Balogh Zsolt György–Kiss Attila–
Polyák Gábor–Szádeczky Tamás–
Szőke Gergely László*

Technológia a jog szolgálatában? – Kísérletek az adatvédelem területén

adatvédelem és technológia – privát szférát erősítő technológiák – beépített adatvédelem elve – Privacy by Design

A technológia fejlődésének társadalomra gyakorolt hatása a társadalomelmélet kedvelt témaköre az elmúlt ötven évben: számtalan szakirodalmi forrás elemzi az információs társadalom kialakulását és az informatikai és kommunikációs technológiák társadalmi hatásait. E társadalmi változások aztán jellemzően leképeződnek a jogalkotásban is, rendszerint több-kevesebb késéssel követve azokat. Az Európai Unió információs társadalom- és médiapolitikájának jogalkotási eredményei, az ahhoz kapcsolódó folyamatos szakmai és éles politikai viták, és egy új jogterület, az infokommunikációs jog kialakulása egyértelműen mutatja ennek jelentőségét.

Az átfogó stratégiai törekvésekkel párhuzamosan ugyanakkor több jogterületen hangsúlyosan megjelentek a technológiai megoldások mint a jogi védelem kiegészítői – érdemes csak a szerzői jog védelmére alkalmazott digitális jogkezelési rendszerekre (DRM),[1] az online média gyermekekre gyakorolt káros hatásai kapcsán felmerülő címkézési-szűrési mechanizmusokra vagy (a tanulmányunk tárgyaként megjelenő) privát szférát erősítő technológiákra (PETs)[2] gondolni. Ezekben az esetekben a technológia közvetlenül is szabályozószerepet tölt be, ezért igen izgalmas

* Dr. Balogh Zsolt György tudományos főmunkatárs, Budapesti Corvinus Egyetem Gazdálkodástudományi Kar Infokommunikációs Tanszék, zsolt.balogh@uni-corvinus.hu; dr. Kiss Attila PhD-hallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Közigazgatási Jogi Tanszék, Informatikai és Kommunikációs Jogi Csoport, kiss.attila@ajk.pte.hu; dr. Polyák Gábor egyetemi docens, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Közigazgatási Jogi Tanszék, Informatikai és Kommunikációs Jogi Csoport, gpolyak@ajk.pte.hu; dr. Szádeczky Tamás egyetemi docens, Óbudai Egyetem TÜV Rheinland Egyetemi Tudásközpont, szadeczky.tamas@kvk.uni-obuda.hu; dr. Szőke Gergely László tudományos segédmunkatárs, PTE ÁJK Közigazgatási Jogi Tanszék, Informatikai és Kommunikációs Jogi Csoport, szoke.gergely@ajk.pte.hu. A tanulmány alapjául szolgáló kutatás az Európai Unió és Magyarország támogatásával, az Európai Szociális Alap társfinanszírozásával a TÁMOP-4.2.2.C-11/1/KONV-2012-0005 azonosító számú „Jól-lét az információs társadalomban” című kiemelt projekt keretei között valósult meg.

[1] Digital Rights Management, a megoldások felhasználási lehetőségeiről l. Lencse Gábor: Tartalomvédelem: DRM. http://www.tilb.sze.hu/tilb/targyak/NGM_TA011_1/DRM.pdf (2014.03.16).

[2] Privacy Enhancing Technologies.

kutatási téma e szerepkör és a jog hagyományos szabályozószerepének egymáshoz való viszonya.[3]

A technológia szabályozószerepe kapcsán mindenképpen utalnunk kell Lawrence Lessig munkásságára.[4] Az amerikai jogász-filozófus professzor szerint a kibertér világában központi, meghatározó szerepet tölt be a „kód",[5] amely alatt az online közeg teljes infrastruktúráját érti: hardverek, szoftverek, az internetet működtető protokollok stb. A kód kényszerítő erejű szabályrendszerként meghatározza a kibertér törvényszerűségeit, a lehetséges és a nem lehetséges viselkedésformákat.[6]

Jelen kutatásunk a technológia és jog viszonyát a személyes adatok védelmével kapcsolatban vizsgálja, mivel az adatvédelmi jog megjelenését az 1970-es évekre kibontakozó technológiai forradalomra adott válaszlépésként is értékelhetjük. Ezt jócskán megelőzően, már az első magánszféra-védelemmel foglalkozó tanulmány, Samuel D. Warren és Louis D. Brandeis sokat hivatkozott, 1890-ben a *Harvard Law Review* hasábjain megjelent, „The Right to Privacy" című írása[7] is alapvetően az adott kor technológiai és társadalmi változásaira – az új, azonnali fényképezést lehetővé tevő fényképezőgép megjelenésére és a bulvársajtó terjedésére – reagált,[8] és az adatvédelmi jog változásait azóta is meghatározza a folyamatos technológiai fejlődésre való reagálás igénye.

E tanulmány azonban nem e történeti fejlődés okait,[9] hanem a technológia szabályozószerepét mutatja be az adatvédelem területén, áttekintve először a privát szférát erősítő technológiák helyzetét, majd a technológia szerepét általánosságban új kontextusba helyező – várhatóan a teljes adatvédelmi szabályozást átható – beépített adatvédelem (Privacy by Design) elvének kialakulását, végül e két jelenség egymáshoz való viszonyát és a jogszabályi környezetben való megjelenését.

[3] A technológia és más – gazdasági, kulturális, politikai – szabályozók kommunikációpolitikában betöltött szerepéről l. Polyák Gábor: Technológiai determinizmus a kommunikáció szabályozásában. *Információs Társadalom*, 2011/2. 31–47.

[4] E témában „Code and other laws of cyberspace" címmel jelent meg első könyve 1999-ben, majd ennek átdolgozott, második kiadása „Code version 2.0" címen 2006-ban került kiadásra.

[5] Lessig remekül rájátszik a „Code" kettős jelentésére: kódexet (jogot) és informatikai értelemben vett kódot egyaránt jelenthet.

[6] „Code is law", l. Lessig, Lawrence: *Code, Version 2.0*. New York, Basic Books, 2006, 5. http://codev2.cc/download+remix/Lessig-Codev2.pdf (2014. 03. 16.).

[7] Warren, Samuel D.–Brandeis, Louis D.: The Right to Privacy. *Harvard Law Review* 1890/4. 195–220. http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/hlr4&id=205&terms=photograph#207 (2014. 03. 16.).

[8] L. erről részletesen Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, 2013/3.

[9] E témakört ugyanis több szempontból is feldolgozta már a hazai jogirodalom, l. Jóri András: *Adatvédelmi kézikönyv. Elmélet, történet, kommentár*. Budapest, 2005, 21–66, valamint Szőke: *i. m.,* passim.

1. A privát szférát erősítő technológiák

A „Privacy Enhancing Technologies" kifejezést 1995-ben, a holland állam és az ontariói adatvédelmi biztos hivatalának közös projektje során használták először.[10] Noha azóta közel két évtized telt el, nem csökkent az érdeklődés az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások fejlesztése iránt. Az adatszivárgások, visszaélési botrányok magas száma jól mutatja, hogy ismét komoly szerepet kaphat a technológiai megoldások alkalmazása az adatvédelem területén, önmagában a szabályozás, önszabályozás és a jogalkalmazás sem tudnak elegendő védelmet nyújtani a felhasználók számára.[11]

1.1. Definíciós kísérletek

A „Privacy Enhancing Technologies" (PETs) kifejezésre nem található általánosan elfogadott meghatározás,[12] az az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneve.[13] A nemzetközi jogirodalom egy gyakran hivatkozott megfogalmazása szerint a PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs magánszférát a személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, anélkül hogy csökkentené az információs rendszer funkcionalitását.[14] Alkalmazásuknak különös jelentősége van minden olyan technológiai fejlesztés során, amelyek esetében magánszemélyek (érintettek) személyes adatait gyűjtik, elemzik, hasznosítják, tehát adatkezelés történik.

A hazai szakirodalomban az angol PETs többféle fordításával is találkozhatunk, gyakran olvasható a „magánszféravédő technológiák"[15] vagy „adatvédelmet elősegítő technikai intézkedések"[16] meghatározás, de a legtalálóbb talán Székely Iván azonos betűszóval rövidíthető fordítása, a „privát szférát erősítő technológiák"[17] elnevezés.

[10] Blarkom, Gilles W. van–Borking, John J.–Olk, Eddy (Ed.): *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*. The Hague, PISA Consortium, 2003, 33.

[11] Székely Iván: Privát szférát erősítő technológiák. *Információs Társadalom*, 2008/1, 22. http://pet-portal.eu/files/oldfiles/articles/2008/02/InfTars_PET.pdf (2014. 03. 17.).

[12] London Economics: *Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security*, 2010. 2. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (2014. 03. 17.).

[13] Burkert, Herbert: *Privacy-Enhancing Technologies: Typology, Critique, Vision*. In Agre, Philip E.–Rotenberg, Marc (szerk.): *Technology And Privacy: The New Landscape*. MIT Press, 1997, 125.

[14] Blarkom van–Borking–Olk: *i. m.,* 36.

[15] Jóri 2005, *i. m.,* 18 és http://doktori-iskola.ajk.pte.hu/files/tiny_mce/File/Archiv2/jori/jori_dolgozat_nyilv.pdf (2014. 03. 17.).

[16] Szádeczky Tamás: *Szabályozott biztonság. Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan.* Pécs, 2011, 164. http://doktori-iskola.ajk.pte.hu/files/tiny_mce/File/Vedes/szadeczky/ertekezes_szadeczky_nyilv.pdf (2014. 03. 17.).

[17] Székely: *i. m.,* 22.

Ezen eszközök alapvető célja, hogy ne csak az adatokat általában, hanem az adatalanyokat, az érintetteket is védjék a visszaélések ellen, és elősegítsék az információs önrendelkezéshez való jog érvényesíthetőségét. A megoldások nem jogi védelmet nyújtanak, de alkalmazásuk tömegessé válása és ennek következményei miatt a jogi szabályozás tárgyaivá válhatnak.[18] Az Európai Parlament és a Tanács személyes adatok feldolgozására vonatkozó, 2012. januárban nyilvánosságra hozott reformcsomagjának tervezetében is szerepelnek közvetve e megoldások, ugyanis az új adatvédelmi célok érvényesítésében a beépített adatvédelem (Privacy by Design) elvnek kiemelt szerepet tulajdonít az európai jogalkotó, melynek egyik legfontosabb eleme a PET-ek alkalmazása és azok terjedésének elősegítése.

1.2. Alkalmazási területek

A privát szférát erősítő megoldások fejlesztésének egyik célja az, hogy a mai számítástechnikai megoldásokat segítségül híva, azok összes előnyét megtartva, magával a technológiával mérsékeljék a privát szférát fenyegető káros hatásokat, megakadályozzák a jogszerűtlen adatkezeléseket, döntési lehetőséget biztosítsanak a felhasználóknak saját adataik sorsáról,[19] így helyreállítsák a felhasználók online szolgáltatásokba vetett bizalmát. A privát szférát erősítő megoldások egyrészt e megfigyelők ellenőrzése nélkül, a magánszféra megőrzése mellett teszik lehetővé az online kommunikációt, böngészést, internetes tranzakciókat,[20] másrészt ellenőrzési lehetőséget adnak az érintetteknek arra vonatkozóan, hogy mely személyes adatok vannak az adatkezelők birtokában, hogy azok felett a számukra biztosított jogi lehetőségekkel élve rendelkezhessenek.[21]

Az Európai Bizottság a magánélet védelmét erősítő technológiákról 2007-ben készült jelentésében hasonlóan határozta meg a PET-ek alkalmazásának célját: *„nehezebbé váljon bizonyos adatvédelmi jogszabályok megszegése és/vagy könnyebb legyen a szabálysértések leleplezése”.*[22] A Bizottság ugyanakkor arra is rávilágított, hogy az utólagos jogérvényesítés és egy eljárás lefolytatása nyilvánvalóan költségesebb és kevésbé hatékony, mint a jogsértés megelőzése, ezért a privát szférát védő technológiák az adatkezelők számára is komoly segítséget nyújtanak ahhoz, hogy szolgáltatásaikat jogszerűen nyújthassák. A Bizottság néhány példával is szemléltette a PET-ek lehetséges típusait.[23] Elsőként az adatokat automatikusan

[18] Jóri (2005): *i. m.,* 18–19.

[19] Társaság a Szabadságjogokért: PET Portál és Blog – Az első magyar fórum a privát szférát erősítő technológiákról. http://tasz.hu/adatvedelem/33 (2014. 02. 27.).

[20] Goldberg, Ian: *Privacy-enhancing technologies for the Internet, II: Five years later.* In Dingledine, R.– Syverson P. (Ed.): *Privacy Enhancing Technologies. Second International Workshop, PET 2002 San Francisco, CA, USA, April 14–15, 2002 Revised Papers.* Springer-Verlag, 2002, 1. http://freehaven.net/anonbib/papers/petfive.pdf (2014. 01. 29.).

[21] Társaság a Szabadságjogokért, uott.

[22] Európai Bizottság: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak az adatvédelemnek a magánélet védelmét erősítő technológiák által történő ösztönzéséről. COM(2007) 228 végleges, Brüsszel, 2007. 3. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:HU:PDF (2014. 03. 19.)

[23] Európai Bizottság (2007): *i. m.,* 4.

anonimizáló alkalmazásokat említette, majd a titkosítási eszközöket, harmadikként a cookie-letiltó alkalmazásokat, végül a „Platform for Privacy Preferences" (P3P) megoldást nevesíti.

A brit információs biztos ajánlásokat is megfogalmazott az alkalmazási területekre. Ilyenek például a biometrikus adatok olyan titkosított tárolása, amelyből nem állítható vissza az eredeti adat (például azok anonimizálásával); valamint az érintettek azon lehetősége, hogy a saját személyes adataikat egy titkosított internetkapcsolaton keresztül ellenőrizzék és frissítsék; valamint az adatok olyan „megcímkézése", amellyel az adatvédelmi felhasználási feltételek közvetlenül az adathoz kapcsolva elérhetőek.[24]

Jan Paul Kolter szintén a PET-ek alkalmazásának gyakorlati oldaláról közelít azok céljának meghatározásakor: szerinte a magánélet védelmében minden felhasználónak szüksége van az adatvédelmi szabályok értelmezésére is, ezért a PET-ek a jogszabályok gyakorlati alkalmazásában segítséget nyújtó technikai megoldások: *„average Internet users rely on technical means that protect personal user information and facilitate a more informative decision about personal data disclosures".*[25]

Székely Iván négy alapvető elvárást fogalmaz meg a privát szférát védő megoldások céljaként: az anonimitást, a pszeudoanonimitást, a megfigyelhetetlenséget és az összeköthetetlenséget. Aktív felhasználók esetében ezek konjunktív teljesülése a cél, míg passzív felhasználók mint érintettek esetében csak az első két elvárásnak kell érvényre jutnia.

Az anonimitás lényege, hogy *„az adatokat, illetve az adatok kezelésével járó* eseményeket*, cselekvéseket nem tudjuk egy meghatározott személlyel kapcsolatba hozni*".

A pszeudoanonimitás jelentése, hogy *„van alanya az adatoknak, de az alany valós kilétét nem ismerjük; egy valós adatalanynak több fedőneve, profilja, virtuális személyisége is lehet".*

A megfigyelhetetlenség alatt azt értjük, hogy *„egy illetéktelen harmadik fél ne észlelhesse, hogy valaki egy távoli erőforrást használ, például nyílt hálózati kapcsolaton keresztül egy internetes folyóirat oldalait tölti le".*

Az összeköthetetlenség pedig akkor áll fenn, ha *„az illetéktelen harmadik fél akár észlelheti is a távoli erőforrás valaki általi használatát, azonban nem tud kapcsolatot teremteni az aktuális használat és az ezt megelőző vagy követő használatok között. Az összeköthetetlenség tehát megakadályozza a felhasználók szokásainak megfigyelését, profilírozását."*[26]

Az alkalmazási területek kapcsán meg kell említeni Goldberg tipológiáját is, aki a PET alkalmazási lehetőségeit vizsgálva három nagy csoportot különböztetett meg:

Az első csoportba tartoznak azok a PET-ek, amelyek a felhasználók anonimitását biztosítják az interneten történő kommunikáció során, elrejtik személyes adatainkat

[24] UK Information Commissioner's Office: *Data Protection Technical Guidance Note: Privacy enhancing technologies (PETs). V2.0*, 2007, 2. http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_ENHANCING_TECHNOLOGIES_V2.ashx (2014. 03. 19.).

[25] Kolter, Jan Paul: *User-Centric Privacy. A Usable and Provider-Independent Privacy Infrastructure.* University of Regensburg, 2009, 2. http://www.ics.uci.edu/~kobsa/phds/kolter.pdf (2014. 03. 19.).

[26] Székely: *i. m.,* 25.

a kommunikáció más résztvevői elől.[27] Ilyenek például az anonim e-mail-küldést lehetővé tevő „remailer"-ek, az egyéb anonimitást és pszeudoanonimitást biztosító rendszerek. Itt említhető az ún. Tor-projekt, amelynek célja, hogy az IP-címek védelmét biztosítva a hagyományos internettől részben független hálózat jöjjön létre, amely a létező infrastruktúrát és megoldásokat használja fel annak érdekében, hogy megakadályozza a hálózati forgalomba való beavatkozást, a cenzúra alkalmazását vagy a hálózat felhasználóinak azonosítását.

A második csoportba tartoznak az olyan privát szférát erősítő technológiák, amelyek az online kommunikáció során átvitt tartalmat védik, elsősorban valamilyen titkosítási megoldással.[28]

Végül a szerző említ néhány „egyéb online környezetben alkalmazott privát szférát védő megoldást", mint a biztonságos online fizetési eszközök, az adathalászat vagy a cenzúrával szembeni eszközök.[29]

Meg kell jegyezni, hogy a PET-megoldások használata korántsem tömeges. A lassú elterjedés okai[30] között meg kell említeni, hogy a PET-ek használatához szükséges informatikai, technológiai ismeretek az átlagfelhasználóknál többnyire hiányoznak,[31] illetve problémát jelenthet az is, hogy általában nincs kézzelfogható eredménye a privát szférát erősítő technológiák alkalmazásának. Ezért alacsony azok népszerűsége, hiszen kevésbé tudatosul egy átlagos felhasználóban, ha visszaéltek személyes adataival, mintha a fizikai világban érné kár.[32] Ezeken a PET-megoldások előnyeinek népszerűsítésével, a felhasználóbarát kialakítással és a könnyű telepíthetőséggel lehetne segíteni.[33]

Ugyanakkor Székely felhívja a figyelmet arra is, hogy az adatkezelők üzleti érdekei is a PET-ek alkalmazása ellen szólnak, és akár a terjedésüket akadályozó lobbitevékenységtől sem riadnak vissza, mivel a személyes adatoknak az adatalanyok tudta és beleeggyezése nélküli felhasználása, elemzése, értékesítése komoly anyagi előnyt jelent számukra.[34]

2. Kísérlet egy új szemlélet elterjesztésére: a Privacy by Design elv jelentősége

A Privacy by Design, azaz a beépített adatvédelem fogalma az 1960-as években az építészetben jelent meg – az informatika világában csak az 1990-es évek közepe

[27] Goldberg, Ian: *Privacy-enhancing technologies for the Internet III: Ten Years Later.* 2007, 2–6. https://www.cs.drexel.edu/~greenie/privacy/pet3.pdf (2014. 03. 19.).

[28] Gyakran alkalmazzák ezeket a felek anonimizálására szolgáló megoldásokkal együttesen. Goldberg (2007): *i. m.,* 7–8.

[29] Goldberg (2007): *i. m.,* 8–10.

[30] E témakörről l. részletesen Kiss Attila: A privátszférát erősítő technológiák. *Infokommunikáció és jog*, 2013/3.

[31] Kolter: *i. m.,* 2.

[32] Thiesse, Frederic: RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems*, 2007/2, 226.

[33] Goldberg 2007, *i. m.,* 10–11.

[34] Székely: *i. m.,* 32.

óta használják a kifejezést.[35] Az elv kidolgozása és elterjesztése – bár egyes elemeiben számtalan szerzőnél megjelent – kétségkívül Ann Cavoukian munkásságának köszönhető, aki a 90-es évektől foglalkozik e kérdéskörrel. Meg kell jegyezni, hogy a szakirodalom először egyértelműen a privát szférát erősítő technológiákkal foglalkozott, a beépített adatvédelem elve a PET-eszközökkel kapcsolatos elméletek továbbgondolásaként, elvi szintre emeléseként jelent meg.

Ann Cavoukian szerint a Privacy by Design lényegében egy filozófia, egy megközelítési mód, amely alapján a magánszféra-védelem szempontjait integrálni kell a különböző technológiák követelményrendszerébe (specifikációjába), azaz az adatvédelmi szabályozás elveit be kell építeni az adatkezelési technológiákba mind a tervezés, mind a működtetés során. A Privacy by Design elv abból indul ki, hogy az informatikai infrastruktúra nagymértékben meghatározza az adatkezelő tényleges cselekvési szabadságát és lehetőségeit. Az elv ugyan eredetileg kifejezetten az infokommunikációs technológia kapcsán jelent meg, később azonban ez kiterjedt az üzleti folyamatok, sőt (visszatérve az építészeti gyökerekhez) a fizikai tervezés területére is.[36] Megjegyezzük, hogy az európai szabályozási tervekbe a beépített adatvédelem elve már kifejezetten e módosult hatókörrel került be: a követelményt nemcsak a technológia kialakítása, de általában az adatkezelési folyamatok megtervezése során is figyelembe kell venni. A gyakorlatban persze e kettő között igen szoros az összefüggés.

A Privacy by Design részletszabályainak kidolgozása alapvetően szintén Cavoukiannak köszönhető. Az általa megalkotott hét alapelv több mint 30 nyelven érhető el, köztük magyarul is.[37]

1. *Reakció helyett proaktivitás: utólagos orvoslás helyett megelőzés.* Fontos kiindulópont, hogy előre számolni kell a személyek magánéletébe beavatkozó eseményekkel, és meg kell akadályozni ezek bekövetkezését. Azaz a káros hatásokat nem utólag kell enyhíteni, hanem meg kell előzni.

2. *Alapértelmezett adatvédelem.* Lényeges momentum, hogy automatikus beállításokkal (úgy, hogy az egyénnek ezért semmilyen külön lépést nem kell tennie) kell maximális védelmet biztosítani a magánszféra számára számítástechnikai környezetben vagy üzleti felhasználás során.

3. *Tervezés során beépített adatvédelem.* A Privacy by Design elv központi elemét adja az a követelmény, hogy a privacyvédelem szempontjait nem utólagos kiegészítésként, hanem már a tervezéstől kezdve figyelembe kell venni, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy a funkcionalitást korlátozná.

[35] Davies, Simon: *Why Privacy by Design is the next crucial step for privacy protection – A discussion paper*, 2010. http://www.i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf (2014. 03. 19.).

[36] Cavoukian, Ann: *Privacy by Design. …Take the challenge.* Information and Privacy Commissioner of Ontario, 2009, 3. http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf (2014. 03. 20.).

[37] Cavoukian, Ann: *Privacy by Design. A hét alapelv* (fordította Péterfalvi Attila és Sziklay Júlia). Ontario (Canada) információs és adatvédelmi biztosa, 2013. http://www.privacybydesign.ca/content/uploads/2013/03/7foundationalprinciples-hungarian.pdf (2013. 08. 11.).

4. *Teljes működőképesség.* A Privacy by Design elvének alkalmazása integrálja az összes jogos érdeket és célt úgy, hogy a veszteségek és a profit ne csak kiegyenlítsék egymást, hanem a végeredmény pozitív mérleggel záruljon.

5. *Teljes életciklusra kiterjedő védelem.* Ha a Privacy by Design már az adatgyűjtés megkezdését megelőzően érvényesül, a hatékony biztonsági előírások az adatkezelés teljes ciklusát átfogják a kezdettől a végig. Az elv alkalmazása tehát elősegíti egy információ életútjának megfelelő kezelését a keletkezésétől a megszűnéséig.

6. *Láthatóság és átláthatóság.* A Privacy by Design elv az adatkezelés valamennyi résztvevőjét az alkalmazott technológiától vagy üzleti megoldástól függetlenül arra sarkallja, hogy a megígért és kinyilvánított céloknak megfelelően járjon el (melyet független értékelésnek is alávethet). Az adatkezelési műveletek így a szolgáltató és a felhasználó számára is átláthatóak.

7. *A felhasználó magánszférájának tisztelete.* A Privacy by Design elve az adatkezelőtől egyértelműen azt követeli meg, hogy az érintett adatvédelmi érdekeit tartsa a legfontosabbnak, szigorú adatvédelmi előírások, megfelelő jelzések és felhasználóbarát megoldások használatával.[38]

Egyes kutatók szerint ezek az elvek jól átültethetőek a gyakorlatba is, mivel a megfogalmazott elvek többsége a jogkövető adatkezelők számára szinte magától értetődő.[39] Álláspontunk szerint azonban a gyakorlati alkalmazás jelentős nehézséget okoz, mivel a megfogalmazott elvek sokkal inkább egy szemléletet, hozzáállást tükröznek, mintsem olyan normatív követelményrendszert, amelynek betartása vagy be nem tartása könnyedén megállapítható.[40] A beépített és alapértelmezett adatvédelem elvének jogszabályi megjelenése az új európai adatvédelmi keretrendszerben várhatóan számos konkrét jogalkalmazási nehézséget vet majd fel.

3. Technológia és a jog találkozása

3.1. Az EU adatvédelmi irányelvének szabályai

Az adatvédelem szabályozása kapcsán a rendszerek biztonságával, adatvédelem-barát kialakításával kapcsolatos legelső általános követelmények már az EU 1995-ös irányelvében[41] megjelentek. „Az adatfeldolgozás biztonsága" alcímet viselő 17. cikke szerint:

(1) „A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyil-

[38] Cavoukian (2013): *i. m.,* 2.

[39] Davies: *i. m.,* 7.

[40] Máshol Davies maga is jelzi, hogy a beépített adatvédelem jelenleg inkább egy koncepció, mintsem egy technika, amelynek sem standardjai, sem mérési módszertana (benchmark) nincs. Ugyanakkor az adatvédelmi szabályozástól nem idegenek az ilyen megoldások, az irányelv adatbiztonságra vonatkozó hatályos rendelkezéseinek jellege is hasonló.

[41] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

vánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen.

Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének."

Az első bekezdés lehetővé teszi az adatkezelők számára, hogy eldöntsék, mely szervezési vagy műszaki megoldás alkalmazásával kívánnak eleget tenni az adatbiztonság követelményének. Tehát jogszerűen járnak el akkor is, ha csak belső szabályzatban rögzítik a megfelelő adatkezelési gyakorlatot, amely alapján eljárva folytatnak személyesadat-kezelést. Nyilvánvaló, hogy nem feltétlenül zajlik elektronikus környezetben minden adatkezelés, ezért ha a jogalkotó előírná a jelentősen nagyobb hatékonysággal működő technikai-műszaki megoldások alkalmazásának kötelezettségét, akkor több gyakori adatkezelési műveletet nem lehetne jogszerűen elvégezni. De mindenképpen szükséges néhány szervezési szabály rögzítése, például egy adatkezelési és adatbiztonsági szabályzat formájában.

Az informatikai biztonság jogi szabályozása kapcsán szakadék tapasztalható a jogalkotás és jogalkalmazás (jogászok), valamint az intézkedések végrehajtói (informatikusok) között.[42] Ennek oka, hogy a jogi követelmények mögötti technikai tartalom nem ismerhető fel könnyen, és ez nehezíti a PET-ekre vonatkozó szabályozás megalkotását. A követelmények felületesek (aminek fő oka a technológiafüggetlenség), a felületesség ugyanakkor rendkívüli módon megnehezíti a jogalkalmazást.[43]

Az irányelv összességében nem segítette elő kifejezetten a magánszférát védő megoldások terjedését. A brit információs biztos megrendelésére készült 2009-es tanulmány szerint ördögi kör alakult ki, amely megakadályozza a privát szférát erősítő technológiák elterjedését. A vállalkozások nem érzik szükségesnek a PET-ek telepítését, mert a jogalkotó nem várja el azok alkalmazását. A jogalkotó nem írja elő a megoldások alkalmazását, mivel nem látnak olyan, megfelelő mennyiségű megoldást az alkalmazások piacán, amely egy ilyen előírást követő hetekben a kialakuló keresletet el tudná látni. A megoldások készítői viszont nem fejlesztenek új technikákat, mivel a vállalkozásoknak azokra nincs igénye, nem kötelesek alkalmazni őket. A jogalkotó ezért az adatkezelőkkel szemben nem ír elő olyan szigorú következményeket arra az esetre, ha nem alkalmaznának ilyen műszaki megoldásokat.[44]

Jelentős elvi-filozófiai előrelépés volt a német Teledienstendatenschutzgesetz (TDDSG)[45] rendelkezése, amely már 1997-ben tartalmazta azt az – adattakarékos-

[42] Szádeczky Tamás: *The Role of the Technology. Auditing and Certification in the Field of Data Security.* In Szőke Gergely László (szerk.): *Privacy In The Workplace. Data Protection Law and Self-Regulation in Germany and Hungary*. Budapest, HVG-ORAC, 2012, 326.

[43] Reidenberg, Joel. R.: Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*, 1998/3, 584.

[44] Robinson, Neil–Graux, Hans–Botterman, Maartan–Valeri, Lorenzo: *Review of the European Data Protection Directive*. RAND Corporation, 2009, 38. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf (2014. 03. 20.).

[45] Gesetz über den Datenschutz bei Telediensten (TDDSG) 1997 I 1871, 3. §.

ságnak nevezett – elvet, amely szerint a *„távszolgáltatást nyújtónak olyan technikai eszközöket kell használnia, amelyek működtetése nem jár személyes adatok kezelésével, illetve a lehető legkevesebb személyes adat kezelésével jár, sőt e szempontokat már az eszközök tervezésekor is figyelembe kell venni”.* A törvényszöveg rendelkezése, amely szerint az adattakarékosság szempontját a tervezés során is figyelembe kell venni, mindenesetre egybecseng a beépített adatvédelem legfontosabb jellemzőjével, a proaktivitás követelményével. Ez a rendelkezés később ugyan bekerült a német szövetségi adatvédelmi törvénybe[46] is,[47] de Európa-szerte egyelőre nem terjedt el.[48]

3.2. Az adatvédelmi reform eredményei

A fenti elemzésre tekintettel véleményünk szerint az európai uniós jogalkotás komoly kihívás előtt áll abban a tekintetben (is), hogy megfelelő hatékonysággal és szigorral érvényre juttassa a beépített adatvédelem elvét és támogassa a privát szférát erősítő technológiák elterjesztését.

A privát szférát erősítő technológiákkal foglalkozó 2007-es közleményében az Európai Bizottság így fogalmaz: *„A Bizottság úgy véli, hogy a magánélet védelmét erősítő technológiákat fejleszteni kell és szélesebb körben kell alkalmazni,* […] *a magánélet védelmét erősítő technológiák javítanák a magánélet védelmét és elősegítenék az adatvédelmi jogszabályoknak való megfelelést. A magánélet védelmét erősítő technológiák alkalmazása kiegészítené a meglévő jogi keretet és végrehajtási mechanizmusokat.”*[49] A adatvédelmi reform kapcsán több szakértő kiemeli, hogy a privát szférát erősítő megoldások használatát nemcsak a felhasználók, de az adatkezelők oldalán is népszerűsíteni kell, segíteni azok beépítését a jelenlegi gyakorlatukba.[50] Az állami intézmények az élen járhatnának a privát szférát erősítő megoldások alkalmazásában, például a P3P technológia bevezetésével, ezzel is példát mutatva más adatkezelőknek. Ezzel ugyanakkor ösztönöznék a technológiák fejlesztését is, hiszen jelentős kereslet alakulna ki a fizetős és ingyenes megoldásokra is.[51]

A reform során a Privacy by Design elve is hangsúlyosan megjelent. A különböző társadalmi konzultációk eredményét összegző dokumentum szerint a részt vevő

[46] Bundesdatenschutzgesetz (BDSG), 3. §.

[47] Jóri (2005): *i. m.,* 65.

[48] Magyarországon az adattakarékosság elve szektorális szabályként már 2004-ben megjelent az elektronikus kereskedelmi törvényben [l. az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, 13/A. § (3) bekezdését].

[49] Európai Bizottság (2007): *i. m.,* 4.

[50] Irion, Kristina–Luchetta, Giacomo: *Online personal data processing and EU data protection reform. Report of the CEPS Digital Forum.* In *Regulatory Policy, CEPS Task Force Reports*. Brussels, Centre for European Policy Studies, 2013, 63.
http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform (2013. 06. 27.).

[51] Bennett, Steven C.: Government options for encouraging use of online privacy-enhancing technologies, *The Privacy Advisor Newsletter,* 2011/2, 2. http://www.jonesday.com/files/Publication/5dd20c2d-d714-47cb-92b3-3112ff38307f/Presentation/PublicationAttachment/b74ca563-9b20-49d4-b3bc-3e2270888348/advisor03_11_Govt.pdf (2013. 06. 29.).

szervezetek jelentős része kifejezetten felhívta a Bizottság figyelmét a beépített adatvédelem mint alapelv rendkívüli reformáló erejére is, és kifejtették, hogy szívesen látnák a rendeletben ezt az elvet mint technikai és szervezeti óvintézkedést a személyes adatok véletlenszerű vagy jogszerűtlen megsemmisítése, elvesztése, módosítása, nyilvánosságra hozatala, vagy bármely más jogszerűtlenül megvalósuló kezelése ellen.

A reformfolyamat 2012 januárjában meghatározó állomáshoz jutott: az Európai Bizottság ekkor tette közzé az európai adatvédelmi irányelv módosításával kapcsolatos koncepcióját, illetve rendelettervezetének szövegtervezetét.[52]

A Rendelettervezetben a „beépített és alapértelmezett adatvédelem" két általános kötelezettséget jelent az adatkezelő számára. Eszerint – az eredeti 2012-es szövegjavaslat alapján – *„az adatkezelő – a technika állására és végrehajtás költségeire tekintettel – mind az adatkezelés módjának meghatározása, mind az adatkezelés során megfelelő technikai és szervezési intézkedéseket hajt végre oly módon, hogy az adatkezelés megfeleljen e rendelet követelményeinek, és biztosítsa az érintettek jogainak védelmét".*[53] Az Európai Parlament illetékes bizottsága[54] által jóváhagyott, és az Európai Parlament plenáris ülésén is nagy többséggel elfogadott szövegjavaslat[55] pontosítja és kiegészíti e követelményeket. A módosító javaslat szerint az intézkedéseket a jelenlegi technikai tudás, nemzetközi legjobb gyakorlat és az adatkezelés kockázata alapján kell megtenni, és az elvet az adatkezelés teljes életciklusa során alkalmazni kell. A javaslat kifejezetten utal arra, hogy a beépített adatvédelem elvének alkalmazása során figyelembe kell venni az esetleges adatvédelmi hatásvizsgálat eredményeit is.[56]

Emellett az adatkezelőnek – a Privacy by Default elv jegyében *„olyan mechanizmusokat kell végrehajtania, amelyek alapértelmezett módon biztosítják azt, hogy kizárólag az adatkezelés egyes konkrét* céljaihoz *szükséges személyes adatok kerülnek kezelésre, és különösen azt, hogy az adatgyűjtés vagy -tárolás* [a LIBE Javaslat alapján emellett az adattovábbítás] *során az adatok mennyisége és az adattárolási időtartam tekintetében sem lépik túl az e célokhoz szükséges legkisebb mértéket. Ezeknek a mechanizmusoknak különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezett módon ne váljanak határozatlan számú egyén számára hozzáférhetővé."*[57]

---

[52] A rendelet szövegtervezetét, valamint az eljáráshoz kapcsolódó dokumentumokat lásd: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011%28COD%29#documentGateway (2014. 03. 19.).

[53] Rendelettervezet, 23. cikk (1).

[54] Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottsága (LIBE).

[55] Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)], Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN (2013. 12. 10.), a továbbiakban LIBE Javaslat.

[56] LIBE Javaslat, 23. cikk (1).

[57] Rendelettervezet, 23. cikk (2).

A Rendelettervezet szövegében ugyanakkor kifejezetten PET-re vonatkozó rendelkezések nincsenek, a megoldásokat az indokolásként funkcionáló preambulum csupán egyszer említi. Több tanulmány is kritikával illette ezért a technológiai megoldásokra vonatkozó rész szövegét. Irion és Luchetta kiemelik, hogy az adatvédelmi szabványok és a PET-ek alkalmazása kötelezővé tételének hangsúlyos elemként kellene megjelennie a köztes szoftverek, az alkalmazás-középrétegek (middleware) szabályozásában, elsősorban technológiasemleges előírások formájában.[58] További hiányosságot jelent, hogy a jelenlegi tervezet elsősorban az adatkezelők és adatfeldolgozók oldaláról közelíti meg a PET-ek szabályozásának problémáját,[59] de nem nyújt támogatást ahhoz, hogy a 2007-es bizottsági koncepciónak megfelelően a technológia a felhasználók szélesebb köréhez juthasson el, több magánszemély védje ezek segítségével a magánszféráját.[60]

Álláspontunk szerint a tervezett szabályozás alapvetően helyes irányt követ. A beépített és alapértelmezett adatvédelemnek valóban elvi követelményként kell megjelennie, csakúgy, mint az adattakarékosság elvének. A privát szférát védő technológiák az ezen elveknek való megfelelést szolgálják, és olyan konkrét eszközöket jelentenek, amelyek támogatása jogszabályi szinten – épp a technológiasemlegességre tekintettel – csak általános megfogalmazással lehetséges, akkor is, ha ez a gyakorlati alkalmazást nehezíti. Kívánatos ugyanakkor, hogy az adatvédelmi hatóságok egyedi, például épp a Privacy by Design elvét konkrét ügyben értelmező döntései nyomán kialakuló joggyakorlat, önszabályozó mechanizmusok (magatartási kódexek, szabványok), és az adatkezelők belső szabályai konkretizálják e szabályokat, és akár előírják konkrét PET-alkalmazások használatát.

4. Következtetések

A tanulmány során áttekintettük, hogy miként jelenik meg a technológia szabályozószerepe a személyes adatok védelme területén. A privát szférát erősítő technológiáknak komoly szerepe lehet abban, hogy segítsék az adatvédelmi szabályok gyakorlati megvalósítását, ugyanakkor terjedésüket számos tényező hátráltatja – részben erre tekintettel e technológiák jogszabályok általi támogatását többen szorgalmazzák. A jogszabályi támogatás véleményünk szerint a beépített adatvédelem elvén keresztül valósulhat meg, a Privacy by Design megközelítés ugyanis annak biztosítására tesz kísérletet, hogy a technológia és jog, mint két szabályozórendszer, ne kioltsa, hanem erősítse egymást, és egyértelműen a technológiát állítsa a – társadalmi elvárásokat végső soron kötelező normaként megjelenítő – jogi szabályozás szolgálatába, megtartva így a jogi szabályozás elsőbbségét. A privát szférát erősítő technológiák e célkitűzések megvalósításának első számú eszközei lehetnek, amely azonban álláspontunk szerint önmagában nem igényel külön jogszabályi

[58] Irion–Luchetta: *i. m.,* 80.
[59] Irion–Luchetta: *i. m.,* 74.
[60] Irion–Luchetta: *i. m.,* 70.

szintű szabályozást – az adott adatkezelések során betöltött konkrét szerepüket az adatvédelmi joggyakorlat, önszabályozó mechanizmusok, illetve az adatkezelők belső szabályai jelölhetik ki.

Abstract

The interaction between technology and data protection is quite well-known and widely accepted in the legal literature concerning privacy protection. This essay tries to sum up the efforts to line up the technology itself to defend one's privacy, often threated by technological development. The essay first shows the relevance of the Privacy Enhancing Technologies (PETs), and the basic concept of the Privacy by Design principle, and then analyses both the current and the proposed European legal regulation focusing on these issues.