástechnikai bűnözéssel összefüggő aktuális kérdései - Adatvédelmi kérdések a Budapesti Egyezmény 2. Kiegészítő Jegyzőkönyv Tervezetével kapcsolatban.” In: Kóhalmi, László (szerk.) PhD Tanulmányok 15., Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola (2021) pp. 23-58.
 15. Balázs, Gáti. 2021. “Some Aspects of Data Protection in Criminal Justice.” In: Kajos, Luca Fanni; Bali, Cintia; Preisz, Zsolt; Polgár, Petra; Glázer-Kniesz, Adrienn; Tislér, Ádám; Szabó, Rebeka (szerk.) 10th Jubilee Interdisciplinary Doctoral Conference : Book of Abstracts = 10. Jubileumi Interdiszciplináris Doktorandusz Konferencia : Absztraktkötet, Pécs, Magyarország : Pécsi Tudományegyetem Doktorandusz Önkormányzat (2021), 128–128.
 16. Balázs, Gáti. “Transformation Of The Digital World And Cybercrime During Covid - 19 Pandemic.” In: Editura, Universul Juridic (szerk.) Dreptul Crizei : Crizele Dreptului, Timisoara, Románia : Universitatea de Vest din Timisoara, Facultatea de Drept (2021) pp. 56-74..
 17. Balázs, Gáti. “Major Legal and Economic Aspects of Digitalization in the EU with Special Attention to Recent Developments on Data Protection.” In: Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Breszkovics, Botond; Szívós, Alexander Roland (szerk.) GAZDASÁG ÉS PÉNZÜGYEK A 21. SZÁZADBAN II. - KONFERENCIAKÖTET = BUSINESS AND ECONOMY IN THE 21ST CENTURY II. – CONFERENCE PROCEEDINGS, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK) (2020) 207 p. pp. 139-154.

Az értekezés témaköréhez nem kapcsolódó közlemények:

1. Tóth, Dávid, and Balázs Gáti. 2022 “Comparative Law Analysis of the Regulation of Stamp Forgery.” POLICE STUDIES: THE PERIODICAL OF THE POLICE SCIENTIFIC COUNCIL 2 (1–2): pp. 56–78.
2. Tóth, Dávid, Gáti Balázs.2022. “Összehasonlító jogi elemzés a bélyeghamisítás szabályozásáról.” RENDŐRSÉGI TANULMÁNYOK 5 (3): pp. 121–144.
3. Gáti Balázs 2021 “A Kiberbűnözés Jellegzetességei És a COVID-19 Járvány Kapcsolata a Statisztikák Tükrében.” In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Rendészet a rendkívüli helyzetekben : húsz éves a Szent László napi konferencia, Pécs, Magyarország : Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport (2021) 433 p. pp. 111-120.
4. Tóth, Dávid, and Balázs Gáti. 2020. “Risk Analysis of Certain Economic Crimes.” In: Szilovics, Csaba; Bujtár, Zsolt; Ferencz, Barnabás; Breszkovics, Botond; Szívós, Alexander Roland (szerk.) GAZDASÁG ÉS PÉNZÜGYEK A 21. SZÁZADBAN II. - KONFERENCIAKÖTET = BUSINESS AND ECONOMY IN THE 21ST CENTURY II. – CONFERENCE PROCEEDINGS, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK) (2020) 207 p. pp. 170-181.

Szerkesztett kötetek:

1. Bendes, Ákos László (szerk.) ; Gáspár, Zsolt (szerk.) ; Gáti, Balázs (szerk.) ; Projics, Nárcisz (szerk.) ; Ripszám, Dóra (szerk.) ; Tóth, Dávid (szerk.) V. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Doktori Iskola (2023) , 214 p. ISBN: 9789636261405
2. Bendes, Ákos László (szerk.) ; Gáspár, Zsolt (szerk.) ; Gáti, Balázs (szerk.) ; Projics, Nárcisz (szerk.) ; Tóth, Dávid (szerk.) IV. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola (2022) ISBN: 9789634299912
3. Bendes, Ákos László (szerk.) ; Diósi, Szabolcs (szerk.) ; Gáspár, Zsolt (szerk.) ; Gáti, Balázs (szerk.) ; Projics, Nárcisz (szerk.) ; Tóth, Dávid (szerk.) III. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai, Pécs, Magyarország : Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Doktori Iskola (2022) , 188 p. ISBN: 9789634299141
4. Kőhalmi László (Szerkesztő), Kulcsár Gabriella (Szerkesztő), Tóth Dávid (Szerkesztő), Gáti Balázs (Szerkesztő), Sándor Enikő (Szerkesztő) Biztonság és jog: Konferenciakötet, Pécs, Magyarország : PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék (2022)