ACTA HUMANA • 2020/1. 67–81. • DOI: 10.32566/ah.2020.1.3

Csődöt mondott csodafegyver? A beépített adatvédelem hiányosságai

DELI GERGELY – MUHARI NÓRA

A 2018-tól alkalmazott Általános Adatvédelmi Rendelet (GDPR) új, az adatok hatékonyabb védelmének biztosítását szolgáló eszközként vezeti be egyebek mellett a privacy by design, azaz a beépített adatvédelem elvét. Ennek értelmében már a tervezési fázisban figyelembe kell venni a GDPR-ban foglalt követelményeket. Tanulmányunk alapállítása, hogy a privacy by design alapelve és a szofisztikált nagyvállalatok által gyakran alkalmazott, a fogyasztói választások tudatos befolyásolására irányuló, egyes esetekben gépi tanuláson alapuló döntéstervezés (choice architecture) között alapjogi sérelemmel járó konfliktus, illetve szabályozási űr állhat fenn. Úgy véljük, hogy a gépi tanulás a magánszférába való egyre látensebb és súlyosabb beavatkozást tehet lehetővé, úgy, hogy mindeközben a privacy by design előírásai nem sérülnek. Jelen tanulmányunkban megvizsgáljuk, hogy a döntéstervezéssel együttjáró fogyasztói manipuláció mikortól valósít már meg alapjogi (magánszféra) sérelmet. Végül javaslatot teszünk a privacy by design alapelvének bővítésére, amelynek segítségével a döntéstervezéssel együttjáró, már jogtalan befolyásolás is kezelhetőbbé válhat.

Kulcsszavak: GDPR, privacy by design, döntéstervezés, nudge, gépi tanulás, profilalkotás, buborékhatás, privacy by randomness, privacy by assistance

Perfect Imperfection? – Deficiences of GDPR's Privacy by Design

Pursuant to the principle 'privacy by design', the data controller must consider data protection aspects, and integrate appropriate measures both before and during data processing, to comply with the GDPR and protect the rights of data subjects. Although, as we presume, there might be a collision between this principle and the growingly popular psychological method of choice architecture. Taking advantage of the latter, more and more companies are using nudges to orientate users' behaviour towards choices of their own interests. This could be claimed legal, but in fact, most of them consciously rely on the indefinite wording of the regulation to verify their far from fair practices. This conflict of privacy by design and nudging draws attention to a regulatory gap, which makes possible the violation of fundamental rights, since privacy and the freedom of choice are likely to be disregarded. In this paper we examine the currently used and prevailing compliance mechanisms

on the market. Also, we seek to demonstrate how major companies can bend the definition of this fundamental principle, to disguise the usage of dark patterns and the abuse of privacy. Thereafter, we elaborate on the possible correlation of choice architecture and machine learning. In the last section we inspect which practices amount to the actual violence of fundamental rights, and we propose a possible advancement of privacy by design.

Keywords: GDPR, privacy by design, choice architecture, nudge, machine learning, profiling, bubble effect, privacy by randomness, privacy by assistance

Bevezetés

Ahogyan azt az Általános Adatvédelmi Rendelet, a GDPR[1] preambuluma is kiemeli, a gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét.[2] Azzal, hogy a hangsúly az elmúlt évtizedekben az ipari termelésről a szolgáltatásnyújtásra és az új tudás létrehozására tevődött át, az információk általános értéke, és azok felelős kezelésének jelentősége drámai mértékben megnőtt. Amellett, hogy e robbanásszerű technológiai fejlődés előnyeit élvezzük, fontos figyelmet szentelnünk arra is, hogy választásaink szabadságát és a személyes adataink feletti irányítást megőrizzük. Az adatvédelem napjainkban már nem pusztán egy jogi elvárás, hanem elengedhetetlen piaci követelmény és döntő tényező a bizalom a jogok és a szabadságok szempontjából jelenkorunk információs társadalmában.[3] Jelen tanulmányunkban a GDPR egyik fő, csodafegyvernek kikiáltott újítása, a *privacy by design* okozta lehetséges veszélyeket elemezzük és újszerű megoldási javaslatokat fogalmazunk meg.

A privacy by design

A GDPR célkitűzéseinek megvalósítása érdekében több alapelvet is meghatároz. Ezek közé tartozik a korábban uniós szabályban még nem nevesített, de a gyakorlatban már ismert *privacy by design*, azaz a beépített adatvédelem elve. A fogalmat Ann Cavoukian, egykori kanadai adatvédelmi biztos használta először az 1990-es években.[4] Azóta egyre nagyobb egyetértés mutatkozik abban, hogy a fejlesztés, a kreativitás és a versenyképesség is egyfajta „előre tervező gondolkodás" által valósíthatók meg a leghatékonyabban, ez pedig az adatvédelemre is igaz.[5] A *privacy by design* prospektív

1 The History of the General Data Protection Regulation.
2 (EU) 2016/679 európai parlamenti és a tanácsi rendelet, (6)–(7) bek.
3 Cavoukian é. n.
4 Buttarelli 2018, 4.
5 Cavoukian 2010.

alapgondolata szerint a jövő adatai védelmének biztosításához már nem lesz elegendő a keretszabályoknak való megfelelés elvárása. Az adatvédelem biztosításának alapbeállítássá, a technológia fejlesztésének nulladik lépésévé kell válnia. Kulcsfontosságú, hogy a felhasználók ezirányú védelmének garantálása a vállalatok prioritásainak, projekt-célkitűzéseinek, tervezési folyamatainak és műveleteinek integráns részévé váljon.[6] A GDPR 25. cikkének a beépített adatvédelemre vonatkozó bekezdése értelmében az adatkezelő a változó valószínűségű és súlyosságú kockázatok figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek hatékony megvalósítása, másrészt az adatvédelmi rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.[7] A normaszöveg hiteles magyar fordítása a következő:

„25. cikk (1) Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába."

A *privacy by design* három átfogó alkalmazási területre terjed ki. Ezek az informatikai rendszerek, az elszámoltatható üzleti gyakorlatok, illetve a fizikai kialakítás és hálózatba kötött infrastruktúra. Az elv célkitűzései az adatvédelem biztosítása, az egyén kontrollja saját személyes adatai felett, illetve a vállalkozásokkal szemben pozitív versenyhelyzet teremtése ezeken a területeken. Ann Cavoukian mindezek elérésére hét alapelvet határozott meg.[8]

Az első elv szerint az adatvédelem legyen „proaktív, nem reaktív; megelőző, nem javító". Már maga a *privacy by design* kifejezés is arra utal, hogy az ennek keretében megtett intézkedések célja az adatok védelmét veszélyeztető helyzetek megelőzése, nem pedig azok utólagos orvoslása. Az elv alkalmazója nem várja meg, míg egy adatvédelmi kockázat valós veszély formájában megtestesül, hanem előzetes lépéseket tesz ennek elkerülése érdekében. A következő elv az „adatvédelem mint alapbeállítás" elve. Ennek értelmében a személyes adatok minden informatikai rendszerben és üzleti gyakorlatban automatikusan védettek. Amennyiben ez az elv érvényesül, az egyén részéről nincs szükség aktív cselekvésre, adatai akkor is sértetlenek maradnak, hiszen azok védelme be van építve a rendszerbe, annak alapértelmezés szerinti részét képezi. A harmadik alapelv a „tervbe ágyazott adatvédelem", amelynek értelmében

6 Cavoukian 2010.
7 2016/679 európai parlamenti és tanácsi rendelet, 25. cikk (1)–(2) bek.
8 Cavoukian 2010.

az informatikai rendszereket és üzleti gyakorlatokat már eleve úgy hozzák létre, hogy struktúrájukban az adatvédelem egy nélkülözhetetlen elem az alapfunkciók működéséhez. A negyedik elv a „pozitív, nem negatív végösszeg". A beépített adatvédelem minden jogos érdeket és célt kölcsönösen előnyös módon igyekszik beilleszteni, ezáltal sem a felhasználó, sem a szolgáltató nem kényszerül kompromisszumra. Nem kíván meg olyan döntést, amellyel a fogyasztó például az adatvédelem és a szolgáltatás közötti választásra kényszerül, hanem megmutatja, hogy e kettő egyszerre is lehetséges. A következő elv az „élethosszig tartó védelem". A *privacy by design-t* már azelőtt beépítik, hogy a technológia bármilyen információval érintkezne, az így létrehozott védőháló pedig minden adat kezelésének elsőtől utolsó pillanatáig biztosítja azok sértetlenségét. Ezáltal garantált, hogy az adatokat megfelelően tárolják, majd a felhasználási folyamat végén szakszerűen megsemmisítik. A hatodik elv a „láthatóság és átláthatóság", azaz hogy minden üzleti gyakorlat és technológia működése során független megerősítésnek legyen kitéve. Minden folyamat megfigyelhető és megérthető mind a felhasználók, mind a szolgáltatók számára. Ann Cavoukian hetedik elve a „felhasználó-központúság". Ennek értelmében a *privacy by design-t* megvalósító tervezőknek és kezelőknek az egyén érdekeit mindenekfelett előnyben kell részesíteniük azáltal, hogy hatékony alapértelmezett adatvédelmi beállításokat, megfelelő tájékoztatást, továbbá felhasználóbarát alternatívákat kínálnak.[9]

Mindazonáltal, a *privacy by design* pontos jelentését a mai napig bizonytalanság övezi. A hét elv, illetve az alapgondolat és kontextusának részletes magyarázata ad némi támpontot, azonban a GDPR 25. cikkében szereplő, egyes alapvető fogalmak pontos meghatározása hiányzik. A „megfelelő intézkedések végrehajtása" kifejezést, de magát a „megfelelő" minősítést sem határozták meg. Ezek definícióit sem a rendelet egyéb szakaszaiban, sem azon kívül, egyéb jogszabályban nem találjuk meg. A problémát súlyosbítja, hogy az uniós szintű adatvédelmi szabályozás 2018 óta már nem irányelv formájú kötelezettség, hanem a tagállami módosításokat kizáró rendeletként hatályos. Ebből kifolyólag az implementáció során nincs lehetőség arra, hogy a nemzeti jogalkotó fórumok a szabályozást továbbértelmezzék, és esetlegesen pontosítsák annak tartalmát a kihirdető jogszabályban. Végeredményben a jogértelmezés a tagállami bíróságok feladatává válik. Megfelelő támpont vagy egzakt iránymutatás hiányában ez pedig a joggyakorlat széttartását eredményezheti. A 25. cikkel kapcsolatban ezért felvetődhetnek normavilágossági és jogbiztonsági problémák.

A brit információs biztos hivatalának (ICO) iránymutatása szerint például a GDPR-ban foglalt elvek megvalósításának egyik módja a szervezeten belül érvényesülő gyakorlati útmutatók kiadása, illetve kockázatfelmérések készítése, amelyek kiindulási pontja lehet a hét alapelv.[10] A Microsoft hivatalos tájékoztatása szerint a *privacy by design* elvével való összhangot a vállalat úgy valósítja meg, hogy az adatok

9 Cavoukian 2010.

10 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (2019. 11. 27.)

védelmének tiszteletben tartását a technológiától elválaszthatatlanná teszi, ezt pedig fejlett és átfogó adatvédelmi szabályzatokkal bástyázza körül.[11]

A beépített adatvédelem elvével való összhang megteremtése és a rendelet előírásainak való megfelelés támogatására ugyan több módszer és javaslat létezik, ugyanakkor a fentebb említettekből következően ezek egyike sem hivatalos részletszabály vagy uniós szervtől származó útmutatás. A GDPR mindössze annyit határoz meg 42. cikkének (1) bekezdésében, hogy a tagállamok és uniós szervek ösztönzik olyan tanúsítási mechanizmusok létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott műveletek megfelelnek a rendelet előírásainak. A *privacy by design* elvét intézményesítő 25. cikk harmadik bekezdése ehhez kapcsolódóan kimondja, hogy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti a beépített adatvédelem követelményeit. Ilyen jóváhagyott mechanizmusok jelenleg kevésbé elterjedtek, ugyanakkor elérhetők egyes tanúsítási segédletek és vázak.[12] Például a beépített adatvédelem kiválósági központja a Ryerson Egyetemen Ann Cavoukian vezetésével lehetőséget nyújt ilyen tanúsítvány megszerzésére, amely a hét, már ismertetett alapelvre épül. A központ tájékoztatása szerint az okirat megszerzői biztosak lehetnek abban, hogy megfelelnek a globálisan elismert legmagasabb szintű adatvédelmi elvárásoknak.[13] Mindazonáltal, a technológiákkal párhuzamosan ezek az elvárások is dinamikusan változhatnak, így kérdéses lehet, hogy egy-egy tanúsítvány milyen időtartamra jelent biztosítékot a tulajdonosa számára. A rendelet előírásainak való megfelelést ezenkívül például a OneTrust vállalat is támogatja, amely széles körű eszköztárat biztosít mindazoknak, akik a *privacy by design*-t a lehető legsikeresebben kívánják implementálni.[14] Egyik kiemelt szolgáltatása az adatvédelmi hatásvizsgálatok hatékony lefolytatásának támogatása.[15] Léteznek továbbá egyes stratégiák is a beépített adatvédelem elvének való megfeleléshez. Jelenleg nyolc ilyen módszer különböztethető meg: a minimalizáció, elrejtés, elválasztás, összegzés, tájékoztatás, irányítás, érvényesítés és bizonyítás,[16] amelyek számtalan független és tagállami hivatalos forrásban is megtalálhatók.[17] Ugyanakkor e stratégiák alkalmazása sem feltétlenül jelenti minden, az elv által támasztott elvárás teljesítését, hiszen annak pontos magyarázatával az unió a mai napig adós.

11 Lynch 2010.
12 Clearwater–Philbrook 2018.
13 www.ryerson.ca/pbdce/certification/ (2020. 04. 02.)
14 www.onetrust.com/ (2020. 04. 02.)
15 www.onetrust.com/products/assessment-automation/ (2020. 04. 02.)
16 Hoepman 2012.
17 www.onetrust.com/products/assessment-automation/ (2020. 04. 02.); *A Guide to Privacy by Design* 2019.

A döntéstervezés jelentette kihívás

A létező szolgáltatások, illetve a szakirodalom elsősorban azzal foglalkozik, hogy a *privacy by design* miképp szervesüljön a tervezési folyamatokban. Kevés figyelem jut azon veszélyekre, amelyek az adatvédelmi alapelv és más tervezési gyakorlatok együttes jelenlétéből adódhatnak. A rendelet szövegének absztrakt megfogalmazását kihasználva a gyártóknak lehetőségük nyílhat olyan adatkezelésre, amely akár a létező adatvédelmi rezsim szerint legális is lehet, mégis komolyan befolyásolhatja a fogyasztói döntés szabadságát, így a magánszféra sérelmét okozhatja.

A beépített adatvédelem elsősorban a tervezési fázisban megnyilvánuló egyéb, profitmaximalizásra optimált technikai megoldásokkal kerülhet kollízióba. Ilyen, már jól ismert és bevett folyamat a döntéstervezés *(choice architecture).* A döntésekről általában elmondható, hogy nem inger- és befolyásmentes környezetben születnek. A döntéshozót számtalan észrevehető és észrevétlen tényező veszi körül, amelyek hatással vannak rá. Az a személy vagy entitás, amely ezt a környezetet a döntéshozó számára megteremti, kialakítja, a döntéstervező.[18]A korai közgazdaságtan alapvető feltevése, hogy az emberek racionálisan gondolkoznak, tehát a döntési alternatívák közül azt fogják választani, amely számukra a legnagyobb hasznossághoz vezet. Ez azonban már az 1970-es években több szempontból is megkérdőjeleződött. A racionalitást számtalan faktor képes igen nagymértékben befolyásolni, miáltal a döntés végkimenetele kifejezetten irracionális is lehet. Egyebek mellett az úttörő munkásságú Daniel Kahneman és Amos Tversky játszottak szerepet az emberi irracionalitás kutatásában és okainak feltárásában.[19] Ők inspirálták a 2017-ben közgazdasági Nobel-díjas Richard Thaler-t is, aki Kahneman és Tversky eredményeiből kiindulva, de immár saját koncepciójaként alkotta meg a döntéstervezés alapgondolatát, illetve az úgynevezett „elmozdítás-elméletet" *(nudge theory).* A döntéstervezés és elmozdítás figyelembe veszi az emberek gondolkodásának bizonyos általános jellemzőit, többek között azt, hogy általában az egyszerűségre törekszenek, korlátozott ideig képesek koncentrálni, és a bonyodalmak elkerülése érdekében hajlandóak az eredeti elképzeléseikkel ellentétesen is cselekedni.[20] A *nudge* nem kényszerít egy bizonyos döntés meghozatalára, de általában érzékelhetően egyszerűbbé teszi a döntéstervező által preferált végeredmény elérését egy másik alternatívához képest. Lehet *nudge* egy utalás, emlékeztető vagy figyelmeztetés is. Thaler szerint fontos ezeket a választásokat orientáló enyhe beavatkozásokat felelősen alkalmazni, hogy a döntési szabadság korlátozása ne merülhessen fel. Ezenkívül az elmozdítás nem erőszakos befolyásolás. Amennyiben egy elmozdítás elhárítása nem könnyű vagy nem olcsó, már nem beszélhetünk elmozdításról, sokkal inkább kényszerről.[21]

18 Thaler–Sunstein–Balz 2014.; Thaler–Sunstein 2008.
19 Kay 2017.; Connor 2019.
20 Connor 2019.
21 Connor 2019.

A gondolatot azóta maga Thaler, de más pszichológiai, gazdasági és egyéb tudományos ágazatban tevékenykedő kutató is továbbtanulmányozta, tartalmát pontosította, és egyre újabb felhasználási lehetőségeit fedezte fel. A *nudge*-módszer a köztudatba is hamar bekerült, illetve egyre nyilvánvalóbbá váltak azok az előnyök, amelyeket alkalmazása kínál. Ennek következtében számtalan kontextusban felhasználták, a legkülönbözőbb célok elérése érdekében. Az Egyesült Királyságban például külön kormányhivatal létezik, amely az emberi viselkedés tanulmányozására fókuszál, majd a tapasztalatokat olyan módon hasznosítja (többek közt a *nudge* alkalmazásával), hogy azok a társadalom érdekeit szolgálják.[22] Az elmozdítások által elérhető előnyök megtestesülhetnek akár profitban, mint tiszta anyagi előny, többletinformáció megszerzésében, amely közvetett materiális előny, hiszen napjainkban az adatok tömeges begyűjtésével és stratégikus felhasználásával komoly nyereség érhető el, vagy járhat egy-egy elmozdítás össztársadalmi, például egészségügyi előnnyel.

Az elmozdítás módszerét természetesen az informatikai rendszerek és szolgáltatások tervezői is kiaknázzák, mi több, ez az ágazat a *nudge* egyik fő alkalmazási területe. Amint azt már fentebb említettük, napjaink információs társadalmában az adatok képviselik az egyik legnagyobb értéket. A böngészőket, applikációkat, okosjárműveket vagy akár az okosotthonokat is mind úgy alakítják ki, hogy minél nagyobb mennyiségű adatot gyűjthetnek be, annál több, jobb, személyre szabottabb szolgáltatásokat nyújthatnak a felhasználók számára. Ezzel azonban végső soron nem az ügyfél, hanem a szolgáltatás kínálója jár jobban, hiszen minél jobban a felhasználó kényelméhez igazítja az adott alkalmazást vagy terméket, ő valószínűleg annál jobban fog ragaszkodni a szolgáltatóhoz, még több adatát osztja meg vele, és adott esetben még több szolgáltatását vásárolja meg.

A legnagyobb informatikai vállalatok, úgymint a Facebook, a Google, a Microsoft, a Netflix vagy az Instagram is szolgáltatásaik működtetése során számos módon mozdítják el a felhasználóik döntését a számukra kedvező irányba. Teszik ezt általában minél több adat megszerzése érdekében. Ahogyan azt már többször említettük, napjainkban szinte minden ágazatban, de kifejezetten a szórakoztatás, szabadidő és szociális háló területein, amelyeken ezek a vállalatok működnek, az adat a fő bevételforrás. Ugyan a felhasználói tevékenység monitorozása, majd az ez alapján elkészült profil reklámozóknak való értékesítése által is gyűjthetők értékes információk, mégis, az igazán személyes adatok, amelyek a tényleges, egyedülálló értéket képviselik a vállalatok körében, tisztességes úton csak korlátozottan hozzáférhetők. Azonban a felhasználói hozzájárulással ezen adatok kezelése is jogszerű. Ezért a cégek a hozzájáruláshoz sokszor nem transzparens tájékoztatás, az alapértelmezett beállítások célzott megadása, illetve a legkisebb ellenállás irányába tartó viselkedési tendencia kihasználása révén próbálnak hozzájutni, amely egyes esetekben felvetheti a tisztességtelenség vádját. A norvég fogyasztói tanács 2018-ban kiadott jelentésében tanulmányozta a Facebook, a Google és a Microsoft felületeit és beállításait abból a szempontból,

22 www.bi.team/about-us/ (2020. 04. 02.)

hogy a *choice architecture* milyen mintázatai fedezhetők fel, illetve azok hogyan nyilvánulnak meg. E vizsgálat szerint mindhárom vállalatnál megállapítható volt, hogy kihasználták az alapértelmezett beállítások által szerezhető előnyöket előre kiválasztott vagy grafikailag kiemelt opciókkal. A Facebook és a Google alapbeállításai eszerint továbbá kifejezetten sértik a személyes adatok védelmét, hiszen a nagyobb védelmet biztosító opcióhoz csak egy hosszabb és bonyolultabb lépéssorozat útján biztosítják az eljutást.[23]

Az utóbbi években a gyarapodó adatvédelmi fenyegetések kezelésére vonatkozó uralkodó koncepció azon alapult, hogy a felhasználók rendelkezzenek az adataik felett hatékonyabb irányítással és azokkal kapcsolatban több információval.[24] A legtöbb államban olyan mechanizmusokat építettek be, amelyek az ügyfél értesítésén és jóváhagyásán alapulnak. A vállalatok is ennek megfelelően több választási lehetőséget és a személyes adatok különböző mértékű felhasználását tették lehetővé.[25] Ugyanakkor ezeknek az intézkedéseknek inkább negatív, mintsem pozitív hatásai figyelhetők meg. Mivel a felhasználók szinte teljes körű irányítás birtokában vannak, ők döntenek személyes adataik sorsáról, hogy azokat mely szolgáltatók számára fedjék fel és milyen tevékenységek során. Az idegen kezelők kiiktatásával ugyan megszűntek egyes veszélyforrások, de egyúttal biztosítékok is. Szakszerű iránymutatás hiányában az egyének sokkal könnyebben meggyőzhetők arról, hogy személyes adataikat kiadják a kezükből. Az elmozdítás módszer segítségével könnyedén elérhető, hogy a szolgáltatás működéséhez nem feltétlenül szükséges, sőt, attól egészen távol álló adatok gyűjtését is engedélyezze egy-egy felhasználó, amennyiben a megfelelő módszerekkel befolyásolják a döntéseit. Végeredményben az állapítható meg, hogy ugyan a döntések szabadok, a szolgáltatók a *choice architecture* segítségével úgy alakítják ki azok környezetét, hogy a lehető legnehezebb legyen megállapítani, mi az, ami ténylegesen a felhasználó érdekét szolgája, és mi az, ami valójában a vállalatét.[26]

A gépi tanulás tovább növeli a veszélyt

Az úgynevezett gépi tanulás tovább növeli a szofisztikált informatikai óriások hatalmát a fogyasztók felett. Mint láttuk, közösségi szinten a *nudge*-ok alkalmazása hatékonynak bizonyulhat, az általánosításuk nagyon nehezen és költségesen megvalósítható, így az egyének szintjén egyértelműen más megközelítés szükséges. Jelenleg az adattudomány, a mesterséges intelligencia és azon belül a gépi tanulás területein zajlik olyan előrejelző módszerek kidolgozása, amelyek nagyszámú, heterogén csoportokra vonatkozóan végeznek méréseket és általánosításokat. Az AI területén belül olyan autonóm és racionális ügynökök tervezésével foglalkoznak, amelyek képesek

23 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (2020. 04. 02.)
24 Adjerid–Acquisti–Loewenstein 2014.
25 Holt 2019.
26 Naughton 2018.

tanulni, előrejelzéseket adni és döntéseket hozni, ezekkel kapcsolatban pedig fejlődni. Mindezt emberi beavatkozás nélkül. Ezek a technológiák az emberi gondolkodást modellezik olyan formulák alapján, mint a Bayes-tétel,[27] neurális hálók,[28] tartóvektor-gépek[29] vagy döntésifa-algoritmusok.[30] Működésük kizárólag a konkrét, megfigyelt döntésekre épül ahelyett, hogy az emberi viselkedést általában próbálná megjósolni.[31] Az ismétlődő tanulás alapú algoritmusok célja egy olyan modell létrehozása, amely különböző adatcsoportok közötti, gyakran rejtett összefüggéseket ír le. A kialakult modellek minden egyes kérdés-felelet által fejlődnek, mivel a kapott visszajelzéseket azonnal beépítik az algoritmusba. A gépi tanulás az utóbbi fél évszázadban terjedt el, és alkalmazási köre napjainkig folyamatosan bővül. Felhasználható egyebek mellett az önvezető járművekben, üzleti adatok előrejelzésének érdekében, az orvosi diagnosztikában, vagy a bankok eszközeként például a hitelnyújtás megkönnyítéséhez.[32]

A gépi tanulásnak több típusát különböztethetjük meg. Az egyik a felügyelt tanulás, amely során egy ember jelen van, és mint oktató irányít. A gép úgynevezett címkézett adatokkal kerül kapcsolatba a felügyelt tanulás során. Ez egy gyakorlópélda-halmaz, amelyben minden példa egy párt alkot. A pár egyik eleme egy *input* adat, a másik pedig a kívánt végeredmény, az *output*. Az oktató betáplálja az alapadatokat az algoritmusba, majd a folyamat végén a helyes kimenetelt, a pár másik felét is megadja. Ezáltal a gépnek meg kell tudni tanulnia a mintát, amellyel eljuthat a megfelelő végkövetkeztetéshez. Ilyen típusú algoritmusok a tartóvektor-gépek, a neurális hálók, illetve a döntési fák is. Egy másik típus a nem felügyelt tanulás, amelyben a gép nem címkézett adatokkal dolgozik. Ennek során az algoritmus magától próbál az *input* adatok alapján szabályokat felfedezni és mintázatokat kialakítani. Nincsenek előre megadott optimális kimenetelek. Megkülönböztethető még a megerősítő tanulás is. Ennek során az algoritmus a környezetével való ismétlődő interakciókból tanul.[33]

A gépi tanulást alkalmazó algoritmusok napjaink leghasznosabb analitikus segédeszközei közé tartoznak, ugyanakkor ezek a technológiák sem veszélytelenek, adatvédelmi szempontból különösen nem. Egy gépi tanuláson alapuló algoritmusba táplált adatok alapján egy személy sem lehet beazonosítható, akihez az adat vagy adattöredék tartozik. Ennek ellenére előfordul, hogy a fejlett, többdimenziós algoritmusok ember által nem észrevehető jegyek alapján mégis képesek konkrét profilt kialakítani. Például több olyan önéletrajz tanulmányozása során, amelyekből eltávolították a nem megjelölését a hátrányos megkülönböztetés elkerülése érdekében, a gép olyan tényezőkből, mint a nyelvhasználat vagy forma, mégis következtetni tud az adott jelentkező

27 https://plato.stanford.edu/entries/bayes-theorem/ (2020. 04. 02.)
28 Siegelmann–Sontag 1992.
29 Patel 2017.
30 Gupta 2017.
31 Rosenfeld et al. 2012; Mitchell 1977.
32 Hrnjic–Tomczak 2019.
33 Fumo 2017.

nemére.[34] Megjegyzendő, hogy a GDPR 22. cikke alapján a profilalkotás jogszerűen is lehetséges, ez azonban az eseteknek csak egy szűk, meghatározott körére vonatkozik.

Egy-egy ilyen algoritmus továbbá ugyanúgy megvalósíthatja az elmozdítás módszerét, ez azonban már eltérő hatásokkal jár, mintha ember befolyásolna embert.[35] A hagyományos *nudge* módszer csak nagyobb embercsoportra alkalmazva volt hatékony, azonban a mesterséges intelligenciák már alkalmasak arra, hogy személyre szabott döntésorientáló tényezőket alkalmazzanak. Továbbá egy erre kifejlesztett gép sokkal több adatot képes egyszerre feldolgozni és analizálni, mint egy ember vagy egy vállalat, így sokkal hatékonyabban is fogja azokat célzott hirdetések formájában felhasználni.[36] Amennyiben a mesterséges intelligencia *input* adatai kifejezetten személyes adatok, a felhasználási lehetőségek gyakorlatilag végtelenek az egyedi emberi viselkedés befolyásolása szempontjából.

A magánszféra változó fogalma

A magánszféra fogalmának meghatározása nehéz, elsősorban azért, mert az nem hazánkból származik, hanem az Amerikai Egyesült Államokból, illetve Magyarországon némileg más tartalommal használatos. Nem definiálható egyszerűen, hiszen számos eltérő kontextusban használják annak érdekében, hogy információval, térbeliséggel, testtel, lélekkel, kommunikációval vagy mással kapcsolatos értékekre utaljanak. Samuel Warren és Louis Brandeis klasszikus meghatározása szerint a magánszféra az „egyedül hagyatáshoz való jog", vagyis annak a lehetősége, hogy az egyének távol tartsák a társadalmat és az államot.[37] Tágabb értelmében a magánszférát gyakran az „információs önrendelkezéssel" kapcsolják össze. E fogalom középpontjában a személyekhez való hozzáférés korlátozása áll, mivel arra a követelésre utal, hogy az egyének befolyásolhassák, mások miként férnek hozzá személyükhöz és a rájuk vonatkozó információkhoz. Az adatvédelmi jogban hangsúlyosan kifejeződik ez a nézet.[38] A magánszféra fogalmát továbbá gyakran hozzák összefüggésbe az autonómiával is.

A fogalom tartalmát a nevesített személyiségi jogok mint egyfajta részjogosítványok adják. A magánélet védelme megközelíthető egyfelől az emberi méltóság, másfelől az egyéni szabadság védelme felől. A magánélet védelmét az emberi méltóság védelméhez kötő megközelítés elsősorban a kontinentális európai jogrendszerekre, míg a személyes (döntési) szabadság védelméhez kapcsoló megközelítés az amerikai jogra jellemző.[39]

A magánszférával és a fogalma alá tartozó jogosultságokkal általában az államok, kormányok, cégek vagy társadalmi szervezetek kerülnek szembe. A magyar Polgári

34 Dorschel 2019.
35 Oremus 2016.
36 Plautz 2018.
37 Warren–Brandeis 1890, 193–219.
38 Raab 2017.; Friedwald–Finn–Wright 2013.
39 Menyhárd 2014, 385.

Törvénykönyv a nevesített személyiségi jogok között szerepelteti mind a személyes szabadság, a magánélet, a magánlakás, a magántitok és a személyes adatok védelméhez való jogot, azaz tulajdonképpen a magánszféra védelmét. Ezek a 2:42. § értelmében a Polgári Törvénykönyv oltalma alatt állnak. Akkor korlátozhatók jogszerűen, ha a korlátozás egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül bizonyos fontos érdekek védelme – így például a közbiztonság, valamint a bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása vagy a közbiztonságot fenyegető veszélyekkel szembeni védelem és veszélyek megelőzése érdekében.

Napjaink digitális társadalmában a magánszférát ugyanakkor már csak egy rendkívül keskeny határvonal választja el a nyilvánosságtól. A valós idejű kommunikáció és információmegosztás fejlődése az elmúlt évtizedekben drámai mértékű volt.[40] A technológiai vívmányok hatására azt tapasztalhatjuk, hogy az emberek mind nagyobb mértékben fedik fel a magánéletüket a nyilvánosság előtt.[41] Ez a legtöbb esetben ráadásul önkéntes. A szolgáltatók többsége közvetett módon hangsúlyozza termékével kapcsolatban, hogy minél több adatot gyűjthet a felhasználóról, annál jobb, személyre szabottabb élményt képes nyújtani.[42]

Tulajdonképpen a hozzánk eljuttatott tartalmak, a beérkező információk bizonyos értelemben személyes adatoknak minősülnek, hiszen a mi tulajdonságainkat, szokásainkat, korábbi fogyasztói döntéseinket tükrözik. Abból az adatcsomagból, amely egy meghatározott egyént mint marketingalanyt céloz, amennyiben a rendszer már elég termékpreferenciával kapcsolatos információt szintetizált róla, egy idő után csak rá lehet visszakövetkeztetni. Azaz már nemcsak a kiáramló információ lesz személyes adat, hanem a beáramló is annak minősül. Továbbá az, hogy minden hozzánk eljutó tartalom egyfajta személyes preferenciaszűrőn halad át, idővel egyfajta buborékhatást eredményez. A választások és döntések alapján egy digitális profilt készítenek az egyénről, majd ennek megfelelően érik behatások, végül ennek eredményeképpen egy önmegerősítő spirálba kerül, ahol a régi identitásának bűvkörében reked, és abból nem tud kitörni. A többség ízlése idővel változik, egyes termékcsoportokat tekintve gyakrabban, egyeseket ritkábban, de a változás törvényszerű. Az, hogy örökösen ugyanolyan tartalmakat látunk, ugyanolyan árucikkek megvételére ösztönöznek minket, az ebbe a természetes változásba történő beavatkozás. Annak ellenére, hogy ez a marketingmódszer tulajdonképpen egy kényszerű helyzetet teremt, és azzal is visszaél, hogy az egyének naponta mennyi időt töltenek online, sajnálatos módon gyakran éri el a célját. A legtöbb felhasználó nem tud róla, vagy pedig nem foglalkozik vele, hogy a tudatát ilyen módon manipulálják, és alkalmazkodik a helyzethez. Megvásárolja ugyanazokat a termékeket és meghozza ugyanazokat a döntéseket, amelyeket az évekkel korábbi énje is meghozott volna, a változásnak és újdonságoknak pedig így nem jut tér, nem fejlődik természetesen az identitás. Üzleti szempontból

40 *The Right to Privacy in the Digital Age* 2015.
41 Simay–Gáti 2015.
42 Yu 2019.

ez a tendencia előnyös, hiszen így az egyes termékekhez, illetve terméktípusokhoz hozzárendelhetnek konkrét fogyasztói csoportokat, így biztosítva azokra a folyamatos keresletet.

Erre a jelenségre ad választ az általunk javasolt egyik új alapelv, a *privacy by randomness,* hiszen kétségtelen, hogy a fentebb leírtak alapján a legújabb generációs adatvédelemnek már a személyiség autonómiáját, az identitás spontán fejlődését is védenie kell. A *privacy by randomness* azt írná elő, hogy a kezelők kötelesek abba az adatcsomagba, amely alapján számunkra a tartalmakat kiküldik, a személyes preferenciákon kívül véletlenszerű információkat is keverni. Ezáltal kapcsolatba kerülhetnénk az eddigi döntéseinkhez hasonló tartalmakkal, ugyanakkor teljesen új, addig ismeretlen termékekkel és szolgáltatásokkal is. Ha ez megvalósulna, az egyén leküzdhetné a buborékhatást, kiszabadulhatna az azonos választások spiráljából, illetve személyisége áteshetne a természetes változásokon. A fizikai valóságban is elkerülhetetlen, hogy olyan dolgokkal találkozzunk, amelyek esetleg nem nyerik el a tetszésünket, tehát az imént említett bezártság-hatás erősödésének elkerülése érdekében szükségszerű ezt a virtuális szférában is, akár az adatvédelem által megteremteni.

Másfelől vitathatatlan, hogy senkinek nincs arra elég ideje vagy hajlandósága, hogy az összes általa használt applikáció vonatkozásában folyamatosan ellenőrizze a személyes adatait. Minden egyes alkalmazással kapcsolatban naprakésznek kellene lennie az egyénnek, hogy valóban törölték-e az adatait onnan, ahol lejárt az azokra vonatkozó tárolhatósági idő, hogy ténylegesen csak olyan célra használta fel az információkat az adatkezelő, amelyhez az egyén kifejezett hozzájárulását adta, vagy, hogy nem használták-e fel az adatokat a tárolhatósági idő lejárta után, hogy az adatvédelem ténylegesen és hatékonyan megvalósulhasson. Ez azonban olyan fárasztó, unalmas és időrabló feladat, amelyet voltaképpen senki nem végez el önként, illetve nem is végez el egyáltalán. Az ilyen irányú kontroll elmaradása ismét egy a személyes adatok védelmét megnehezítő, gondatlan tendencia, még akkor is, ha az egyén ezt tulajdonképpen idő hiányában önhibáján kívül teszi. Éppen ezért a javasolt új alapelv, a *privacy by assistance* értelmében előírás lenne minden felhasználó mellé egy digitális adatvédelmi asszisztens rendelése. Ez a technikai segítő az imént említett összes vonatkozásban folyamatos figyelemmel kísérné az érintett személyes adatait. Felügyelné azok hollétét és felhasználását, hogy a *privacy by randomness* elve megvalósul-e, hogy az alapértelmezett beállítások valóban az adatvédelem szempontjából barátságosak, illetve gondoskodna mindenfajta visszaélés elkerüléséről, vagy esetlegesen értesítené az érintettet a nem megbízható kezelőkről is. Az asszisztens a már említett *nudge-ok* által terelhetné őt bizonyos célok felé is, az érintett választásának megfelelően. Az asszisztens így ösztönözhetné a felhasználót tanulásra vagy akár egészségesebb életmódra, a szerint, hogy ő milyen erre vonatkozó utasítást ad neki.

Összegzés

A fentiek alapján jól érzékelhető összefüggés rajzolódik ki a magánszféra, illetve határainak elmosódása és a többek közt erre építő gépi tanulásos algoritmusok, mesterséges intelligenciák között. A magánszférát hagyományosan teljes körű védelem illeti, ezt azonban leggyakrabban éppen a fogyasztók, e védelem jogosultjai hiúsítják meg. Olyan szolgáltatásokat vásárolnak vagy használnak tömegesen, amelyek célja kifejezetten a magánszférába való bejutás, az ott „található" személyes adatokhoz való hozzáférés. A szolgáltatók az érzékeny adatok megszerzését követően algoritmusaik segítségével még célzottabban szólítják meg felhasználóikat és virtuális profilt alakítanak ki róluk. Ez végeredményben oda vezethet, hogy egy platform adott esetben több információval rendelkezik az egyénről, mint ő saját magáról. Az algoritmus bizonyos élethelyzetekben szinte eggyé válik a magánszférával.

Véleményünk szerint a hatályos adatvédelmi rezsim elégtelen e kihívásokkal szemben. A *privacy by design* bizonyos esetekben csak tetézi a bajt azzal, hogy még tudatosabbá teszi a döntéstervezést. Az érintett egyének adatszuverenitása ma már nem védhető a személyes adatok eddigi, belülről kifelé irányuló adatmozgásra fókuszáló szabályrendszerével. Paradigmaváltásra van szükség. Ennek keretében a virtuális térben a magánszférát a kívülről származó kvázi személyes adatok ellen is védelmezni szükséges a buborékhatás kivédése érdekében. A hatályos adatvédelmi rendszer reformja érdekében két új alapelv, az egymásra épülő *privacy by randomness* és a *privacy by assistance* bevezetését szorgalmazzuk.

Felhasznált irodalom

Adjerid, Idris – Acquisti, Alessandro – Loewenstein, George (2014): *Framing and the Malleability of Privacy Choices*. Elérhető: www.econinfosec.org/archive/weis2014/papers/AdjeridAcquistiLoewenstein-WEIS2014.pdf (2020. 04. 02.)

Cavoukian, Ann (2010): *Privacy by Design – The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices.* Elérhető: https://collections.ola.org/mon/24005/301946.pdf (2020. 04. 02.)

Clearwater, Andrew – Philbrook, Brian (2018): *Privacy by Design and GDPR: Putting Policy into Practice.* Elérhető: www.cpomagazine.com/data-privacy/privacy-by-design-and-gdpr-putting-policy-into-practice/ (2020. 04. 02.)

Connor, Tom (2019): *Helping people make better choices — Nudge Theory and Choice architecture*. Elérhető: https://medium.com/10x-curiosity/helping-people-make-better-choices-nudge-theory-and-choice-architecture-431a3a40b688 (2020. 04. 02.)

Dorschel, Arianna (2019): *Rethinking Data Privacy: The Impact of Machine Learning*. Elérhető: https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60 (2020. 04. 02.)

Friedwald, Michael – Finn, Rachel L. – Wright, David (2013): *Seven Types of Privacy*. Elérhető: www.researchgate.net/publication/258892458_Seven_Types_of_Privacy (2020. 04. 02.)

Fumo, David (2017): *Types of Machine Learning Algorythms You Should Know*. Elérhető: https://towardsdatascience.com/types-of-machine-learning-algorithms-you-should-know-953a08248861 (2020. 04. 02.)

Gupta, Prashant (2017): *Decision Trees in Machine Learning*. Elérhető: https://towardsdatascience.com/decision-trees-in-machine-learning-641b9c4e8052 (2020. 04. 02.)

Hoepman, Jaap-Henk (2012): Privacy Design Strategies. Elérhető: www.cs.ru.nl/~jhh/publications/pdp.pdf (2020. 04. 02.)

Holt, Kris (2019): *Instagram Is Giving Users More Control Over Their Privacy*. Elérhető: www.forbes.com/sites/krisholt/2019/10/15/instagram-is-giving-users-more-control-over-their-privacy/#716391afce85 (2020. 04. 02.)

Hrnjic, Emir – Tomczak, Nikodem (2019): *Machine learning and behavioral economics for personalized choice architecture*. Elérhető: www.researchgate.net/publication/334248859_Machine_learning_and_behavioral_economics_for_personalized_choice_architecture (2020. 04. 02.)

Kay, John (2017): *Behavioural economics: did Kahneman and Tversky change the world?* Elérhető: www.prospectmagazine.co.uk/magazine/behavioural-economics-did-kahneman-and-tversky-change-the-world (2020. 04. 02.)

Lynch, Brendon (2010): *Privacy by Design at Microsoft*. https://blogs.microsoft.com/on-the-issues/2010/11/30/privacy-by-design-at-microsoft/ (2020. 04. 02.)

Menyhárd Attila (2014): A magánélethez való jog elméleti alapjai. *In Medias Res,* 11. évf. 2. sz. 384–406. Elérhető: http://media-tudomany.hu/archivum/a-maganelethez-valo-jog-elmeleti-alapjai/ (2020. 04. 02.)

Mitchell, Jeremy (1977): A Systematic Approach to Analysing Consumer Complaints. *Journal of Consumer Studies and Home Economics,* Vol. 1, No. 1. 3–20. DOI: https://doi.org/10.1111-/j.1470-6431.1977.tb00183.x

Naughton, John (2018): *More choice on privacy just means more chances to do what's best for big tech*. Elérhető: www.theguardian.com/commentisfree/2018/jul/08/more-choice-privacy-gdpr-facebook-google-microsoft (2020. 04. 02.)

Oremus, Will (2016): *Who Controls Your Facebook Feed*. Elérhető: www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html?via=gdpr-consent (2020. 04. 02.)

Patel, Savan (2017): *Chapter 2: SVM (Support Vector Machine) – Theory*. Elérhető: https://medium.com/machine-learning-101/chapter-2-svm-support-vector-machine-theory-f0812effc72 (2020. 04. 02.)

Plautz, Jessica (2018): *Google Maps Is Personalizing Dining and Activity Recommendations, and Will Even 'Match' You to Restaurants*. Elérhető: www.travelandleisure.com/travel-tips/mobile-apps/google-maps-percentage-match (2020. 04. 02.)

Raab, Charles D. (2017): A magánszféra mint biztonsági érték. *Replika,* 103. évf. 3. sz. 81–95. 82. Elérhető: http://epa.oszk.hu/03100/03109/00006/pdf/EPA03109_replika_103_081-095.pdf (2020. 04. 02.),

Rosenfeld, Avi – Zukerman, Inon – Azaria, Amos – Kraus, Sarit (2012): Combining Psychological Models with Machine Learning to Better Predict People's Decisions. *Synthese,* Vol. 189, No. S1. 81–93. DOI: https://doi.org/10.1007/s11229-012-0182-z

Siegelmann, Hava T. – Sontag, Eduardo D. (1992): *On The Computational Power of Neural Nets*. DOI: https://doi.org/10.1145/130385.130432

Simay Attila Endre – Gáti Mirkó (2015): *Nyilvánosság és magánélet a mobiltelefon és a közösségi média használat tükrében*. Elérhető: www.researchgate.net/publication/281319103_Nyilvanossag_es_maganelet_a_mobiltelefon_es_a_kozossegi_media_hasznalat_tukreben (2020. 04. 02.)

Thaler, Richard H. – Sunstein, Cass R. (2008): *Nudge: Improving Decisions about Health, Wealth, and Happiness*, New Haven, Yale University Press.

Thaler, Richard H. – Sunstein, Cass R.– Balz, John P. (2014): *Choice Architecture. The Behavioral Foundations of Public Policy, Ch.* 25, 2014. Elérhető: www.sas.upenn.edu/~baron/475/choice.architecture.pdf (2020. 04. 02.)

Warren, Samuel – Brandeis, Louis (1890): The Right to Privacy. *Harvard Law Review,* Vol. 4, No. 5. 193–219. DOI: https://doi.org/10.2307/1321160

Yu, Allen (2019): *How Netflix Uses AI, Data Science, and Machine Learning – From A Product Perspective*. Elérhető: https://becominghuman.ai/how-netflix-uses-ai-and-machine-learning-a087614630fe (2020. 04. 02.)

Jogforrás

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Internetes források

Bayes' Theorem (2003). Stanford Encyclopedia of Philosophy. Elérhető: https://plato.stanford.edu/entries/bayes-theorem/ (2020. 04. 02.)

The Behavioural Insights Team. Elérhető: www.bi.team/about-us/ (2020. 04. 02.)

Buttarelli, Giovanni (2018): *Preliminary Opinion on Privacy by Design.* Opinion 5/2018. The European Data Protection Supervisor. Elérhető: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (2020. 04. 02.)

Deceived by Design (2018). Elérhető: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (2020. 04. 02.)

A Guide to Privacy by Design (2019). AEPD. Elérhető: www.aepd.es/media/guias/guia-privacidad-desde-diseno_en.pdf (2020. 04. 02.)

The History of the General Data Protection Regulation. European Data Protection Supervisor. Elérhető: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (2020. 04. 02.)

ICO: *Data protection by design and default.* Elérhető: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (2019. 11. 27.)

OneTrust hivatalos oldal. Elérhető: www.onetrust.com/ (2020. 04. 02.)

Privacy by Design Certification. GPS by design Center. Elérhető: www.ryerson.ca/pbdce/certification/ (2020. 04. 02.)

Relevant GDPR Articles. OneTrust. Elérhető: www.onetrust.com/products/assessment-automation/ (2020. 04. 02.)

The Right to Privacy in the Digital Age (2015). United Nations Human Rights Office of the High Commissioner. Elérhető: www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx (2020. 04. 02.)