EÖTVÖS LORÁND TUDOMÁNYEGYETEM ÁLLAM-ÉS JOGTUDOMÁNYI KAR
ÁLLAM-ÉS JOGTUDOMÁNYI DOKTORI ISKOLA

Boros Anita

AZ ADATVÉDELMI COMPLIANCE JOGI ÉS ÜZLETI KIHÍVÁSAI

DOKTORI ÉRTEKEZÉS
TÉZISEK

A kutatási téma vezetője: Balogh Zsolt György

Budapest,
2025

1.1. A kitűzött kutatási feladat és annak előzményei

Az adatvédelmi jog az egyik legdinamikusabban fejlődő jogterület, amely folyamatos kihívások elé állítja a jogalkotó közösséget. A XXI. században már elkerülhetetlenül, az üzleti- és magánélet egyre jelentősebb része helyeződik át a digitális világba. Az induló vállalkozások többségénél nincs fizikai tér, ezen a színtéren pedig az adat tudás, a tudás pedig maga a hatalom. Ahogyan a brit matematikus Clive Humby már 2006-ban kijelentette „az adat az új olaj”[1] az információ számít az egyik legfontosabb erőforrásnak. Sőt mi több, ma már azt sem túlzás kijelenti, hogy a nagy mennyiségű adat birtoklása már az olajnál is értékesebb. Éppen ezért, az adatvédelem megfelelő szintjének biztosítása, kiemelt jelentőséggel bír e modern gazdaságban. [2]

Ennek megfelelően, az adatvagyonnal való gazdálkodás a vállalati stratégiák, innovációk egyik fontos eleme. Azon vállalatok, amelyek célzatosan használják a big data által nyújtott lehetőségeket, és jobban tudják az adatokat hasznosítani, tárolni és kezelni, illetve megosztani az illetékesekkel és megvédeni az illetéktelenektől, komoly versenyelőnyre tehetnek szert.

Ezzel párhuzamosan, a magánélethez kapcsolódó botrányok mennyisége és hatása növekvő. Az Európai Unió jogrendszere, már eddig is szigorú szabályokat írt elő a személyes adatok kezelésére és szankciókat is meghatároz azokkal szemben, akik az adatkezelés során nem járnak el jogszerűen. Az Európai Bíróság elé is egyre több olyan ügy került, amely ütközteti a magánélethez való jogot és az üzleti érdekeket.[3] Ebből is látszik, hogy adataink biztonsága egyre nagyobb jelentőséggel bír. Sok esetben viszont, a technológiai fejlődés egy olyan tempót diktál, amellyel a jogalkotás nem tud lépést tartani,[4] így megtörténhet, hogy míg a vállalati szféra gyorsan kihasználja az általa nyújtott kiváló lehetőségeket, a magánszemélyek, magánéletük megvédése érdekében, eszközök nélkül maradnak. Az adatvédelmi rendelkezések pontos megalkotása, és szankciók meghatározása eleinte a tagállamok kezében volt, figyelembe véve az Európai Unió

---

[1] Nisha Talagala, Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,entity%20that%20drives%20profitable%20activity., letöltve: 12.10.2023.

[2] Jon Suarez -Davis, Data isn’t ‘the new oil’ - it’s way more valuable than that, https://www.thedrum.com/opinion/2022/12/12/data-isn-t-the-new-oil-it-s-way-more-valuable,

[3] T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt, Data Protection: CJEU case law review – 1995-2020, https://www.dpcuria.eu/case-law-review-1995-2020.pdf, letöltve: 12.10.2023.

[4] Polyák Gábor, Szőke Gergely László: Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére, https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2704/1967, 31.o.

adatvédelmi irányelvének rendelkezéseit. Így a digitális piaci helyzet kezdett eltorzulni Európában, hiszen a közösség szintjén nem volt teljesen egységes a szabályozás.

2016. április 27-én az Európai Parlament és a Tanács elfogadta a 2016/679 rendeletet (a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendeletet), amely felváltotta a 95/46/EK adatvédelmi irányelvet, illetve minden olyan nemzeti jogszabályt, ami erre épült.

Kutatási témám aktualitását tehát, az általános adatvédelmi rendelet (GDPR – General Data Protection Regulation) indokolja, amely célja, az egységes digitális piac megteremtése és a személyes adatok kezelésével kapcsolatos biztonsági, állampolgári önrendelkezési kérdések szabályozásának korszerűsítése.

Kutatásom, a növekvő adatvédelmi compliance kötelezettségekből eredő kihívásokra reagál: bemutatja, a hazai és nemzetközi szakirodalom kritikus értékeléseit az adatvédelmi kötelezettségek betartásával kapcsolatban, és annak az üzleti szférára gyakorolt hatásait.

Míg a GDPR alapelvei minden szervezetre egyformán vonatkoznak, a megfelelés gyakorlati megvalósítása jelentősen eltérhet a kis- és középvállalkozások (KKV-k) és a nagyvállalatok között. Ugyanakkor, figyelembe véve, hogy a kis- és középvállalkozások az Európai Unió vállalkozásainak 99 %-át teszik ki[5], az adatvédelmi szabályozás sikeressége nagyban megmutatkozik a KKV-k megfelelési szintjének mértékében.

Az új adatvédelmi Rendelet bevezetésével, az adatvédelmi szabályok körüli bizonytalanságok nem szűnnek meg létezni, sőt az egységesített szabályozás betartásának kikényszerítése a rendelet számtalan általános megfogalmazása miatt bonyolult feladat.

Különböző földrajzi régiók vagy akár iparágak specifikus helyzetéből adódóan, a rendelet szabályainak történő megfelelés szintje, vagy a szabályoknak való megfelelés mértéke eltérhet.

Jelen tanulmány, nem kevesebb célt tűz ki maga elé, mint annak bizonyítása, hogy a korlátozott erőforrásokkal és információkezelési rendszerrel rendelkező cégek számára, az adatvédelmi megfelelés rengeteg munkát és komoly anyagi terhet jelent, hiszen a már meglévő adatkezelési szabályoknak való megfelelés mellett, olyan új kötelezettségeket vezet be az adatkezelők és adatfeldolgozók számára, amelyek idő és pénzigényes folyamatok kialakítását követelik. Ilyen például, az elszámoltathatóság alapelve, amely a nemzeti hatóságoktól a szervezetekre ruházza a

[5] European Commision, Annual Report on European SMEs 2023/2024, Luxembourg: Publications Office of the European Union, 2024, 6.o.

felelősséget és arra kötelezi őket, hogy bizonyítani tudják a jogszabályoknak való teljes körű megfelelést. Különösen, a nagy mennyiségű személyes adatot kezelő vállalatoknak jelent ez komoly felelősséget, hiszen a megfelelés nem csak jogi kérdés, átfogóan érinti a folyamatmenedzsmentet, kontrollkörnyezet és az üzleti folyamatokat is, emellett nagyon sok területet kihívás elé állít, ilyen például a munkavállalókkal kapcsolatos adatkezelések, amely már figyelemmel van az otthoni munkavégzésre, a saját eszköz használatára, online marketingre, nem is beszélve a nemzetközi kereskedelem és együttműködésről, amelyhez szükség van személyes adatok Európai Unión kívülre történő továbbítására.

A hatályos adatvédelmi szabályozást tekintve, jelen kutatás hipotézise a következőképpen fogalmazható meg: egy kis- vagy közepes méretű vállalat számára, nem lehetséges megfelelő időt és erőforrást fordítani az adatvédelmi megfelelés magas szintjének elérése.

1.2. A kutatás során alkalmazott tudományos módszerek és elemzések

Ezen hipotézis alátámasztása érdekében, jelen tanulmányban bemutatom a mértékadó hazai és nemzetközi szakirodalom kritikus értékeléseit az adatvédelmi kötelezettségek betartásával kapcsolatban, és annak az üzleti szférára gyakorolt hatásait. Az általános adatvédelmi rendelet irányadó rendelkezéseinek boncolgatása mellett, megvitatásra kerülnek a 29. cikk szerinti adatvédelmi munkacsoport (WP29), az Európai Adatvédelmi Testület (EDPB) valamint különböző nemzeti adatvédelmi hatóságok állásfoglalásai, iránymutatásai, ajánlásai és az általuk meghatározott különböző megfelelési módszerek is. Elemzésre kerül továbbá, több nemzeti hatóság által kiszabott bírság, amely segít megismerni az adatvédelmi hatóságok álláspontjait, illetve feltárni azokat a területeket, ahol legkevésbé sikeres az adatvédelmi megfelelés.

További célom, az új adatvédelmi rendelet értelmezési kérdéseinek, illetve jogi szabályozásának hiányosságának feltárása. A felmerülő jogkérdéseket összevetve, egy átfogó képet alkotok az európai egységes szabályozás következményeiről, majd arra is kitérnék milyen jövőbeli problémákkal ütközhetünk az adatvédelem terén és erre milyen esetleges megoldások létezhetnek.

A fent említett kérdéskörök elemzése, meghatározza a dolgozat szerkezetét és a kutatás módszertanát, amely egyrészt történeti-leíró, illetve leíró-kritikai elemzést foglal magába.

Ugyanakkor, a tanulmány nagyban kívánok támaszkodni forráselemzésre, és szekunder adatok elemzésére egyaránt, elsősorban jogforrásokra, nemzetközi szerződésekre, törvényekre, rendeletekre, bírói és más jogalkalmazó szervek joggyakorlatára és a vonatkozó jogtudományi irodalomra támaszkodva. A kutatás célja, az adatvédelmi szabályok mozgatórugóink feltárása, a

szabályszerűségek megértése. Nem az általánosságra, hanem a specifikumokra helyezem a hangsúlyt, így a deduktív módszert alkalmazva, az általános megállapítások felől határozok majd meg egyre egyedibb megállapításokat. Ezt követi majd, a szakirodalomból merített esetek jellemzőinek összegzése, az elméleti következtetések megfogalmazása.

A dolgozat első fejezete, feltárja a magánélethez való jog és az adatvédelem közötti kapcsolatot, majd átfogó képet kíván adni az adatvédelmi szabályozás hatásairól, felsorolva annak pozitív és negatív következményeit. Ezt követően a dolgozat két nagy részre tagolódik. Az első felében, az adatvédelmi rendeletben meghatározott kötelezettségeket boncolgatjuk, amely során minden kötelezettség kapcsán kitérünk az esetleges megfelelési nehézségekre és értelmezési kérdésekre. A dolgozat második felében, a megfelelés során leggyakrabban előforduló gyakorlati kihívásokra fektetjük a hangsúlyt.

Figyelembe véve, a mesterséges intelligencia rohamos elterjedését és fejlődését, elengedhetetlennek tartottam, hogy a dolgozatban a mesterséges intelligenciára vonatkozó adatvédelmi kérdések boncolgatásával is foglalkozzunk.

1.3. A kutatás főbb eredményei és azok hasznosítási lehetőségei

A kutatás elvégzése, olyan tanulságok levonására ad lehetőséget, amely az adatvédelmi megfelelésben, valós segítséget nyújthat a vállalatok számára. A dolgozat egészében törekszünk feltárni, nem csak a rendelet értelmezési kérdéseit, de igyekszünk azokra választ is találni.

Másodsorban a jogszabályi követelmények tárgyalása mellett, hasznos gyakorlati tanácsokat is megfogalmazok, amely támaszpont lehet a vállalatoknak a megfelelő folyamataik és információs rendszereik kialakításában. A gyakorlati kihívások fejezetben, olyan területek kerülnek elemzésre, amelyek a legtöbb vállaltot érintenek, hiszen az online jelenét és ezzel járó adatkezelések adatvédelmi kihívásainak leküzdése, valamint a munkahelyi adatkezelések megfeleltetése az első lépést jelenti az adatvédelmi compliance útján.

Dolgozatom rámutat arra, hogy egy sikeres adatvédelmi megfelelés lebonyolítása összetett feladat. Az adatkezelőnek folyamatosan lépést kell tartania az értelmezési és törvényi változásokkal, figyelnie kell vennie mind a külső, mind a belső tényezők lehetséges veszélyeit, biztosítania kell a meglévő vagy a megfelelés során kialakult szervezeti gyakorlatok betartását, reagálnia kell az érdekelt felek kérdéseire, és mindezek felett, olyan vezetői készséggel kell rendelkeznie, amely biztosítja a szervezeten belüli megfelelő hozzáállást.

A KKV-k szempontjából, az adatvédelmi szabályok bevezetése, sok esetben csak egy újabb feladat, kötelezettség, amelyet a vállalkozásokra rónak, valamint egy olyan költség és kiadás, amely számukra akár versenyhátránnyal is járhat.[6]

Az elszámoltathatóságról szóló fejezetből kiderül, hogy a jelenlegi szabályozás alapján az elszámoltathatóság magában foglalja az adatkezelő legfontosabb feladatát, akinek ezentúl nem csak felelősséget kell vállalnia a rendeletben megfogalmazott alapelvek és kötelezettségek betartásáért, de képesnek kell lennie bizonyítani is a megfelelését. Az elszámoltathatóság elvének megértése, a hatékony adatvédelem sarokkövévé és az EU adatvédelmi törvény, politika és szervezeti gyakorlat domináns trendjévé vált. Ezen alapelv betartása nélkül nem beszélhetünk adatvédelmi megfelelésről, amelyről a vállalatok többsége megfeledkezik. A GDPR hatálybalépését követően, a KKV-nak jelentős problémát okoz beazonosítani, hogy rájuk milyen mértékben vonatkozik a rendelet, melyek azok adatkezelési tevékenységek, amelyek különös figyelmet igényelnek, valamint milyen dokumentumokat kell előállítaniuk, és folyamatokat átalakítaniuk a megfelelés bizonyítása érdekében. [7]

A hatásvizsgálatra és az alapértelmezett és beépített adatvédelemre vonatkozó fejezetekből kiderül továbbá, hogy az adatvédelmi compliance részeként az adatvédelmi szabályozás elveit be kell építeni az adatkezelési technológiákba, mind a tervezés, mind a működtetés során. A technológiát úgy kell megtervezni és megvalósítani, hogy egész életciklusát a demokratikus társadalmainkat meghatározó alapvető jogokkal és értékekkel kompatibilis módon lehessen megvalósítani. Ugyanakkor, a hatásvizsgálat elvégzése, mint ahogy a beépített adatvédelem vállalati kultúrába való bevezetése nem tekinthető standard, minden vállalat szempontjából ugyanolyan formában teljesíthető kötelezettségnek. Az adatkezelőknek, esetről estre dönteniük kell a megfelelő szervezeti és technikai intézkedések alkalmazásáról, amely függhet a szervezet méretétől, célcsoportjától vagy akár főtevékenységétől. A beépített adatvédelem egy stratégia, egy hosszú távú tervezés alapköve, amely megköveteli az adatvédelmi alapelvek és az érintettek jogainak és szabadságainak tiszteletben tartását már az első lépéstől kezdve, bármilyen üzleti folyamatról legyen szó. Mindez, lehetetlen az adatvédelmi tudatosság fejlesztése nélkül, amelyet úgy a

---

[6] Egy 2019-es felmérés szerint, a megkérdezett európai vállalatok 27 százaléka számolt be arról, hogy 1.000 és 10 ezer euró közötti összeget költött az adatvédelmi megfelelésre, forrás: https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/

[7] Dr. Zemplenyi Adrienne: A KKV-k tapasztalatai a GDPR alkalmazásával kapcsolatban, STARII záró konferencia, https://naih.hu/files/dr-Zemplenyi-Adrienne_A-KKV-k-tapasztalatai-a-GDPR-alkalmazasaval-kapcsolatban_STARII-zarokonferencia.pdf, 1.o. letöltve: 12.12.2024., 2.o.

munkavállalóknak, mint a vezetőknek szükséges elsajátítani. Figyelemmel tehát, a beépített adatvédelem elveire, egy megfelelő adatvédelmi irányítási keretrendszer bevezetése, az adatvédelmi elszámoltathatóság követelményét operacionalizálja. Egy keretrendszer ugyanis, igazolhatóvá teszi az adatvédelmi kontrollok bevezetését és azok alkalmazását, a kockázatcsökkentő intézkedések dokumentáltságát és ezek belső vagy külső fél általi ellenőrzését.
Az adatvédelmi tisztviselőre vonatkozó fejezet egyértelművé teszi, hogy a legtöbb adatkezelést végző vállalatnak szüksége van adatvédelmi tisztviselőre vagy legalább egy adatvédelmi kérdésekben jártas, a törvényt és az adatvédelmi gyakorlatot jól ismerő szakemberre. Az átláthatóság elvének történő megfelelés érdekében, nagyon sok esetben szakmai nézőpontra, tudásra, véleményre lehet szükség. A rendelt, de még a munkacsoport iránymutatásai is többnyire általános jellegűek, emiatt nagyon sok helyen értelmezési kérdések adódhatnak.
Mindezek ellenére, egy adatvédelmi szakember behívása a vállalati, főként KKV-s, struktúrába komoly anyagi vonzatot jelent, amit egyértelműen nem minden szervezet képes megengedni magának.
Az adat- és kiberbiztonságot valamint az incidenskezelést tárgyaló fejezet egyértelmű konklúziója, hogy a mai, rendkívül összekapcsolt digitális környezetben a személyes adatok védelme még soha nem volt ennyire kritikus. A növekvő kiberfenyegetések, az adathalászat és a magánélet védelmével kapcsolatos növekvő aggodalmak miatt, a szervezetekre óriási nyomás nehezedik az érzékeny információk, különösen a személyes adatok védelme terén. A GDPR által meghatározott incidens reakció megtervezése, kulcsfontosságú elem a vállalat megfelelőségi stratégiájában, amely döntő szerepet játszik az adatbiztonság megsértéséből eredő károk minimalizálásában és a gyors helyreállítás biztosításában. Szintén kritikus fontossággal bír az incidenskezelési szabályzat elkészítése, amely részletesen meghatározza hogyan kell az incidenseket észlelni, jelenteni, eszkalálni és megoldani. Az incidenskezeléssel kapcsolatban, a KKV szektorban, elsődleges probléma az incidens beazonosítása, amely többnyire az adatvédelmi tudatosság hiányának tudható be. A már sokat említett munkavállalói tudatosítás, itt kulcsfontosságú szerepet játszik, hiszen gyakran az alkalmazottak az első védelmi vonalat jelentik az esetleges incidensek megelőzésében vagy beazonosításában. A második leggyakoribb probléma, az incidens bejelentésének és nyilvántartásának elmaradása, hiszen figyelembe véve a gazdasági érdekeket, a szervezetek félnek az esetleges bírságtól vagy reputációs veszteségtől, amely akár egy incidens

bejelentés következménye is lehet. Megfelelő incidenskezelési eljárások kialakítása és betartása nélkül viszont, nem beszélhetünk teljeskörű adatvédelmi megfelelésről.

Meghatározó probléma továbbá, hogy a döntéshozók legtöbbször nem ismerik fel az informatikai adatbiztonság fontosságát, valamint az ilyen biztonsági rendszerek kialakítására irányuló forrás is legtöbb esetben hiányzik.[8]

Az érintettek jogaival foglalkozó fejezetből kitűnik, hogy a magánszemélyek nagyobb betekintést és jogokat kapnak az adataik kezelésével kapcsolatban, ezzel párhuzamosan a vállalatok ez irányú kötelezettségei növekednek. Az érintettek jogainak tiszteletben tartása, és kérelmeikre történő megfelelő és a GDPR-ban meghatározott határidőn belüli válaszolása, szintén láthatóan megnöveli a megfelelés költségeinek mértékét.

Ugyanakkor, jogellenes adatkezelés esetén az érintettek kártérítési igényeket, polgári jogi perben, a Ptk. rendelkezéseire hivatkozva érvényesíthetik. Mindemellett a Ptk. alapján nevesített személyiségi jogok körében rögzített, a személyes adatok védelméhez való jog esetében, az érintettek sérelemdíj iránti igényt is támaszthatnak. Az adatvédelmi jogsértéssel összefüggő polgári jogi felelősség tehát, a KKV-et is terheli.

A *szerződéses felelősséggel* kapcsolatban, megfigyelhetjük, hogy a szervezetek nemcsak az általuk kezelt személyes adatok biztonságáért felelnek, hanem azt is biztosítaniuk kell, hogy minden olyan külső szervezet, amellyel személyes adatokat osztanak meg, szigorú biztonsági intézkedéseket hajt végre a személyes adatok megfelelő szintű védelme érdekében. Ez alapján tehát, az adatkezelő egyik fontos kötelezettsége, nem csak szakmai szempontból kiemelkedő, de az adatvédelmet tekintve is megfelelő garanciákat nyújtó szerződéses partnerek (adatfeldolgozók vagy közös adatkezelők) kiválasztása, illetve az adatkezeléssel kapcsolatos felelősségek pontos meghatározása. A jól megfogalmazott, adatkezelési megállapodások nem csak a megfelelőség biztosításában segíthetnek, hanem az elszámoltathatóság egyik lényeges dokumentuma, valamint az üzleti partnerek közötti bizalmi kultúra kialakításában is segítséget nyújthat.

Továbbá, az *adatkezelések jogszerűségének* biztosítása érdekében, minden adatkezelési művelet a jogszabálynak megfelelő jogalappal kell rendelkeznie, amely főként a kis- és középvállalkozások számára, számos kihívást jelent. Mint azt az erről szóló fejezetben hangsúlyozom, ezek a kihívások főként a korlátozott erőforrások, a szakértelem hiánya és a megfelelési követelmények összetettségéből adódnak.

[8] Dr. Zemplenyi Adrienne, *op. cit.,* 5.o.

Bár a GDPR hat jogalapot biztosít az adatkezelésre, a KKV-k gyakran küzdenek a megfelelő jogalap felismerésével és helyes használatával, mivel gyakran nem rendelkeznek külön jogi vagy adatvédelmi szakemberekkel, ami hibákhoz vagy mulasztásokhoz vezet a jogalap kiválasztása és igazolása során. Ennek következtében, gyakran megfigyelhető, hogy túlzott mértékben támaszkodnak a hozzájárulásra, mint a látszólag legegyszerűbb megoldásra.

Mindemellett, a szerződéses akarat és a GDPR szerinti hozzájárulás mint a személyes adatok kezelésének jogalapja közötti különbségtétel, kritikus fontosságú az adatvédelem és a szerződéses kötelezettségek bonyolultságának megértéséhez a mai digitális gazdaságban.

A Ptk. 6:58. §-a alapján a szerződés a felek kölcsönös és egybehangzó jognyilatkozata, amelyből kötelezettség keletkezik a szolgáltatás teljesítésére és jogosultság a szolgáltatás követelésére.

Ez esetben, a joghatás kiváltását szolgáló akaratnyilatkozat (szerződéses hozzájárulás), magában foglalja egyfelől a polgári jogi jogalany szándékát, valamint annak kifejezésére szolgáló eszközt a szóban, írásban vagy ráutaló magatartás formájában tett nyilatkozatot.[9]

Ez alapján, a szerződéses hozzájárulás a felek közötti megállapodásra utal, amely alapján a felek vállalják hogy a szerződésbe foglalt rendelkezéseket elfogadják.

Ezzel szemben, a GDPR szerinti hozzájárulás, amelynek *„szabadon megadottnak, konkrétnak, tájékozottnak és egyértelműnek”* kell lennie, amely elsősorban, az érintettek jogainak védelmét és autonómiájuk biztosítását szolgálja, a személyes adataik kezeléséről való döntésben.

A szerződés tartalmába foglalt adatkezelési feltételek, azt a benyomást kelthetik, hogy az érintett a szerződés aláírásával az adatkezeléshez a 6. cikk (1) bekezdés a) pontja szerinti hozzájárulását adja meg. Egyidejűleg az adatkezelő tévesen feltételezheti, hogy a szerződés aláírása a 6. cikk (1) bekezdésének a) pontja értelmében vett hozzájárulásnak felel meg. Fontos megjegyezni viszont, hogy e kettő két teljesen eltérő fogalom. Különbséget kell tenni a szolgáltatási feltételek szerződés megkötése érdekében történő elfogadása, valamint a 6. cikk (1) bekezdésének a) pontja szerinti, a konkrét adatkezeléshez adott hozzájárulás között, mivel ezek a fogalmak eltérő követelményekkel és jogi következményekkel járnak.

Szintén kihívást jelenthet, hogy a megváltozott adatkezelési célok a jogalap megváltozásával is járnak, amit a vállaltok nehezen vagy egyáltalán nem ismernek fel.

---

[9] Juhász Ágnes: A szerződéses akarat és annak egyes értelmezési kérdései, különös tekintettel a szerződés részleges érvénytelenségére, Miskolci Jogi Szemle, 17. évfolyam (2022) 2. szám (1. különszám), https://doi.org/10.32980/MJSz.2022.2.2008, 190.o.

Mint az a joggyakorlatból kiderül [10], a legtöbbet megsértett cikkek az 5., a 6. és a 32. cikk, amely azt jelzi, hogy a cégek leginkább az általános adatkezelési elvek betartásával, az érvényes hozzájárulás megszerzésével, valamint a megfelelő jogalap kiválasztásával és a biztonsági intézkedések végrehajtásával küszködnek. Ezek a kihívások, a GDPR követelményeinek összetettségéből adódik, ami nem kevés adminisztratív teherhez vezet.

Végül de nem utolsó sorban, azt is megfigyelhetjük, hogy a mesterséges intelligencia minden méretű vállalkozás számára változást hozott, forradalmasítja a vállalatok működését és az ügyfelekkel való kapcsolattartást. Míg a nagyvállalatok gyorsan képesek implementálni az AI-technológiákat, a kis- és középvállalkozás számára túlzott költségekkel járhat az ezzel kapcsolatos kiberbiztonsági intézkedések, titkosítási technológiák való befektetést, valamint az adatvédelmi szabályoknak való megfelelés biztosítása.

A kutatás során, négy fő kihívást azonosítottunk a KKV-k megfelelési folyamatait tekintve: technikai, jogi, szervezeti és jogszabály értelmezési kihívásokat. Mindegyik kategórián belül különböző problémákat figyelhetünk meg, mint például az erőforrások korlátozottságát, a vállalati kultúra változtatásának nehézségét, a partnerekkel való együttműködésre irányuló nehézségeket és a szabályozás értelmezésének és megértésének összetettségét. A tanulmány során azonosított kihívások, jól mutatják a GDPR-nak való megfelelés sokrétűségét, figyelembe véve a mai technológiailag fejlett és összekapcsolt világban gyűjtött, feldolgozott és tárolt személyes adatok hatalmas mennyiségét. Mindezeket figyelembe véve, egyértelművé válik, hogy egy átlagos KKV nem rendelkezik megfelelő emberi és anyagi erőforrásokkal, amit az adatvédelmi megfelelésre tudna fordítani, ezáltal, általában nem is törekszik az adatvédelmi megfelelés magas szintjének elérésére.

[10] Statista, Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range, https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/, letöltve: 12.01.2025.

1.4. A doktori értekezés témakörében készült publikációk jegyzéke

Boros Anita: Obținerea consimțământului persoanei vizate în teorie și în practică, Jurnalul Baroului Cluj, 01/2022 44-60. o., https://www.baroul-cluj.ro/wp-content/uploads/2022/07/boros.pdf.

Boros Anita: Adatvédelmi megfelelés: privacy by design és a hatásvizsgálat mint az elszámoltathatóság eszközei, Themis: Az Elte Állam- és Jogtudományi Doktori Iskola elektronikus folyóirata, 2020. 7-28. o.

Boros Anita: Az adatvédelmi tisztviselő mint az elszámoltathatóság sarokköve, Themis: Az Elte Állam- és Jogtudományi Doktori Iskola elektronikus folyóirata, 2022, DOI: 10.55052/themis.2022.2.6.32.

Boros Anita: Principiul responsabilității în prelucrarea datelor cu caracter personal, Jurnalul Baroului Cluj, 02/2021, https://www.baroul-cluj.ro/wp-content/uploads/2021/12/boros.pdf.

Boros Anita: Jogos érdek mint az adatkezelés jogalapja az elméletben és a gyakorlatban Themis: Az Elte Állam- és Jogtudományi Doktori Iskola elektronikus folyóirata, 2021, 7-33. o.

Boros Anita: Issue of cookie consent in the light of applicable eu laws, RODOSZ konferenciakötet, Kárpát-medencei Magyar Doktoranduszok Interdiszciplináris konferenciája, Társadalom és Innováció, 2020.

Boros Anita: A web-sütik használatának adatvédelmi kérdései, Pro Futuro - A jövő nemzedékek joga, Évf. 10 szám 3 (2020), https://doi.org/10.26521/PROFUTURO/2020/3/8746.

E tézis alapjául szolgáló irodalom:

Dr. Zemplenyi Adrienne, A KKV-k tapasztalatai a GDPR alkalmazásával kapcsolatban, STARII záró konferencia, https://naih.hu/files/dr-Zemplenyi-Adrienne_A-KKV-k-tapasztalatai-a-GDPR-alkalmazasaval-kapcsolatban_STARII-zarokonferencia.pdf

European Commision, Annual Report on European SMEs 2023/2024, Luxembourg: Publications Office of the European Union, 2024.

Jon Suarez -Davis, Data isn't 'the new oil' - it's way more valuable than that, https://www.thedrum.com/opinion/2022/12/12/data-isn-t-the-new-oil-it-s-way-more-valuable

Juhász Ágnes: A szerződéses akarat és annak egyes értelmezési kérdései, különös tekintettel a szerződés részleges érvénytelenségére, Miskolci Jogi Szemle, 17. évfolyam (2022) 2. szám (1. különszám), https://doi.org/10.32980/MJSz.2022.2.2008

Nisha Talagala, Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,entity%20that%20drives%20profitable%20activity.

Polyák Gábor, Szőke Gergely László: Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére, https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2704/1967.

Statista, Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range, https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/

T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt, Data Protection: CJEU case law review – 1995-2020, https://www.dpcuria.eu/case-law-review-1995-2020.pdf.