

TECHNOLÓGIAI DETERMINIZMUS ÉS JOGI SZABÁLYOZÁS, KÜLÖNÖS TEKINTETTEL AZ ADATVÉDELMI JOG FEJLŐDÉSÉRE¹

A műszaki-technológiai fejlődés folyamatos szabályozási kihívást jelent. A jogi szabályozás a technológiai fejlődés azon társadalmi következményeinek utólagos leképeződése, amelyek ösztársadalmi, politikai jellegű döntéseket indokolnak. Jelen tanulmány célja a technológiai fejlődés és a jogi szabályozás közötti kölcsönhatások elemzése a kommunikációs eszközök területén. A tanulmányban vizsgáljuk azokat a szabályozási helyzeteket, amikor a kommunikációs technológiák a szabályozás tárgyává válnak. Ugyanakkor e technológiák a szabályozási célok megvalósításában is felhasználhatók, találunk példákat a technológia szabályozási eszközként való alkalmazására. Az adatvédelem mint a technológiai fejlődésre különösen érzékeny szabályozási terület mindkét esetre kínál aktuális példákat, a tanulmány második fele ezeket veszi számba.

• • • • •

1. BEVEZETÉS

A műszaki–technológiai fejlődés folyamatos szabályozási kihívást jelent. A jogi szabályozás a technológiai fejlődés azon társadalmi következményeinek utólagos leképeződése, amelyek ösztársadalmi, politikai jellegű döntéseket indokolnak. Ily módon a jogi szabályozás szükségszerűen „fut” a technológiai fejlődés után, nem pusztán abban az értelemben, hogy a változásokra mindig csak utólag reagálhat – ami nem a jogi szabályozás gyengeségét, hanem egyszerűen annak társadalmi szerepét mutatja –, de abban az értelemben is, hogy a jogalkotás napirendjét a technológiai változások kényszerítően meghatározzák. A technológiai, illetve az ahhoz kapcsolódó társadalmi változásokra a jogi szabályozásnak számos esetben *muszáj* reagálnia, keretet szabnia a létrejövő vagy megváltozó társadalmi viszonyoknak. Így válik a technológia a jogi szabályozást ösztönző, sőt bizonyos értelemben determináló tényezővé: azon keresztül a társadalmi viszonyokat folyamatosan hozzá kell igazítani a műszaki-technológiai környezethez. Ez természetesen nem jelenti sem azt, hogy a technológia lenne

¹ Az azonos című, a NEMESLAKI András (szerk.): *E-közszolgálatfejlesztés. Elméleti alapok és tudományos kutatási módszerek* című kötetben megjelent tanulmány rövidített változata.

az egyetlen „determináló” erő a jogalkotási folyamatban, sem azt, hogy a jogi keretek megfogalmazásában, az érintett társadalmi viszonyok alakításában ne lenne mozgásteret a szabályozónak. Arra azonban feltétlenül okot ad, hogy vizsgáljuk a jogi szabályozás és a technológiai fejlődés közötti kölcsönhatásokat.

A technológiai determinizmus legismertebb képviselője *Marshall McLuhan*, aki a társadalom minden változását lényegében egyetlen tényezőre, a kommunikációs eszközök és lehetőségek változására vezette vissza. Annak ellenre, hogy a társadalmi folyamatok ilyen értelmezése nyilvánvalóan leegyszerűsítő, a kommunikációs eszközök fejlődése és a társadalmi átalakulások között nagyon is könnyű párhuzamosságokat találni. Jelen tanulmány célja a technológiai fejlődés és a jogi szabályozás közötti kölcsönhatások elemzése a kommunikációs eszközök területén. A kommunikáció szabályozásában lépten-nyomon olyan kifejezésekbe botlunk, mint a „frekvenciaszűkösség”, a „szűk keresztmetszetek” vagy éppen a hálózati semlegesség. Ez arra utal, hogy a szabályozó is gyakran a technológiai kényszerek eredményeként tünteti fel saját döntéseit, különösen akkor, ha ezzel egyébként szélesíteni képes a szabályozói mozgásterét.

1.1. A kommunikációs technológia mint a szabályozás tárgya

A technológia abban az esetben válik legnyilvánvalóbban a szabályozás tárgyává, amikor a szabályozás kifejezetten az adott technológiát érintő műszaki, minőségi követelményeket határoz meg.

Ennek legközvetlenebb esete a szabványosítás. A szabvány – a vonatkozó magyar jogszabály meghatározásában² – elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételt alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyeknek az alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb. A szabványosítás alapvetően nem állami feladat, az állam a megfelelő felkészültségű szervezetek kijelölésében és felügyeletében vesz részt. A szabványosítás nemzetközi és európai szinten is megvalósulhat, és egyes megoldások gyakran külön eljárás nélkül válnak de facto szabvánnyá.

Közvetettebb módon szabályozza a technológiát az a megoldás, amely nem valamely konkrét technológia vagy szabvány alkalmazását írja elő, hanem meghatározza azokat a követelményeket, illetve használati jellemzőket, amelyeket bármely alkalmazott technológiának teljesítenie kell. Ez a technológiasemleges megoldás jellemzi például a távközlési hálózatokkal kapcsolatos biztonsági követelmények megfogalmazását. Az elektronikus hírközlésről szóló törvény azt a nagyvonalú kötelezettséget támasztja a távközlési szolgáltatókkal szemben, hogy az általuk meghozott műszaki és szervezési intézkedéseknek a szolgáltatás nyújtásával kapcsolatban jelentkező kockázatoknak megfelelő biztonsági szintet kell nyújtaniuk.³ Sem a

2 A nemzeti szabványosításról szóló, 1995. évi XXVIII. törvény.

3 2013. évi C. törvény az elektronikus hírközlésről, 156. §.

törvény, sem más jogszabály nem határozza meg közelebbről a megfelelő biztonsági szint jellemzőit, a rendelkezés megsértéséért azonban a szolgáltató felelősséggel tartozik.

Hasonló szabályozási módszert követ az elektronikus dokumentumok hitelességét biztosító elektronikus aláírás szabályozása: a jogalkotó törvényben határozza meg azokat a kritériumokat, amelyek teljesülésének esetén az elektronikus aláírás meghatározott joghatások kiváltására – írásba foglalt, illetve meghatározott bizonyító erejű okirat létrehozására – alkalmas.⁴ Mivel azonban a szabályozás olyan műszaki környezetben jött létre, amelyben gyakorlatilag egyetlen – a kétkulcsos kriptográfián alapuló – technológia biztosította a szabályozási követelményeket, mind a követelmények megfogalmazása, mind a szabályozás fogalomhasználata⁵ az adott technológiához igazodik.

1.2. A technológia mint a szabályozás eszköze

A technológia egyes esetekben közvetlen szabályozási eszközzé, a jogszabályok érvényesülésének közvetlen feltételévé válhat. E folyamat ismert példái a gyermekek védelmét szolgáló, a televíziós műsorterjesztésben vagy az online tartalomterjesztésben használt szűrőrendszerek, amelyek a nem kívánt tartalom megjelölésével és szűrésével segítik e tartalmak elkerülését.⁶

A távközlés-szabályozás a személyes adatok védelmét is csak a megfelelő műszaki intézkedések biztosításával tartja megvalósíthatónak. A törvény szerint a szolgáltató csak úgy választhatja meg, és minden esetben úgy üzemeltetheti az elektronikus hírközlési szolgáltatás nyújtása során alkalmazott elektronikus hírközlő eszközöket, hogy biztosítani tudja: személyes adat kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez elengedhetetlenül szükséges.⁷ Ugyanez az előírás vonatkozik az online, elektronikus kereskedelmi szolgáltatások nyújtóira.⁸ E szabályozási megoldás a jogalkotó részéről annak fel- és beismerését igazolja, hogy a jogszabályok önmagukban képtelenek védelmet nyújtani a komplex kommunikációs rendszerek felhasználóinak. A jogszabályok érvényesíthetősége attól függ, hogy a rendszer alapjául szolgáló technológiák formálhatók-e a szabályozói igényeknek megfelelően. Ez a jogalkotó oldalán egyfajta kiszolgáltatottságot jelent, s ennek következtében saját mozgásterét kizárólag az infrastruktúra üzemeltetőivel való együttműködésben, kölcsönös függésben alakíthatja.

A technológia és a jogi szabályozás egymásrautaltságára a szerzői jogban is több példát találunk. Az interneten megjelenő, szerzői jogot sértő tartalmak eltávolítása azok fizikai elérhe-

4 Fokozott biztonságú elektronikus aláírás például az az elektronikus aláírás, amely *a)* alkalmas az aláíró azonosítására; *b)* egyedülállóan az aláíróhoz köthető; *c)* olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak; *d)* a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető (az elektronikus aláírásról szóló, 2001. évi XXXV. törvény 2. § 15.).

5 Lásd például aláírás-létrehozó és aláírás-ellenőrző adat, lenyomat.

6 POLYÁK Gábor: Hatalomleosztás. Nemzetközi önszabályozási kísérletek. In: *Médiakönyv 2002* (szerk.: ENYEDI NAGY Mihály-POLYÁK Gábor-dr. SARKADY Ildikó), Enamiké, Budapest, 2002, 475–487.

7 Az elektronikus hírközlésről szóló, 2003. évi C. törvény 154. § (4).

8 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló, 2001. évi CVIII. törvény 13/A. §.

tetlenné tételével valósítható meg, a tömeges szerzői jogi jogsértések ellen pedig a felhasználók internet-hozzáféréseinek korlátozásával védekezik a szabályozás.⁹ A digitális jogkezelő rendszerek¹⁰ a szerzői jogi törvény szerint a szerzői jog jogosultja által nem engedélyezett cselekmények megelőzésére vagy megakadályozására szolgáló eszközök, megoldások.¹¹ Beemelésük a jogi szabályozásba nemcsak azt a célt szolgálja, hogy ezzel a jogalkotó elismerje e rendszerek létjogosultságát, egyúttal a jogi eszközök hatékonyságának korlátozottságát. A szabályozás kifejezetten védelemben részesíti magát a digitális jogkezelő rendszert is: a műszaki intézkedés megkerülése önmagában is jogsértésének minősül, függetlenül az adott cselekmény szerzői jogi következményeitől. A jogalkotó ezzel kifejezetten ösztönzi e műszaki intézkedések alkalmazását – amelyeknek a célszerűségét a piac nem feltétlenül igazolta vissza –, jutalmazza a szerzői jogi jogosultak saját szellemi termékeiknek a védelmében tett erőfeszítéseit. Ez egyrészt annak beismerése, hogy a jog önmagában nem képes megoldani a szerzői jogi jogosultak problémáit, másrészt egyfajta felelősségmegosztást is mutat, jelezve az érintettek felé, hogy maguk is tegyék meg a szellemi javaik védelméhez szükséges lépéseket.

A jogalkotó tehát számos esetben támaszkodik a technológiai megoldásokra, és időnként kifejezetten elvárja az érintettektől a szabályozási célok megvalósítását szolgáló technológiák alkalmazását.

2. A TECHNOLÓGIA ÉS A SZABÁLYOZÁS KÖLCSÖNHATÁSA AZ ADATVÉDELEM TERÜLETÉN

2.1. A technológia mint a szabályozás eszköze és tárgya az adatvédelem területén

Több más jogterülethez hasonlóan az adatvédelem területén is hangsúlyosan megjelentek a technológiai megoldások mint a jogi védelem kiegészítői. Az ún. privát szférát erősítő technológiák (PETs)¹² alkalmazásának során a technológia tehát közvetlen szabályozó szerepet tölt be, amely azonban fokozatosan – eleinte elsősorban az adatbiztonságra vonatkozó szabályok, majd egy általános elv (egyelőre inkább célkitűzés), a beépített adatvédelem elve (Privacy by Design) megjelenésével – az adatvédelmi szabályozás tárgyává is vált. A továbbiakban e két jelenséget és azok egymáshoz való viszonyát elemezzük.

2.1.1. A privát szférát erősítő technológiák

A „Privacy Enhancing Technologies” kifejezést 1995-ben, a holland állam és az ontariói adatvédelmi biztos hivatalának közös projektjének során használták először. Noha azóta eltelt közel két évtized, nem csökkent az érdeklődés az egyén identitását, személyazonosságát

9 HAJDÚ Dóra: A fájlcsere elleni küzdelem egy lehetséges útja – Három a francia igazság? *Infokommunikáció és Jog*, 2011/3., 95–103.

10 GYENGE Anikó: Digitális jogkezelési rendszerek a szerzői jogban, *Infokommunikáció és Jog*, 2004/2., 50–56.

11 A szerzői jogról szóló, 1999. évi LXXVI. törvény 95. §.

12 Privacy Enhancing Technologies.

védő technikai és szervezeti megoldások fejlesztése iránt.¹³ Az adatszivárgások, visszaélési botrányok magas száma jól mutatja, hogy ismét komoly szerepet kaphat a technológiai megoldások alkalmazása az adatvédelem területén, önmagában a szabályozás, az önszabályozás és a jogalkalmazás sem tud elegendő védelmet nyújtani a felhasználók számára.¹⁴

A „Privacy Enhancing Technologies” az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneve.¹⁵ Egy ennél részletesebb meghatározás 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.¹⁶

A PET alkalmazásának alapvető célja, hogy ne csak az adatokat általában (mint az adatbiztonsági intézkedések), hanem az érintetteket is védjék a visszaélések ellen, elősegítve információs önrendelkezési joguk gyakorlását. A PET jellemzően anonimitást vagy pszeudoanonimitást biztosító alkalmazásokat, a közlés bizalmasságát biztosító titkosítási eszközöket, „cookie-letiltó” alkalmazásokat, biztonságos fizetési eszközöket stb. ölel fel.¹⁷

2.1.2. A Privacy by Design-elv jelentősége

A Privacy by Design-elv kidolgozása és elterjesztése – bár egyes elemeiben számtalan szerzőnél megjelent – kétségkívül Ann Cavoukian munkásságának köszönhető, aki a kilencvenes évektől tanulmányozza e kérdéskört. Az adatvédelmi szakirodalom először egyértelműen a privát szférát erősítő technológiákkal foglalkozott, a beépített adatvédelem elve a PET-eszközökkel kapcsolatos elméletek továbbgondolásaként, elvi szintre emeléseként jelent meg.¹⁸

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 kiterjedt az üzleti folyamatok, sőt (visszatérve az építészeti gyökerekhez) a fizikai tervezés

13 KISS Attila: A privátszférát erősítő technológiák. *Infokommunikáció és Jog*, 2013/3., 113–119.

14 SZÉKELY Iván: Privát szférát erősítő technológiák. *Információs Társadalom*, 2008/1., 20–34.

15 BURKERT, Herbert: Privacy-Enhancing Technologies: Typology, Critique, Vision. In.: AGRE, Philip E. – ROTENBERG, Marc (eds.): *Technology and Privacy: The New Landscape*. The MIT Press, 1998, 125–142.

16 BLARKOM, van, G. W. – BORKING, J. J. – OLK, J. G. E (ed.): *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*. College bescherming persoonsgegevens, 2003.

17 KISS Attila: A privátszférát erősítő technológiák. *Infokommunikáció és Jog*, 2013/3., 113–119.

18 BÖRÖCZ István – SZÖKE Gergely László: A beépített adatvédelem (Privacy by Design) elve. *Infokommunikáció és Jog*, 2013/3., 120–125.

területére is.¹⁹ Megjegyezzük, hogy a beépített adatvédelem elve már kifejezetten e módosult hatókörrel került be az európai szabályozási tervekbe: a követelményt nemcsak a technológia kialakítása, de általában az adatkezelési folyamatok megtervezése során 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 alapelv²⁰ több mint harminc nyelven érhető el, köztük magyarul is.

Álláspontunk szerint a Privacy by Design-elv gyakorlati alkalmazása jelentős nehézségeket okoz, mivel a megfogalmazott elvek sokkal inkább egy szemléletet, hozzáállást tükröznek, mintsem olyan normatív követelményrendszert, amelynek a betartása vagy be nem tartása könnyedén megállapítható. A beépített és alapértelmezett adatvédelem elvének jogszabályi megjelenése az új európai adatvédelmi keretrendszerben várhatóan számos konkrét jogalkalmazási nehézséget vet majd fel.

2.1.3. A technológia és a jog találkozása az európai adatvédelmi jogban

Az Európai Unió jogalkotása jelenleg komoly kihívás előtt áll a tekintetben (is), hogy az adatvédelmi reform során megfelelő hatékonysággal és szigorral érvényre juttassa a beépített adatvédelem elvét, és támogassa a privát szférát erősítő technológiák elterjesztését.

Az új európai adatvédelmi rendelet tervezetében²¹ végül a „beépített és alapértelmezett adatvédelem” „csak” mint két általános kötelezettség jelent meg. E szerint 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”. Az Európai Parlament által elfogadott LIBE-javaslat pontosítja és kiegészíti e követelményeket, e szerint az intézkedéseket a jelenlegi technikai tudás, a nemzetközi legjobb gyakorlat és az adatkezelés kockázata alapján kell megtenni, és az elvet az adatkezelés teljes életciklusa alatt alkalmazni kell. A javaslat kifejezetten utal arra, hogy a beépített adatvédelem elvének alkal-

19 CAVOUKIAN, Ann (2009): *Privacy by Design...* Take the challenge, Information and Privacy Commissioner of Ontario; www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf (A letöltés ideje: 2014. március 20.)

20 Ezek: 1. reakció helyett proaktivitás; 2. alapértelmezett adatvédelem; 3. tervezés során beépített adatvédelem; 4. teljes működőképesség biztosítása; 5. teljes életciklusra kiterjedő védelem; 6. láthatóság és átláthatóság; 7. a felhasználó magánszférájának tisztelete. A Privacy by Design részletes elemzését lásd Böröcz, Szőke, 2013.

21 Az adatvédelmi reform keretében a Bizottság 2012-ben kiadott új adatvédelmi rendelet elfogadására vonatkozó javaslatát az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottsága (LIBE Bizottság) alaposan átdolgozta, majd 2014. március 12-én az Európai Parlament plenáris ülése elfogadta. E cikkben a rendelettervezet e szövegverzióját használjuk: 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; www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN (2013.12.10.), a továbbiakban: rendelettervezet.

mazásakor figyelembe kell venni az esetleges adatvédelmi hatásvizsgálat eredményeit is.²² 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.”²³

A rendelettervezet szövegében ugyanakkor nincsenek kifejezetten a PET-re vonatkozó rendelkezések, a megoldásokat az indokolásként funkcionáló preambulum csupán egyszer említi. Néhány tanulmány kritikával illette ezért a technológiai megoldásokra vonatkozó rész szövegét. Irion és Luchetta kiemelik, hogy az adatvédelmi szabványok és a PET-ek alkalmazásának kötelezővé tétele hangsúlyos elemként kellene hogy megjelenjen a köztes szoftverek, a középrétegek (middleware) szabályozásában, elsősorban technológiasemleges előírások formájában. További hiányosságot jelent, hogy a jelenlegi tervezet elsősorban az adatkezelők és -feldolgozók oldaláról közelíti meg a PET-ek szabályozásának problémáját, de nem nyújt támogatást ahhoz, hogy a technológia a 2007-es bizottsági koncepciónak megfelelően a felhasználók szélesebb köréhez juthasson el, ezeknek a segítségével több magánszemély védje a magánszféráját.²⁴

Álláspontunk szerint azonban 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, amelyeknek a 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 – döntéseinek nyomán kialakuló joggyakorlat, önszabályozó mechanizmusok (magatartási kódexek, szabványok) és az adatkezelők belső szabályai konkretizálják e szabályokat, és akár előírják meghatározott PET-alkalmazások használatát.

22 Rendelettervezet, 23. cikk (1).

23 Rendelettervezet, 23. cikk (2).

24 IRION, Kristina – LUCHETTA, Giacomo (2013): Online personal data processing and EU data protection reform. Report of the CEPS Digital Forum. In: *Regulatory Policy*. CEPS Task Force Reports, Centre for European Policy Studies.