AZ EURÓPAI BEÉPÍTETT ADATVÉDELEM

-tézisfüzet-

1. BEVEZETÉS

A történelem során a magánélet védelme megérdemelt és kitüntetett figyelmet kapott. Mégis, a magánélet fogalmának konceptualizálására tett kísérletek egyike sem tudta leírni annak minden összetevőjét[1]. A magánélet védelmét szolgáló jogi keretrendszer megújjítása nem forradalmi, inkább evolúciós jelenség. Ezt bizonyítja az alkalmazandó jogszabályokban rögzített adatvédelmi elvek viszonylagos statikussága[2] is. Míg a jogi háttér alapjai nem változtak, addig a technológiák megvalósításának módja igen, méghozzá gyakran olyan átláthatatlan szinten, amely az adatvédelmi jogászok számára örökös pereskedésekhez és vitákhoz szolgált alapul.

Fontos kiemelni, hogy a magánélet védelme és *per a contrario*[3] annak megsértése nem egzakt tudomány. Nem meghatározott paramétereken alapul, és nem teszi lehetővé pontos „eredmények" leközlését sem. Ez nem egy lejárt parkolójegy esete, ahol a késéssel töltött percek, tehát az állampolgár jogellenes magatartása, könnyen átfordíthatóak egy közigazgatási bírságra. A közigazgatás szempontjából az említett jogellenes magatartásra kiszabott büntetés gazdasági értéke eléggé visszatartó erejű kell legyen ahhoz, hogy megakadályozza a jövőbeni kísérleteket. Az állampolgár szemszögéből nézve azonban ez a játékelméleten alapuló kockázat *vs.* jutalom kérdése. Amennyiben a bírság csak egy bizonyos szintet érhet el, és korlátozott gazdasági értéket képvisel az állampolgár pénzügyi helyzetére nézve, talán a jogellenes parkolás értékes perceiből származó előnyök meghaladják a bírság kifizetése miatt elszenvedett pénzügyi veszteséget.

Mégis miben más az, ha egy állampolgár magánéletének szentségét sértik meg? Ilyenkor az állampolgár egy olyan kombinált eseménysorozatnak van kitéve, amely a magánélethez való jog súlyos megsértését válthatja ki, és kárt okozhat. Így a magánélet védelmének megsértése esetén az állampolgárok által elszenvedett kár legtöbbször nem közvetlen, és nem is azonnal kimutatható. Snipe ékesszólóan érvel amellett, hogy az állampolgárok különbözőképpen értékelik a magánélet védelmét, és hogy ugyanazon hálózat különböző tagjai valójában nem tarthatnak fenn különböző

[1] Részletesen lásd Acquisti et al. 2016, pp. 2-48.
[2] Értsd, hogy hosszú ideig nem változik.
[3] Az ellenkezőjére való hivatkozásként ismert, olyan állítást jelöl, amelyet azért tartanak helyesnek, mert egy adott eset nem cáfolja meg. A *per a contrario* érveket gyakran használják a jogban, hogy olyan problémákat oldjanak meg, amelyekre egy adott jogrendszer jelenleg nem terjed ki.

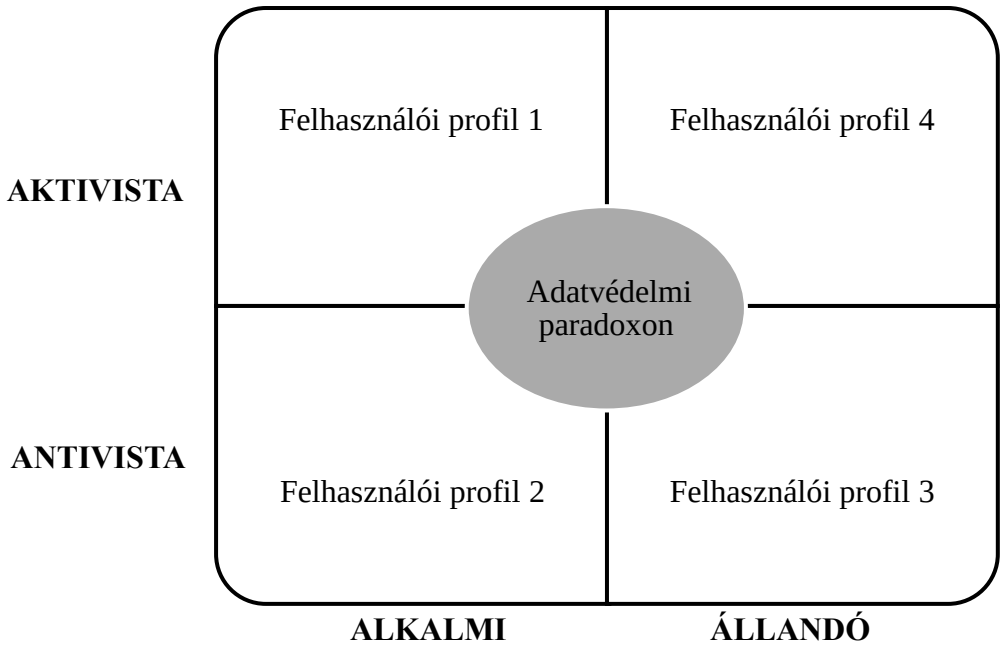
szintű magánélet védelmére irányuló gyakorlatokat[4]. A hálózat az internetszolgáltatókra és más, hálózati hatással bíró informatikai szolgáltatásokra (*pl.* e-mail) utal[5]. A hálózatokban a magánélet védelmének e piacai minden felhasználó digitális lábnyomát magukba szívják[6]. És tudjuk, hogy a társadalom digitalizációjának előrehaladtával az aktív felhasználók számának növekedése miatt a magánélet védelmének piacai egyre nagyobbak lesznek. Jonson szerint 2021 januárjában világszerte 4,66 milliárd aktív internetfelhasználó volt, ami a világ népességének 59,5 százalékát tette ki[7].

Az egyre növekvő magánélet védelmének piacai magukban hordoznak egy újabb fontos kérdést: létezik-e infrastruktúra inverzió az adatvédelmi piacokon? Az infrastruktúra-inverzió fogalmát Andreas M. Antonopoulos használta, aki úgy határozta meg, hogy egy olyan jelenség, amikor egy új technológiának először a régi infrastruktúrát kell használnia, és ez konfliktust és nyomást hoz létre, amely később infrastruktúra-inverzióhoz vezet[8]. Érvelése szerint ezt az okozza, hogy az új technológia adoptálásának első néhány évében az általa megzavart meglévő technológiának kell az újat magán hordoznia[9]. A magánélet védelmének piacain is láthatóak az infrastruktúra inverziójának jelei. Még ha az aktív internethasználók világszerte adatvédelmi paradoxonban szenvednek is, a technológiai fejlődés jelen van. Egy egyszerű példával élve, az AdBlock Plus[10] az internetes böngészőkben való széles elterjedése is alátámasztja ezt a feltételezést. A *Statista* kutatási részlege a legutóbbi negyedéves eredmények szerint a mobil reklámblokkoló böngészők havi aktív felhasználóinak száma elérte az 586 millió főt[11]. Továbbá a felhasználók egyre gyakrabban alkalmaznak magánéletet védő eszközöket a webhasználat közben. E tekintetben a Brave böngésző 2021 szeptemberében elérte a 36 millió havi aktív felhasználót[12].

Mit értünk adatvédelmi paradoxon alatt? Az adatvédelmi paradoxon azt az ellentmondást mutatja be, amely a felhasználók magánéletük védelmére irányuló szándéka és a felhasználók tényleges

[4] Snipe 2021.
[5] *Ibid.*
[6] A felhasználó az állampolgárokat jelenti.
[7] Jonshon, 2021.
[8] Antonopoulos, 2017.
[9] *Ibid.*
[10] Az AdBlock Plus egy ingyenes bővítmény, amely lehetővé teszi a felhasználó számára, hogy testre szabja webes élményét. A felhasználó blokkolhatja a hirdetéseket vagy letilthatja a nyomon követést.
[11] Statista 2021, https://www.statista.com/statistics/606357/mobile-adblocking-browser-users-worldwide/ [2021.09.23.].
[12] Brave Announcements, 2021, https://brave.com/36m-mau/ [09.24.2021].

viselkedése között a magánélet védelmének piacain mutatkozik. A fogalomról Susanne Barth és Menno D.T. de Jong[13] készítettek szisztematikus szakirodalmi áttekintést. Arra a következtetésre jutottak, hogy a felhasználó döntéshozatali folyamatát, ami a magánéletre vonatkozó információk felfedésére való hajlandóságot illeti, általában két szempont vezérli: (1) egy kockázat-haszon értékelés és (2) a nem vagy elhanyagolhatónak ítélt kockázat értékelése[14] . E kutatásra reflektálva, úgy gondoljuk, hogy az adatvédelmi és magánéleti kockázatokkal szembeni felhasználói felfogás egy két-két dimenziós mátrixban ábrázolható, ahol az adatvédelmi paradoxon a mátrixból felépíthető négy különböző felhasználói profil metszéspontjában helyezkedik el. Az *1. ábra* az adatvédelmi paradoxon áttekintését mutatja be. Ezt a mátrixot értelmezve négy különböző felhasználói profilt tudunk létrehozni:



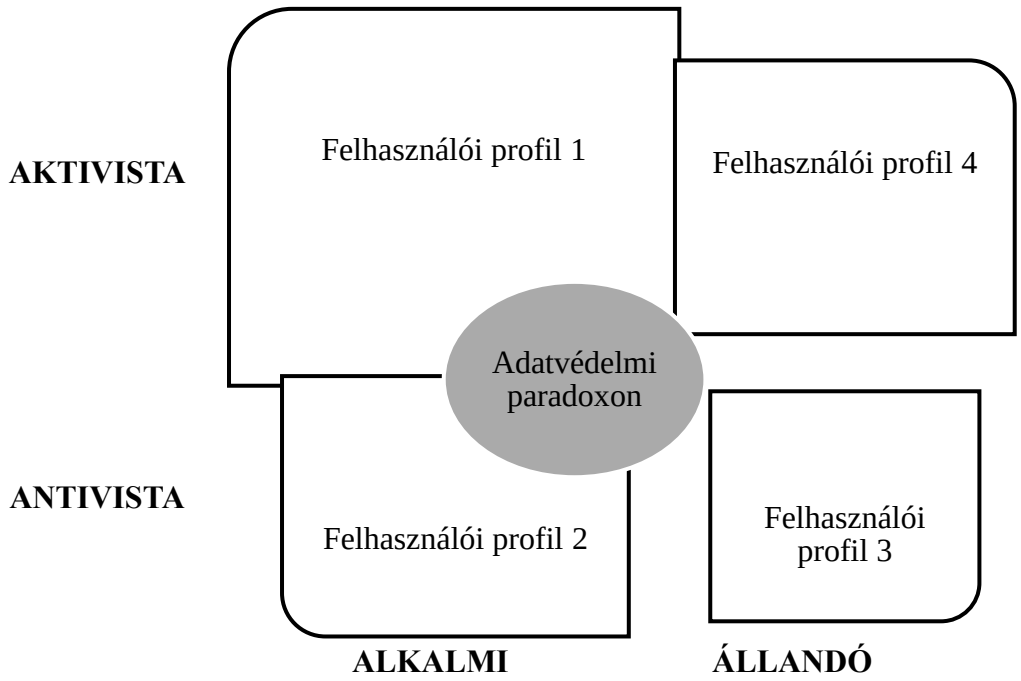
Ábra 1. Az adatvédelmi paradoxon áttekintése.

a. **Felhasználói profil 1 – az alkalmi aktivisták:** Olyan felhasználók, akik botrányos események bekövetkeztével hangoztatják a nyilvánosság felé a magánélet megsértésével kapcsolatos aggályaikat.
b. **Felhasználói profil 2 - alkalmi antivisták:** Olyan felhasználók, akik kockázat-haszon értékelés alapján hajlandóak elfogadni az adatvédelem és a magánélet megsértését.

[13] Barth - de Jong 2017, pp. 1038-1058.
[14] Ibid.

c. **Felhasználói profil 3 - állandó antivisták:** Olyan felhasználók, akiknek a kockázatértékelései elhanyagolhatónak vagy egyáltalán nem létezőnek minősülnek, és így egyszerűen figyelmen kívül hagyják a magánélet megsértésére vonatkozó kockázatokat.
d. **Felhasználói profil 4 - állandó aktivisták**: Olyan felhasználók, akik soha nem hajlandóak elfogadni az adatvédelem és a magánélet megsértését, mivel kockázat-haszon értékelésük mindig az utóbbi felé hajlik.

Kutatásunkban azzal érvelünk, hogy a digitalizáció és a magánélet védelmének piacait érintő infrastruktúra inverziója át fogja alakítani az előbb bemutatott felhasználói csoportok méretét, ezzel együtt megváltoztatva az adatvédelmi paradoxon elhelyezkedését is. Megítélésünk szerint az Európai Unió (EU) adatvédelmi szabályozása és a hozzá kapcsolódó stratégia végül az állandó antivisták teljes eróziójához fog vezetni. Mivel az EU adatszuverenitása[15] egyre hangsúlyosabbá válik, a tagállamokban működő szervezeteknek jobban kell összpontosítaniuk a szabályozási környezettel való megfelelésre. A *2. ábra* ezt a tendenciát szemlélteti az adatvédelmi paradoxon aktualizált áttekintésében.



Ábra 2. Az adatvédelmi paradoxon aktualizált áttekintése.

[15] Az adatszuverenitás azt az elképzelést képviseli, hogy az összegyűjtött adatokra az adott nemzet törvényei és irányítási struktúrái vonatkoznak. Az uniós adatszuverenitás az Európai Unión belül gyűjtött adatokra vonatkozik.

Ennek fényében hasznosnak tartjuk, ha a beépített adatvédelem (Privacy by Design, PbD) fogalmát európai szemszögből értelmezzük. Célunk, hogy ezt úgy tegyük meg, hogy elemezzük annak természetét, alkalmazását és érvényesítését. Kutatásunkban új a PbD elvekre alkalmazható megállapításokat fedezünk fel. Mindezzel szándékunk az európai beépített adatvédelem végső megértése, amely segít majd eligazodni az európai adatvédelmi piacokon zajló infrastrukturális inverzióban.

2. KUTATÁSI KONTEXTUS

Peffers és tsai. szerint az információs rendszerek kutatása egy alkalmazott kutatási tudományág abban az értelemben, hogy gyakran alkalmazza más tudományágak, például a közgazdaságtan, az informatika és a társadalomtudományok elméleteit az információs technológia (Information Technology, IT) és a különböző tudományok metszéspontjában felmerülő problémák megoldására[16]. Az informatika napjaink gazdaságának folyamatosan fejlődő ágazata. A szervezetek által kifejlesztett informatikai rendszerek gyorsan és széles körben terjednek, miközben az ilyen rendszereken keresztül keletkező adatmennyiség minden várakozást felülmúl. Mind a személyes, mind a nem személyes adatok kulcsfontosságú tényezői az egységes digitális piacnak, amely koncepció célja, hogy üzleti lehetőségeket és új üzleti modelleket kínáljon az EU egész területén.

A közelmúltban történt nagy visszhangot kiváltó adatvédelmi incidensek ugyanis arra késztették a fogyasztókat, hogy elmeneküljenek az olyan szolgáltatóktól, amelyek nem védték megfelelően az adatokat. Vannak azonban olyan esetek, amelyeknél nincs menekülési útvonal. Ilyen például a munkaadó és a munkavállaló közötti munkaviszony, ahol a munkaadó által generált és feldolgozott adatmennyiség veszélyes a munkavállaló információs magánéletére nézve. Az információs magánéletet, mint fogalmat Koops és tsai. tárgyalták, ahol a szerzők a magánélet nyolc különböző típusát határozták meg, megállapítva azt is, hogy az információs magánélet:

> *a [magánélet] minden egyes alaptípusának átfogó szempontja, amelyet az az érdek jellemez, hogy [az érintett személyek] megakadályozzák a saját magukra vonatkozó*

[16] Peffers et al. 2007, 45. o.

információk gyűjtését, és hogy ellenőrizzék a mások számára jogszerűen hozzáférhető, saját magukra vonatkozó információkat[17].

Szervezeti szempontból ez megfelelési és biztonsági kockázatot jelent, amelyet gyakran megfelelő adatkezeléssel kezelnek. Az a munkaadó, aki kiszervezi szolgáltatásait külső szolgáltatók felé, fokozza a megfelelési és biztonsági kockázatokat. A szervezetek közvetlenül vagy közvetve kiteszik magukat ezeknek a kockázatoknak. Egyik ilyen kockázat az adatvédelmi incidens bekövetkezése, melyet a jelenleg hatályos jogszabályi keretben páratlanul szigorúan büntetnek. Mivel a kockázati fenyegetés állandó, a szervezeteknek erős bizalommal kell lenniük szolgáltatójuk megfelelőségi szintje iránt. Abban az esetben, ha a szolgáltatásokat felhőalapú számítástechnikán (Cloud Computing, CC) keresztül nyújtják, a kockázat még tovább nőhet. Egy felhő alapú környezetben valószínűleg más szervezetek is csatlakoznak az infrastruktúrához: felhő-brókerek, felhő-ellenőrök, felhő-közvetítők és egyéb ügynökök. Így a felhőalapú információs társadalommal összefüggő adatkezelésre vonatkozó szabályok adatvédelmi ökoszisztémája (Privacy Ecosystem, PECO) legalább három, de néha még annál is több kulcsfontosságú résztvevőből álló interoperabilitási zónaként határozható meg[18] .

Ugyanakkor, a magánélet és az adatvédelem jelenlegi követelményei arra engednek következtetni, hogy a technológiai és szabályozási intézkedések nem biztosítottak kielégítő védelmet a felhasználók számára az információs és kommunikációs technológiák (Information and Communication Technologies, ICT) terén[19].

Ez az egyik oka annak, hogy az adatvédelem és az adatbiztonság mára az IT rendszerek alapvető összetevője és jellemzője. Az EU ennek előmozdítására elfogadta az Ann Cavoukian[20] által megfogalmazott és mára már globális szinten közismert PbD-elveket. A PbD-elvek azonban mint olyanok nem kerültek be a GDPR 5. cikkében előírt alapvető adatvédelmi elvek közé. Ezek inkább az integritás és a bizalmas jelleg elvének kiterjesztését jelképzeik, mivel a beépített adatvédelem

[17] Koops et al. 2016, 568. o.
[18] Ezek között megemlítendő az adatkezelő aki IT szolgáltatást vagy megoldást igénybe vevő ügyfél, az adatfeldolgozó mint a megoldás szolgáltatója, a megoldás szolgáltatója által az ellátási láncban igénybe vett további alvállalkozó szervezetek, valamint az egyének mint érintettek, akiknek az adatai feldolgozásra kerülnek.
[19] van de Pas - van Bussel 2015, 186. o.
[20] Cavoukian 2013, pp. 2-3.

módszertani megközelítése nagyobb hangsúlyt fektet az adatbiztonságra, mint a magánélet védelmére[21]. Cavoukian által javasolt PbD hét alapelve röviden a következőképpen írható le:

a. Proaktív, nem reaktív; megelőző, nem orvosló: megelőzi és megakadályozza a magánéletet sértő eseményeket, mielőtt azok bekövetkeznének. Röviden, a jogsértést okozó esemény előtt történik, nem pedig utána.
b. A magánélet védelme mint alapértelmezett beállítás: ha az egyén nem tesz semmit, akkor a magánélete érintetlen marad. Az egyénnek nem kell cselekednie a magánéletének védelme érdekében. Röviden, a magánélet védelme alapértelmezés szerint be van építve a rendszerbe.
c. A tervezésbe beágyazott adatvédelem: az IT rendszerek alapvető funkcióinak egyik alkotóelemévé válik. Az adatvédelem a rendszer szerves részét képezi, anélkül, hogy a funkcionalitás csökkenne. Röviden, nem egy utólagos kiegészítés.
d. Teljes funkcionalitás - pozitív összegű, nem zéró összegű: segít elkerülni a hamis kettősségek látszatát, mint például az adatvédelem és az adatbiztonság közötti konfliktushelyzetet. Röviden, mindkettő lehetséges egyidőben.
e. Végponttól végpontig tartó biztonság - teljes életciklus-védelem: a rendszerbe az első információgyűjtés előtt beágyazott védelem az érintett adatok teljes életciklusára kiterjed, a kezdetektől a végpontig. Röviden, ez egy bölcsőtől a sírig tartó védelem.
f. Láthatóság és átláthatóság: az alkotóelemek és műveletek láthatóak és átláthatóak maradnak a felhasználók és a szolgáltatók számára egyaránt. Röviden, az IT rendszer megbízható és ellenőrzött.
g. A felhasználói adatvédelem tiszteletben tartása: megköveteli a fejlesztőcsapatoktól, hogy az egyén érdekeit tartsák szem előtt az olyan intézkedésekkel, mint az erős adatvédelmi alapértelmezett beállítások, a megfelelő értesítés és a felhasználóbarát lehetőségek biztosítása. Röviden, az IT rendszer egyértelműen felhasználó-központú.

3. KUTATÁSI CÉL ÉS HIPOTÉZIS

[21] Fabiano 2017, 731. o.

A doktori disszertáció egy interdiszciplináris kutatási terv eredményeit tartalmazza. Ez a terv az európai PbD-elvek alkalmazását, mint teljes funkcionalitás koncepcióját kívánja tárgyalni[22]. Célja annak feltárása, hogy létezik-e egyéni és sajátos európai beépített adatvédelem, valamint azt hogyan alkalmazzák és hogyan érvényesítik. A tézis arra a gondolatra épít, hogy az európai beépített adatvédelem a disruptív innováció katalizátorává válhat. A disruptív innovációhoz egy lépést hozzáadva, az infrastruktúra inverziójának lehetőségét tárgyalja[23]. Ezért holisztikus szemléletet alkalmaz a szabályozási környezetre[24] és a szoftvertervezésre[25] mint kutatási területek keresztmetsztére.

Vitatható, hogy az információs társadalommal kapcsolatos fejlesztések során feltételezhetően nem elégségesek a magánélet védelmére és az adatvédelemre vonatkozó stratégiák. Martens és Teuteberg úgy rendelkezett, hogy az információs társadalommal kapcsolatos szakirodalomban csak kevés explicit értékelési megközelítés található a referenciamodellekkel kapcsolatban, amelyek többsége azonban nem vezet meggyőző eredményekhez[26]. Ehhez képest a PbD-elveket beágyazó információs rendszerek kétségtelenül gazdasági előnyökkel járnak. Ezek az előnyök fontos szerepet játszanak a felhasználók elégedettségében. A PbD-elvek alkalmazása stratégiai jelentősségű.

A kutatási célkitűzés annak bizonyítása, hogy a szoftverarchitektúrában a PbD-elvek alkalmazását a magánélet védelmére és az adatvédelemre vonatkozó jogszabályokból eredő követelmények vezérlik, és bár azok az üzleti célok által manipuláltak, végül a disruptív innováció termékeként az infrastruktúra inverzióját elősegítő IT rendszerekké alakulnak. Ennek érdekében úgy véljük, hogy Európában a PbD-elvek inkább az adatok anonimizálására és az adatbiztonságra összpontosítanak. Gyakorlatilag az új szoftvermegoldásoknak a lehető legkevesebb személyes

[22] Cavoukian 2006, pp. 3-4.
[23] *Az infrastruktúra-inverzió fogalmát akkor használják, amikor egy új technológiának először a régi infrastruktúrát kell használnia, és ez konfliktust és nyomást okoz, ami infrastruktúra-inverzióhoz vezethet. Amikor egy új technológiát vezetnek be, sokan gyorsan azt mondják: "Látod, ez egyáltalán nem működik, lassú, vagy nem működik olyan jól". Ez nem újdonság. Ez történik minden alkalommal, amikor egy új, disruptív hatású technológia jelenik meg; az elfogadását követő első néhány évben a meglévő technológiának, amelyet megzavar, el kell azt viselnie. Amikor egy disruptív technológiát vezetünk be, ellenállásba ütközünk. Az ellenállás az első reakció. Azok járnak sikerrel, akik folytatják - még akkor is, ha a társadalom többi része azt mondja nekik, hogy őrültek. Kezdetben a disruptív technológiának egy olyan világban kell élnie, amelyet az általa felváltott technológia számára hoztak létre. Az infrastruktúra inverziója az, amikor az új technológia a régi infrastruktúrán él, majd megfordul. Kiépítjük az infrastruktúrát, majd a régi infrastruktúra ráépül az új technológiára tervezett infrastruktúrára.* (Antonopoulos 2018).
[24] Bygrave 2010, 179-198. o.
[25] Sommerville 2008, 241-266. o.
[26] Martens - Teuteberg 2011, 8. o.

adattal kell működniük, egyenértékű nem személyes adatokkal helyettesítve azokat. Amennyiben a helyettesítés nem lehetséges, a kezelésüknek a szervezet számára megfizethető legmagasabb biztonsági előírások mellett kell történnie. Bizonyos értelemben ez az adatvédelemi szabályok visszafogott, a magánélet védelmére vonatkozó szabályok pedig hangsúlyosabb alkalmazását fogja eredményezni. A kutatási hipotézist az európai PbD-elvek érvényesítése köré építjük fel. Megpróbáljuk megérteni, hogy ennek az érvényesítésnek milyen hatásai vannak. Arra törekszünk, hogy megtudjuk, az adatvédelmi hatóságok (Data Protection Authorities, DPAs) úttörő szerepet játszanak-e a magánélet védelmének új megközelítésében. Ezért szeretnénk mérni a tevékenységüket.

4. KUTATÁSI RÉS ÉS KÉRDÉS

Az adatvédelem és a magánélet védelmének szabályozása kiemelkedő fontosságú[27]. A magánélet védelme és az adatvédelem kiágazásai még soha nem jutottak ilyen messzire és ilyen hatékonysággal. A tudomány jelenlegi állása alapján, a szakirodalmi apparátus vizsgálata után megállapítható, hogy a magánélet védelmével és az adatvédelem elégtelen szintjével kapcsolatos aggályok az információs társadalommal összefüggő területeken megalapozottak, és mérsékelt szintű vitát váltanak ki. Különösen a beépített adatvédelmi alapelveknek adatvédelmi hatóságok általi érvényesítését kutatják kevéssé.

A doktori disszertációban beazonosítjuk ezt a konkrét részterületet, amely a kutatási rést biztosítja. Szándékunk, hogy gazdagabbá tegyük a PbD-elvek alkalmazásának érvényesítésére vonatkozó szakterületet azáltal, hogy közérthetővé tesszük azt. Ezért kutatási kérdésünk arra irányul, hogy feltárjuk, mérhető-e a PbD-elvek alkalmazásának érvényesítése, és ha igen, milyen lehetséges módjai vannak ennek?

Kutatási eredményeink segíthetnek a szervezeteknek abban, hogy leküzdjék az adatvédelem alkalmazasával kapcsolatos nehézségeket saját szervezetükben. Továbbá az eredmények rávilágítanak olyan gyakorlatokra, amelyek oktató jellegűek az adatvédelmi hatóságok számára.

5. KUTATÁSI MÓDSZERTAN

[27] Löhe - Blind 2015, 5. o.

Mertens a kutatást olyan szisztematikus vizsgálatként írja le, amelynek során adatokat gyűjtenek, elemeznek és valamilyen módon értelmeznek annak érdekében, hogy "*egy oktatási vagy pszichológiai jelenséget megértsenek, leírjanak, megjósoljanak vagy ellenőrizzék, vagy hogy az ilyen összefüggésekben az egyéneknek nagyobb hatalmat adjanak*"[28] . Azt javasolja továbbá, hogy "a *kutatás meghatározásának pontos természetét befolyásolja a kutató elméleti kerete*", az elméletet pedig arra használják, hogy kapcsolatot teremtsenek a jelenséget leíró vagy magyarázó konstrukciók között, megpróbálva azt hasonló eseményekkel összekapcsolni[29]. Mackanzie és Knipe azt is előírja, hogy az elméleti keretet, amely különbözik az elmélettől, néha paradigmának nevezik[30] és befolyásolja a tudás tanulmányozásának és értelmezésének módját[31]. A paradigma kiválasztása határozza meg a kutatás szándékát, motivációját és elvárásait[32]. A paradigma kijelölése nélkül nincs alapja a későbbi választásoknak a módszertan, a módszerek, a szakirodalom vagy a kutatási terv tekintetében[33]. Ezeket a megállapításokat szem előtt tartva mindenekelőtt a kutatási paradigmát határoztuk meg.

A tudományos kutatásban számos kutatási paradigma van jelen, mint például: pozitivista, konstruktivista, interpretivista, transzformatív, emancipációs, kritikai, pragmatista és dekonstruktivista paradigmák. A kutatási kérdés megválaszolására és a kutatási cél elérésére több paradigma is alkalmas, személyes motiváció miatt a pragmatikus paradigmát öleltük el. A pragmatizmus kutatói a "mit" és "hogyan" típusú kutatási kérdésére összpontosítanak[34]. Ez jól tükröződik a doktori disszertáció kutatási kérdésében is. A pragmatikus paradigma lehetővé teszi és ösztönzi a vegyes kutatási módszerek alkalmazását is, ami biztosítja az átfogó kutatáshoz szükséges rugalmasságot. Creswell megemlíti, hogy a pragmatikus paradigma a "kutatási kérdést" helyezi a középpontba, és több megközelítést alkalmaz a probléma megértésére[35] .

Ez a kutatási paradigma olyan módszertanok kialakításához ajánlott, amelyek mind az akadémiában, mind a gyakorlatban hasznosak lehetnek. Mégis, a létező kutatási paradigmák híres kutatói úgy vélekednek, hogy ilyen esetben a kockázat abban rejlik, hogy a kutatási kérdés

[28] Mertens 2005, 2. o.
[29] Ibid.
[30] A szerzők hivatkoznak Mertens paradigmákról szóló tanulmányára is.
[31] Mackenzie - Knipe 2006.
[32] Ibid.
[33] Ibid.
[34] Creswell 2003, 11. o.
[35] Ibid.

központi elemmé válik és az adatgyűjtési és elemzési módszereket a kutató úgy választja ki, mint amelyek a legvalószínűbbek, hogy betekintést nyújtanak a kérdésbe, anélkül, hogy hűséget tanúsítanának bármely alternatív paradigma felé[36]. Ezért megállapítható, hogy a pragmatikus paradigma problémaközpontú és a valós gyakorlatra orientált[37]. Mindazonáltal a transzformatív paradigma is rendelkezik kulcsfontosságú jellemzőkkel, amelyeket előszeretettel alkalmaztunk a kutatás során. Ilyenek például annak részvételi és változásorientált jellemzői[38].

A kutatás során a Mackanzie és Knipe által meghatározott kutatási térképet követtük[39]. A kutatási térképet a kutatás lefolytatásának általános útmutatójaként használják. A térkép követése megelőzi az alacsony módszertani illeszkedés szintjén felmerülő problémákat is, amint azt Edmondson és McManus a legmegfelelőbb módszertan megtalálására vonatkozó átfogó iránymutatásukban leírták[40]. A kutatás során egy átdolgozott Akciótervezési Kutatási Módszertant (Action Design Research, ADR) alkalmaztunk[41]. Ez helyszíni és asztali munkát egyaránt igényelt. Az alternatívákat, mint az egyszerűsített akciókutatás és az esettanulmányi kutatás, szintén fontolóra vettük. Az esettanulmányokon alapuló kutatás különösen hasznos bizonyos problématípusok esetében, mivel alkalmas a gyakorlatban tevékenykedő szakemberek tudásának megragadására. Baxter és Jack is arra a következtetésre jutott, hogy a kvalitatív esettanulmány olyan kutatási megközelítés, amely megkönnyíti egy jelenség kontextuson belüli feltárását különböző adatforrások felhasználásával[42]. Ez biztosítja, hogy a kérdést nem egy lencsén keresztül, hanem többféle lencsén keresztül vizsgáljuk, ami lehetővé teszi a jelenség többféle aspektusának feltárását és megértését[43]. Figyelemre méltó azonban, hogy Yin szerint az esettanulmányra alapuló kutatást akkor kell megfontolni, ha a kutató nem tudja manipulálni a vizsgálatban részt vevő alanyok viselkedését[44]. Yin kijelentése a saját kutatásunk szempontjából elengedhetetlen fontossággal bír. A helyszíni munka során a kutatási folyamatba bevont célcsoportok viselkedését

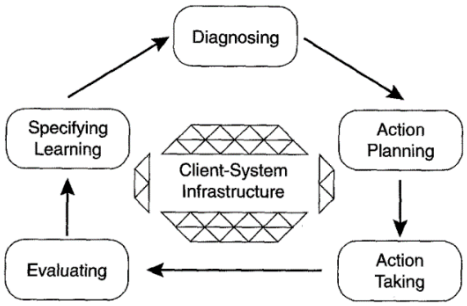
[36] Mackenzie - Knipe 2006.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Edmondson - McManus 2007, 1170. o.
[41] Mullarkey - Hevner 2018, pp 1-16.
[42] Baxter - Jack 2008, 544. o.
[43] Ibid.
[44] Idézi: Baxter - Jack, 555. o.

végig befolyásolhattuk. Ez volt az egyik oka annak, hogy az esettanulmányi kutatási módszert nem tekinthettük optimális megoldásnak.

Másrészt az ADR-t a tudományos ismeretek megszerzésének intervencionista megközelítéseként határozzák meg, amely a posztpozitivista hagyományban szilárd alapokon nyugszik[45]. Az intervencionista megközelítés a transzformatív paradigmához is illeszkedik. Ezt a kutatók kétlépcsős folyamatként magyarázzák:

a. a *diagnosztikai szakasz a* társadalmi helyzetnek a kutató és a kutatás alanyai által közösen végzett elemzését foglalja magában; és
b. a *terápiás szakasz az* együttműködésen alapuló változtatási kísérleteket foglalja magában, ahol ilyen változtatásokat vezetnek be, és azok hatásait tanulmányozzák[46] .

A megfelelő minőségű kutatási munka biztosításához ebben a kutatásban további struktúrákat vezetünk be az ADR-re. Így az akciótervezési kutatási módszertan ciklus öt, többször ismétlődő fázist tartalmazott: (1) diagnosztizálás, (2) akciótervezés, (3) akciók végrehajtása, (4) értékelés és (5) a tanulás meghatározása[47] , amint azt a *3. ábra* szemlélteti.



Ábra 3. Akciókutatási ciklus[48] .

Baskerville és Wood-Harper a módszer jellemzőit azonosította az akciókutatás ideális területeivel kapcsolatban, amikor a következőket írják elő:

a. a kutató a kutatásban aktívan részt vesz, és mind a kutató, mind a szervezet számára várható előnyökkel jár;

[45] Baskerville - Wood - Harper 1996, 237. o.
[46] Ibid.
[47] Ibid.
[48] Ibid.

b. a megszerzett tudás azonnal alkalmazható. A kutató ilyenkor nem egy távolságtartó megfigyelő, hanem egy aktív résztvevő, aki explicit, világos fogalmi kereteken alapuló új ismereteket kíván hasznosítani; és
c. a kutatás egy ciklikus folyamat, amely összekapcsolja az elméletet és a gyakorlatot[49].

6. ADATGYŰJTÉS ÉS ELEMZÉS

Először, a választott kutatási módszer megkövetelte a szisztematikus és ismétlődő adatgyűjtést. A kutatási terv rendszeres havi és heti találkozókat feltételezett a különböző IT projekteken dolgozó fejlesztő csapatokkal. A doktori disszertáció elkészítésének teljes időtartamában a szerző minden ilyen projektben tanácsadói szerepkört látott el adatvédelemmel kapcsolatos kérdésekben. Az alkalmazott kutatási módszerek jellegéből adódóan itt az adatgyűjtés longitudinális volt. Ezeket arra használtuk, hogy az elemzett konvergens technológiák és az európai beépített adatvédelem elvei közötti kompatibilitást elemezzük. Ehhez kapcsolodó munkánkat a disszertáció 6. fejezetében mutatjuk be. A különböző projektekben való együttműködés jellegéből adódóan itt tanúi lehetünk olyan informatikai megoldások kialakulásának, amelyek az európai PbD-elvek alkalmazását magukba foglalják, miközben megtartják fő funkcionalitásaikat.

Másodszor, teljesen strukturált interjúkat használtunk a nemzeti adatvédelmi hatóságnál dolgozó interjúalanyok tudásának kinyerésére. Bár hat interjúalannyal vettük fel a kapcsolatot, csak háromtól kaptunk választ. Az interjúalanyok kiválasztása az országok által kiszabott legmagasabb bírságok és az országok által kiszabott összes bírság legmagasabb száma alapján történt. Az interjúalanyoktól levont következtetéseinket a disszertáció 7. fejezete ismerteti. Ezeket a Miles és tsai.[50] által leírt technikákkal elemeztük, ahol a kvalitatív adatokat kvantitatív adatokra kódoltunk át. A fejezetben anonimizált interjúválaszokat használtunk.

Harmadszor, félig strukturált interjúkra támaszkodtunk, hogy megértsük, mit jelent a szervezeti adatvédelem az ilyen szervezetekkel dolgozó szakértők számára. A saját szakértői hálózatunkat használtuk fel arra, hogy több európai országot lefedő interjúalany-állományt hozzunk létre. A cél az volt, hogy megértsük, hogyan kezelik a szervezetek a PbD-elvek alkalmazásából eredő kihívásokat azáltal, hogy folyamatos, átfogó és hatékony adatvédelmi programokat biztosítanak.

[49] Ibid., 239. o.
[50] Miles et al. 2014, pp. 7-18.

Ezt azért találtuk lényegesnek kutatni, mert ha nincs bevezetett szervezeti adatvédelmi program, akkor kevés az esélye annak, hogy a PbD-elvek alkalmazása bekerüljön az ilyen szervezetek üzleti gyakorlatába. Az interjúk során különböző országokat részesítünk előnyben, mivel így többféle megközelítést fedezhetünk fel. Az interjúk feljegyzéseit a disszertáció 3. fejezetében mutatjuk be. A fentiekkel megegyezően az interjúválaszokat itt is anonimizáltuk.

Az összegyűjtött hatalmas mennyiségű kvantitatív és kvalitatív adatmennyiség végül lehetőséget adott tartalomelemzésre és páronkénti összehasonlításra is. A PbD-elvek alkalmazására alapozott rendszerarchitektúrák összehasonlító vizsgálatát így a doktori disszertáció az 5. fejezete ismerteti. Ennek a fejezetnek elsősorban nem az a feladata, hogy a kiválasztott architektúrákat kommentálja. Ehelyett inkább arra irányul, hogy bemutassa azon területek gazdagságát, amelyeken a PbD-elvek gyakorlati alkalmazásra találhatnak. Ebben a fejezetben azt demonstráljuk, hogy a magánélet védelme hogyan lép túl a tisztán elméleti kereteken és képez lenyomatot a gyakorlatban.

A kutatási kérdés megválaszolása érdekében a doktori disszertáció 7. fejezetében szövegbányászatot, döntési fa modellezést és a GDPR-bírságok előrejelző elemzését végeztük el gépi tanulási technikák segítségével. Itt a Rapidminer és az R adatelemzési szoftvereket használtuk. Ez a tanulmány leghangsúlyosabb része. Ettől vártuk a legjelentősebb eredményeket és a jogi adatelemzés, mint megcélzott szakterület gazdagodását.

7. TERMINOLÓGIA

A felhasználók manapság személyes adataikkal és magánéletükkel fizetnek; nem mindig járnak jól, ha a szolgáltatások "ingyenesek"[51]. Ezáltal az adat az értéklánc csúcsára kerül, és a digitális korszak új valutájává, valamint globális szintű üzleti lehetőségeket kínáló fogalommá válik. A nagyméretű adatállományok kora számos szervezet stratégiai döntéshozatalában központi szerepet játszik. A nagyméretű adatokkal együtt a magánélet védelmével kapcsolatos aggályok új dimenziói is felmerülnek[52]. Egyre több szervezet alkalmazza az adatvezérelt üzleti modelleket és stratégiákat, hogy versenyelőnyt szerezzen és tartson fenn versenytársaival szemben[53]. A személyes adatok túlzott mértékű kezelésének megakadályozására az EU reformcsomagot

[51] Stucke - Grunes 2016, 9. o.
[52] Mantelero 2017, 139-154. o.
[53] Stucke - Grunes 2016, 9. o.

fogadott el[54], amelynek célja, hogy a világon a legmagasabb szintű adatvédelmi normákat biztosítsa. A jogi eszközök nagyban befolyásolják a szervezetek üzleti modelljeit azáltal, hogy meghatározzák a jogszerű tevékenységek határait meghatározó kötelező normákat. A személyes adatok kezelésére vonatkozó szabályok hatálya alá tartozó szervezeteknek részt kell venniük az imperatív normák jogszabályi rendszerében.

Az innovációt gyakran úgy írják le, mint egy ötlet vagy találmány olyan áruvá vagy szolgáltatássá való átalakításának folyamatát, amely értéket teremt és amelyért a felhasználók fizetnek. A PbD-elvek alkalmazása révén az innováció megjelenhet termék- és folyamatszinten, de akár üzleti modellek szintjén is.

A disruptív innovációt illetően két jellegzetes tulajdonságra lehet következtetni. Először is, a piacra lépők megvethetik a lábukat azáltal, hogy a figyelmen kívül hagyott szegmenseket céloznak meg, és termékeiket alacsonyabb áron kínálják. Ezek a termékek az ilyen vásárlók igényeihez képest megfelelőbb funkcionalitást képviselnek, ahol az árkülönbségből adódó hozzáférhetőség egy fontos szempont. Emellett egyes disruptív innovációk új piacok szegmentálásból is eredhetnek, amikor a cégek olyan piacokat hoznak létre, amelyek korábban nem léteztek[55]. Másodszor, a disruptív innovációk addig nem találnak fogást a többségi vásárlókon, amíg a minőség nem éri el az ő színvonalukat[56].

Az EU reformcsomagját megalkotók feltételezték, hogy létezik egy egészséges piac az adatvédelmi technológiák és termékek vagy szolgáltatások számára, amely ösztönözheti a személyes adatok védelmének alkalmazását; vagy, hogy ez reformcsomag segít egy ilyen piac létrehozásában[57]. Így a kisebb erőforrásokkal rendelkező szervezeteknek lehetőségük nyílik arra, hogy felkarolják a felhasználóközpontú termékek létrehozásának megközelítését, és elcsábítsák azokat a vásárlókat, amelyeket a hagyományos piaci szereplők e miatt elhanyagolnak. Ennek

[54] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: GDPR); Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a természetes személyeknek a személyes adatok illetékes hatóságok által a bűncselekmények megelőzése, kivizsgálása, felderítése vagy büntetőeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása céljából történő feldolgozása tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.
[55] Christensen et al. 2015, 47. o.
[56] Ibid.
[57] Bygrave 2017, 118. o.

következménye, hogy a szervezeteknek el kell dönteniük, milyen mértékben kötelezik el magukat a PbD-elvek alkalmazása mellett. Minden bizonnyal egy ilyen üzleti modell a többi szervezetet a vásárlók bizalmának elnyeréséért folytatott versenyre hívja. Nem szabad azonban elfelejteni, hogy a disruptív innováció egy folyamat, nem pedig egy termék; a diszruptorok gyakran olyan üzleti modelleket építenek, amelyek nagyon különböznek az inkumbensekétől, és az ilyen innovációk közül egyesek sikeresek lehetnek, mások elbukhatnak[58]. Ráadásul nincs tényleges garancia arra, hogy egy ilyen üzleti modell nyereséghez vezet, mivel nem minden disruptív innováció sikeres[59].

A magánélet és az adatvédelem egymással összefüggő fogalmak, bár nem szinonimák. Míg a magánélet védelme a magánszféra védelmét jelenti, addig az adatvédelem az egyén magánérdekeinek védelmét szolgálja. Röviden összefoglalva azt értjük ez alatt, hogy a magánélet védelme érdekében védjük a személyes adatokat is. Mi indokolja ezt a jogi védelmet? Gellert és Gutwirth úgy véli, hogy a magánélet és az adatvédelem különböző gyakorlatok termékei, mint például a politika, a jog, az etika, a gazdaság vagy a vallás. Szerintük a kihívás nem annyira az, hogy megtaláljuk az ezek "mögött" lévő alapvető egységet, mint inkább az, hogy megértsük, hogy - mivel mindegyik egyedi - hogyan hatnak egymásra és hogyan artikulálódnak[60]. A magánélet védelmét az Emberi Jogok Európai Egyezményének (EJEE) 8. cikkének (1) bekezdése rögzíti[61]. Továbbá a magánélet tiszteletben tartásához való jogot az EU Alapjogi Chartájának (EUCFR) 7. cikke is szentesítette[62]. Bár ezeket külön-külön szabályozzák, az olvasó megfigyelheti, hogy a magánélet és az adatvédelem fogalmai között szoros kapcsolat áll fenn. Sőt mi több, az olyan további kifejezések, mint a "titoktartás"[63] , a "bizalmasság"[64] és a "biztonság"[65] saját értelmezéssel rendelkeznek. A titoktartást és a biztonságot az egyén privilegizált állapotának részének tekintjük, míg a titoktartás szorosabban kapcsolódik az adatvédelemhez. A magánélet fogalma bizonyos

[58] Christensen et al. 2015, 48-49. o.
[59] Ibid., 50. o.
[60] Gellert - Gutwirth 2013, 522. o.
[61] Emberi Jogok Európai Egyezménye, www.echr.coe.int
[62] Az EU Alapjogi Chartája, HL, C 364/10, 2000.12.18.
[63] Az elrejtettség vagy rejtőzködés állapotaként hivatkoznak rá.
[64] Az az etikai alapelv, amely szerint személyes adatokat nem lehet nyilvánosságra hozni, kivéve, ha a nyilvánosságra hozatalt engedélyező hozzájárulás megvan.
[65] Egy személyt, épületet, szervezetet vagy országot fenyegetések, bűncselekmények vagy támadások ellen védő intézkedések összessége.

mértékig mindezeket magában foglalja. Ugyanakkor a magánélet és az adatvédelem között átfedések vannak, hiszen Gellert és Gutwirth így érvel[66]:

> *Mindent egybevetve, az adatvédelem és a magánélet védelme olyan módon fedik egymást, hogy az adatvédelem egyszerre tágabb és szűkebb, mint a magánélet védelme. Szűkebb, mert csak a személyes adatok kezelésével foglalkozik, míg a magánélet védelme szélesebb körű. Szélesebb azonban, mert a személyes adatok kezelésére vonatkozik, még akkor is, ha ez utóbbi nem sérti a magánéletet. A magánélet védelme is tágabb és szűkebb: vonatkozhat olyan adatok kezelésére, amelyek nem személyesek, de mégis érintik az egyén magánéletét, míg nem vonatkozik olyan személyes adatok kezelésére, amelyek nem tekinthetők a magánéletet sértőnek. Az is elmondható, hogy a személyes adatok kezelése nemcsak a magánélet védelme, hanem más alkotmányos jogok szempontjából is következményekkel járhat, és ez a legnyilvánvalóbb, akkor amikor az egyénekre vonatkozó adatok kezelése a diszkriminációs kockázatot hordoz.*

A magánélet és az adatvédelem kiemelt kettőssége nagyon fontos szempont, amelyet újra kell vizsgálnunk. Amint azt Kokott és Sobotta kifejtette, az EUCFR-ben a két jog közötti különbségtétel nem pusztán szimbolikus[67]. Az Európai Unió Bíróságának (EUB) és az Emberi Jogok Európai Bíróságának (EJEB) ítélkezési gyakorlata megerősíti a fogalmak közötti különbségeket. Az EJEB ítélkezési gyakorlata már a legkorábbi szakaszokból kifejti a személyes adatok fogalmát a 108. egyezményre való hivatkozással[68]. A személyes adat fogalmát úgy határozza meg, mint "bármely azonosított vagy azonosítható személyre vonatkozó információt"[69]. A személyes adatnak nem csak az egyént közvetlenül azonosító információkra (*pl.* vezeték- és utónév)[70], hanem minden olyan elemre is ki kell terjednie, amely közvetve azonosít egy személyt (*pl.* dinamikus IP-cím)[71].

A személyes adatok gyűjtésének kérdésével kapcsolatban jelentős számú ügyet tárgyaltak. A kormányzati szervek által végzett titkos megfigyeléssel összefüggésben úgy rendelkeztek, hogy a

[66] Gellert - Gutwrith 2013, 526. o.
[67] Kokott - Sobotta 2013, 223. o.
[68] Az Európa Tanács 1981. január 28-i 108. számú egyezménye a személyes adatok gépi feldolgozása során az egyének védelméről
[69] Amann kontra Svájc, 2000, 65. bek.; Haralambie kontra Románia, 2009, 77. bek.
[70] Guillot kontra Franciaország, 1996, 21-22. bek.; Güzel Erdagöz kontra Törökország, 2008, 43. bek.; Garnaga kontra Ukrajna, 2013, 36. bek.; Henry Kismoun kontra Franciaország, 2013, bek. 25.
[71] Benedik kontra Szlovénia, 2018, 107-108. bek.

visszaélések elleni megfelelő és elégséges garanciák megléte alapvető fontosságú[72]. Az EJEB álláspontja szerint a polgárok titkos megfigyelésére vonatkozó adatkezelések csak annyiban tolerálhatók, amennyiben az a demokratikus intézmények védelméhez feltétlenül szükségesek[73]. Az ilyen beavatkozást releváns és elégséges indokokkal kell alátámasztani, és arányosnak kell lennie az elérni kívánt jogos céllal vagy célokkal[74]. A jognak kellően pontos, hatékony és átfogó biztosítékokat kell nyújtania a megfigyelésre irányuló adatkezelések elrendelése és végrehajtása, valamint a lehetséges jogorvoslatok biztosítása tekintetében[75].

Az adatvédelem modernkori kihívásait a technológiai fejlődés, az algoritmusok és a mesterséges intelligencia növekvő használata is eredményezte. E tekintetben ítélet született az ujjlenyomatok és biológiai minták gyűjtéséről és tárolásáról[76] , az arcfelismerésről[77], a mobiltelefon-szolgáltatók előfizetői adatok tárolására és a hatóságok kérésére történő átadására vonatkozó gyakorlatáról[78] vagy a hatóságok közvetlen, technikai eszközökkel történő hozzáféréséről a mobiltelefonos kommunikációkhoz[79].

Megjegyezték továbbá, hogy az interneten található tartalmak és közlések által az emberi jogok és szabadságok gyakorlására és élvezésére, különösen a magánélet tiszteletben tartásához való jogra nézve jelentett kár kockázata minden bizonnyal nagyobb, mint a sajtó által okozott káré, különösen a keresőmotorok fontos szerepe miatt[80]. A véleménynyilvánítás szabadsága és a személyes adatok védelme közötti érdekek közötti egyensúlyról szóló tudományos vita is mindeközben folyamatosan fejlődött. E tekintetben az EJEB úgy rendelkezett, hogy az internetes archívumok hozzájárulnak a hírek és információk megőrzéséhez és hozzáférhetővé tételéhez[81]. Az egymással versengő jogok közötti egyensúly megteremtésében a tagállamok számára biztosított mérlegelési jogkör nagyobb, ha a múltbeli eseményekről szóló hírarchívumokról van szó, nem pedig az aktuális eseményekről szóló hírekről szóló tudósításokról[82]. A sajtó azon kötelezettsége, hogy a

[72] Emberi Jogok Európai Bírósága 2020, 30. o.
[73] Klass és társai kontra Németország, 1978, 42. bek.; Szabó és Vissy kontra Magyarország, 2016, 72-73 bek.
[74] Segerstedt-Wiberg és társai kontra Svédország, 2000, 88. bek.
[75] Szabó és Vissy kontra Magyarország, 2016, 89. bek.
[76] S. és Marper kontra Egyesült Királyság, 2008, 112. bek.
[77] Gaughran kontra Egyesült Királyság, 2020, 70-98. bek.
[78] Breyer kontra Németország, 2020, 88. bek.
[79] Zakharov kontra Oroszország, 2015, 302-305. bek.
[80] M.L. és W.W. kontra Németország, 2018, 91. bek.
[81] Times Newspapers Ltd kontra Egyesült Királyság (1. és 2. sz.), 2009, 45. bek.
[82] Ibid. 45.

felelős újságírás elveinek megfelelően járjon el, biztosítva a közzétett történelmi, nem pedig a romlandó információk pontosságát, szigorúbb, ha az anyag közzététele nem sürgős[83]. Erre példaként említhető, hogy az EJEB egy olyan ügyben, amelyben 1,2 millió személy adózására vonatkozó személyes adatok tömeges áramlását tették közzé egy magazinban, majd ezt követően szöveges üzenetküldő szolgáltatás útján terjesztették, szintén úgy döntött, hogy nem áll fenn az automatikus terjesztés közérdekűsége[84].

Mindezekben az esetekben a magánélethez fűződő érdekek és a személyes adatok védelme között interferencia áll fenn. Ezek azért léteznek egymás mellett, mert lényegileg és formailag különböznek egymástól. Az egyik kihívás, amellyel a fejlesztők és a szoftvermérnökök folyamatosan szembesülnek, az a zavarosnak tűnő jogi terminológia, amelyet a magánélet védelmére és az adatvédelemre vonatkozó jogszabályok használnak. A kutatásban végzett tanácsadási munka során a célcsoportok ezt a zavaros terminológiát és annak nehéz megértését szintén visszaigazolták. Mint látható, ezek a fogalmak nem felcserélhetők egymással. Érdekesség azonban, hogy a szoftverfejlesztésben egy harmadik kifejezés, a "*privacy engineering*" fogalma nyert teret.

8. KONKLÚZIÓ

Kutatásunkban arra jutottunk, hogy az európai PbD-elvek alkalmazását három egymással versengő erő alakítja: a a szabályozás, az üzleti célok és a rendszerarchitektúrák. Ezek az erők etikai, gazdasági és technológiai szempontból hordoznak magukban sajátosságokat.

Ebben a kutatásban az európai PbD-elvek koncepciójának megértésére vállalkoztunk. Megvizsgáltuk annak természetét, alkalmazását és érvényesítését. Arra a következtetésre jutottunk, hogy az európai PbD-elvek két szempontból is kevéssé kutatott területek: szervezeti szinten (az egyéni szinthez képest); és főként a hatóságok általi érvényesítésének módját illetően. Az utóbbival kapcsolatban arra törekedtünk, hogy jelentős tudományos hozzájárulást nyújtsunk. Érdekelt bennünket, hogy az adatvédelmi hatóságok az európai PbD-elveket vizsgálva olyan hatásokat gyakorolnak-e, amelyek úttörő szerepet játszhatnak a magánélet védelmének új

[83] Ibid.
[84] C-73/07. sz. ügy, Satakunnan Markkinapörssi Oy és Satamedia Oy kontra Finnország [2017] ECLI:EU:C:2008:727, 175-197. bek.

megközelítéseiben. Ezért dolgoztuk ki tevékenységük mérésének lehetséges módjait, oly módon, hogy akár jogászi képesítéssel nem rendelkező szakemberek is megértsék munkánkat.

Választ ígértünk arra a kutatási kérdésre, hogy mérhető-e az európai PbD-elvek alkalmazásának érvényesülése, és ha igen, milyen lehetséges módjai vannak ennek? Kvantitatív és kvalitatív adatokon végeztünk adatelemzést, hogy a lehető legjobban megválaszolhassuk ezt a kérdést. Válaszunk egy mérsékelt igen, miszerint a PbD-elvek alkalmazásának érvényesítése mérhető. Bár ezen a ponton csak az elég jó mérési módokkal kell beérnünk, és nem szabad elmerülnünk a legoptimálisabb vagy legjobb módok kutatásában.

Ennek egyik oka az, hogy a PbD-elvek alkalmazásának érvényesítését vizsgáló ügyek körülményei kimagaslóan testreszabottak. Ezt a vonatkozó jogszabály megsértése esetén kiszabható közigazgatási bírságok összegének előrejelzésére szolgáló modellek létrehozása során mutattuk ki. Ezeknek az eseteknek a klaszterezése adatelemzési szempontból egy nagy kihívás volt.

A második ok, amiért nem ajánlott a legjobb mérési mód kutatása, az az Európában létező adathiány. Ez a probléma abban a filozófiai álláspontban gyökerezik, amelyet az európai jogalkotó az EU-n belüli adatgyűjtés témájában a mai napig képvisel. Az európai jogalkotók minden bizonnyal nem kedvelik azokat a programokat, amelyek gigantikus mennyiségű személyes adatot gyűjtenek az uniós polgároktól.

A harmadik okot az adatvédelmi hatóságok gyakorlatából kitűnő különbségek adják. Ezek a különbségek az adatvédelmi hatóságok eltérő szintű kompetenciáiból, jelentési struktúráiból, személyi állományaiból és működésükben szerzett gyakorlati tapasztalataikból származnak.

A fenti korlátozásokon túlmutatva, az európai PbD-elvek alkalmazásának érvényesítésére szolgáló mérési módszerek léteznek. Méréseink néhány alapvető megállapításhoz vezettek, melyeket a következők szerint ismertetünk:

a. **Az európai PbD-elvek alkalmazása "adatkímélő" üzemmódban működik:** azt állítjuk, hogy a mobiltelefonok adatkímélő üzemmódjához hasonlóan, ahol a legtöbb alkalmazás és szolgáltatás csak Wi-Fi kapcsolaton keresztül kap háttéradatokat, Európában az adatgyűjtést és adatkezelést minimálisra csökkentik. Tehát az európai PbD-elvek alkalmazása lényegében az adattakarékosságról szól. Kutatásunk részben

megcáfolta azt a meggyőződésünket, hogy ez a koncepció inkább az adatbiztonságra irányul.

b. **Az európai PbD-elvek alkalmazása platformfüggetlen:** a dolgozatban különböző infrastruktúrákat és konvergens technológiákat mutatunk be, amelyek kompatibilisek az európai PbD-elvek alkalmazásával. Így a koncepció valóban technológiasemleges.
c. **Az európai PbD-elvek alkalmazása egy eszközhasználati kötelezettség:** azt állítjuk, hogy az adatvédelmi hatóságok az európai PbD elvek alkalmazását eszközhasználati kötelezettségként kezelik. Egyszerűbben fogalmazva, a szervezeteknek először adatvédelmi hatásvizsgálatot kell végezniük, hogy megtudják, mely eszközök támogatják az adatkezelési tevékenységeiket, majd ezeket PbD-elvek szerinti kötelezettségük alkalmazni.
d. **Az európai PbD-elvek alkalmazása szorosan területi jellegű:** kutatásunkban arra a következtetésre jutottunk, hogy a PbD-elvek alkalmazásának érvényesítése nagymértékben függ a földrajzi mutatóktól (azaz országoktól és tartományoktól). A különböző szintű adatvédelmi kultúrák még mindig jelen vannak Európában. Ugyanakkor egyetemesen igaz, hogy az európai PbD-elvek alkalmazása erős uniós adatszuverenitást ír elő.

Fontos kiemelni, hogy a személyes adatok anonimizált adatokkal való hatékony helyettesítése talán bizonyos adatvédelmi törvények és rendeletek alkalmazásának elkerülését eredményezi. Ugyanakkor kiemelendő az is, hogy több törvény is létezik a magánélet védelmére. Ezek egy részhalmazának (*azaz a személyes adatok védelmének*) kizárása nem értelmezhető "mindent szabad" ideológiaként, amely nyitva hagyja az ajtót a magánéletet sértő üzleti gyakorlatok tömeges elterjedése előtt.

Hasonló módon több üzleti modell is ösztönzőként tartalmazza a PbD-elvek alkalmazását. Az ilyen üzleti modellekkel rendelkező szervezetek döntéshozói a PbD-elveket marketingeszközként használják. Ennek célja olyan stratégiáik kidolgozása, melyek megragadják vagy felgyorsítják a fogyasztói hűséget.

Végül, de nem utolsó sorban a rendszerarchitektúrák tervezői kulcsfontosságú szerepet játszanak a PbD-elvek alkalmazása során az információs társadalomban. A fejlesztőknek a tervezők által megfogalmazott elképzeléseket kell megvalósítaniuk. Szükség van a szerepkörök közötti

természetes szétválasztásra. A tervezőknek koordinált kapcsolatot kell kialakítaniuk és fenntartaniuk a fejlesztőkkel, miközben az ICT-hez kapcsolódó különböző szervezeti szempontokat (*pl.* a felelősségek egyeztetett megosztása) kezelik. A kutatók arra keresve a választ, hogy a fejlesztők miért nem képesek a magánélet védelmére vonatkozó intézkedéseket az információs társadalommal összefüggő rendszerekbe beépteni, néhány releváns következtetésre jutottak. Senarath és Arachchilage empirikus vizsgálatot végeztek, amelynek eredményeképpen olyan problémákra világítottak rá, mint a rendszerarchitektúrák és adatvédelmi követelmények közötti ellentmondások jelenléte, az adatvéldemi követelmények megfelelő megvalósításról való meggyőződés hiánya vagy az ilyen követelményekkel kapcsolatos ismeretek hiánya[85] . Hadar és tsai. egy másik jelentős problémát is találtak: a fejlesztőket aktívan elriasztják attól, hogy az információs magánélet védelmét prioritásként kezeljék, mivel elvárják, hogy megfeleljenek a szervezeti légkör által diktált normáknak és gyakorlatoknak[86]. Egy másik megállapítást Bednar és tsai. jelöltek meg, amely szerint a fejlesztőknek meg kell küzdeniük az adatvédelmi jogászokkal, és csak azért foglalkoznak az adatvédelemmel kapcsolatos kérdésekkel, mert erre kötelezik őket[87].

Annak ellenére, hogy frusztrációt okoz, az információs adatvédelem operacionalizálása leginkább a fejlesztők gondolkodásmódjától függ. Ezt a felelősséget azonban teljes egészében az ő kezükbe helyezni megalapozatlan teher. Ha a rendszerarchitectúrát tervezők aktívan vállalják az adatvédelemmel kapcsolatos követelmények teljesítését, a fejlesztők sokkal nagyobb biztonságban érzik magukat, mivel képzett személyek irányítják őket. Ehhez szükséges olyan oktatási programok bevezetése, amelyek a tervezőket ilyen tudással vértezik fel. Ezek a tervezők olyan rendszerarchitektúrák tervezésére kell összpontosítaniuk, amelyek a PbD-elvek alkalmazását tartják a középpontban. Így végső soron megvalósulhat a magánélet védelmére fókuszáló architektúrafejlesztés.

9. IRODALOMJEGYZÉK

1. Acquisti, A., Taylor, C. R., and Wagman, L. (2016): *The Economics of Privacy*. Journal of Economic Literature, Vol. 52, No. 2, 2016; Sloan Foundation Economics Research Paper No. 2580411.
2. Antonopoulos, A. (2018): Infrastructure Inversion by Andreas M. Antonopoulos. Steemit. Available at: https://steemit.com/bitcoin/@pbgreenpoint/infrastructure-inversion-by-andreas-m-antonopoulos [04.04.2021].

[85] Senarath - Arachchilage 2018, 4. o.
[86] Hadar et al. 2017, 20. o.
[87] Bednar et al. 2019, pp. 137-138.

3. Barth, S. and de Jong, M. D.T. (2017): *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*, Telematics and Informatics 34, no. 7, pp. 1038-1058.
4. Baskerville, R. and Wood-Harper, T. (1996): *A Critical Perspective on Action Research as a Method for Information Systems Research.* Journal of Information Technology. 11. 235-246. 10.1080/026839696345289.
5. Baxter, P., and Jack, S. (2008): *Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers.* The Qualitative Report, 13(4), 544-559.
6. Bednar, K., Spiekermann, S. and Langheinrich, M. (2019): *Engineering Privacy by Design: Are engineers ready to live up to the challenge?*, The Information Society, 35:3, 122-142, DOI: 10.1080/01972243.2019.1583296
7. Bygrave, L. (2010): *Privacy and Data Protection in an International Perspective*. Scandinavian studies in law, 165-200.
8. Bygrave, L., (2017): *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements.* Oslo Law Review, Volume 4, No. 2.
9. Cavoukian, A. (2013): *Privacy by Design*. Information and Privacy Commissioner of Ontario.
10. Cavoukian, A., (2006): *Creation of a Global Privacy Standard*. Available at: www.pc.on.ca/images/Resources/gps.pdf
11. Christensen, C.M., Raynor, M. and McDonald, R. (2015): *What is disruptive innovation?* Harward Business Review, December 2015.
12. Edmondson, A. and McManus, S. (2007): *Methodological Fit in Management Field Research*. Academy of Management Review. 32. 1155-1179. 10.5465/AMR.2007.26586086.
13. Fabiano, N. (2017): *Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard*. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, 2017, pp. 727-734.
14. Gellert, R. and Gutwirth, S. (2013): *The legal construction of privacy and data protection.* Computer Law and Security Review. 29. 522–530. 10.1016/j.clsr.2013.07.005.
15. Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S. and Balissa, A. (2018): *Privacy by designers: software developers' privacy mindset*. Empirical Software Engineering. 23. 10.1007/s10664-017-9517-1.
16. Jonshon, J. (2021): Global digital population as of January 2021, Statista, Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/
17. Kokott, J. and Sobotta, C. (2013): *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*. International Data Privacy Law. 3. 222-228. 10.1093/idpl/ipt017.
18. Koops, B.-J., Newell, B.-C., Timan, T., Škorvánek, I., Chokrevski, T., and Galič, M. (2016): *A Typology of Privacy*. University of Pennsylvania Journal of International Law 38(2): 483-575 (2017); Tilburg Law School Research Paper No. 09/2016.
19. Löhe, M. G. and Blind, K. (2015): *Regulation and standardization of data protection in cloud computing*. ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, 2015, pp. 1-6. doi: 10.1109/Kaleidoscope.2015.7383634.
20. Mackenzie, N. and Knipe, S. (2006): *Research dilemmas: Paradigms, methods and methodology*. Issues in Educational Research. 16. 193-205.
21. Mantelero, A. (2016): *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*. 10.1007/978-3-319-46608-8_8.
22. Martens, B. and Teuteberg, F. (2011): *Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model*. AMCIS 2011 Proceedings - All Submissions. Paper 228. http://aisel.aisnet.org/amcis2011_submissions/228.

23. Mertens, D.M. (2005): *Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches*. (2nd ed.) Thousand Oaks: Sage.
24. Miles, M. B. (2014): *Qualitative data analysis: a methods sourcebook* / Matthew B. Miles, A. Michael Huberman, Johnny Saldaña, Arizona State University. — Third edition. Thousand Oaks: Sage.
25. Mullarkey, M. T. and Hevner, A. R. (2018): *An elaborated action design research process model*. European Journal of Information Systems, DOI:10.1080/0960085X.2018.1451811.
26. Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. (2007): *A Design Science Research Methodology for Information Systems Research*. Journal of Management Information Systems, 24:3, 45-77, DOI: 10.2753/MIS0742-1222240302.
27. Senarath, A., and Arachchilage, N., (2018): *Why developers cannot embed privacy into software systems? An empirical investigation*. 211-216. 10.1145/3210459.3210484.
28. Snipe, M. (2021): 'The Markets for Privacy', Yale Journal of Law & Technology. Availablet at: https://yjolt.org/blog/market-privacy
29. Sommerville. I. (2015): *Software Engineering* (8th. ed.).
30. Stucke, M. E. and Grunes, A. P. (2016): *Introduction: Big Data and Competition Policy*. Oxford University Press.
31. van de Pas J. and van Bussel G. (2015): *Privacy Lost - and Found? The information value chain as a model to meet citizens' concerns*. The Electronic Journal Information Systems Evaluation Volume 18 Issue 2, (pp185- 195).

10. DÖNTVÉNYEK

1. C-73/07, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [2007], ECLI:EU:C:2008:727
2. Amann kontra Svájc, 2000
3. Benedik kontra Szlovénia, 2018
4. Breyer kontra Németország, 2020
5. Garnaga kontra Ukrajna, 2013
6. Gaughran kontra Egyesült Királyság, 2020
7. Guillot kontra Franciaország, 1996
8. Güzel Erdagöz kontra Törökország, 2008
9. Haralambie kontra Románia, 2009
10. Henry Kismoun kontra Franciaország, 2013
11. Klass és társai kontra Németország, 1978
12. M.L. és W.W. kontra Németország, 2018
13. S. és Marper kontra Egyesült Királyság, 2008
14. Segerstedt-Wiberg és társai kontra Svédország, 2000
15. Szabó és Vissy kontra Magyarország, 2016
16. Times Newspapers Ltd kontra Egyesült Királyság (1. és 2. sz.), 2009
17. Zakharov kontra Oroszország, 2015