Eötvös Loránd Tudományegyetem

Állam-és Jogtudományi Kar

Alkotmányjogi Tanszék

Demokrácia 2.0?

A Big Data alapú adatkezelés demokratikus hatalomgyakorlást érintő kihívásai

Témavezetők:

Dr. Somody Bernadette
Dr. Székely Iván

Szerző:

Váradi Zsanett

Kézirat lezárásának dátuma: 2018. 12. 01.

I. Bevezetés

„Nem biztos, hogy jót tesz neked, ha kiszolgálják az ízlésedet!”[1] Talán ez a dalszövegrészlet ragadja meg legtömörebben írásom mondanivalóját. A dolgozat az adatvédelem új, alkotmányjogi kihívásaira világít rá a technológiai szingularitás[2] jegyében. A Big Data alapú adatgyűjtő és elemző technikák szemléltetésével szeretnék rámutatni arra, hogy az egyén kezébe adott jogvédelmi eszköz, az információs önrendelkezési jog mint alapjog ilyen magas szintű technológiai fejlettség mellett már nem feltétlenül adekvát. A tömeges adatgyűjtést eredményező, magas szintű megfigyelési módszerek segítségével ugyanis nem csak egyéni szinten jelenik meg az adatvédelmi szabályok megsértése mint alapjogsérelem. Ha az információs hatalmasságok minden egyes állampolgárról képesek kialakítani ún. személyiségprofilt, amely alapján manipulatív módszerekkel befolyásolni tudják az egyének gondolatait, cselekedeteit, úgy ez a jelenség a tágan értelmezett demokratikus intézményrendszert is veszélyezteti. A dolgozat a Big Data jelenség demokrácia-deficitet is eredményező hatásaira kívánja felhívni a figyelmet, és keresi az adatvédelem terén az új garanciális megoldásokat.

A dolgozatban tárgyalt, a demokráciát intézményesen veszélyeztető jelenségtömeg kétségtelenül multidiszciplináris megközelítést igényel. A társadalomfilozófiai és informatikai perspektíva elengedhetetlen, de a hangsúlyt a jogi szempontokra helyezem. Ezek közül az adatvédelem jogi szabályozása fontos – természetesen nem az egyetlen – kulcs lehet a jelenség elemzése kapcsán. A dolgozatomban felvonultatok néhány Big Data-specifikus adatvédelmi problémát, s ezeken keresztül vizsgálom azt a kérdést, hogy a demokratikus intézményrendszer védelmének szempontjából a technológia fejlődésével miért és hogyan szükséges együtt fejlődnie az állampolgárok személyes adatok védelméhez való alapvető jogát biztosító jogi garanciáknak.

Az információs önrendelkezés azon a fikción alapul, hogy az egyén képes önkéntes, határozott, megfelelő tájékoztatáson alapuló, egyértelmű döntéseket hozni személyes adatai tekintetében.[3] A fikció kifejezés használata szándékos, hiszen a Big Data jelenség folytán már alappal állítható, hogy a hagyományos dogmatikai keretek szétfeszültek: a technológia olyannyira

[1] Részlet a Bonanza Banzai: Induljon a Banzáj c. dalából.
[2] A kifejezés annak a jövőbeli eseménynek a bekövetkeztére utal, mikor az exponenciális technológiai fejlődés eléri azt a pontot, amely olyan társadalmi változásokat eredményez, hogy azt a jelen embere képtelen felfogni.
[3] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) 3. § 7. pont.

felülírta az adatkezelési szokásokat, hogy azután csak kullog a hagyományos alapú önrendelkezési megközelítés. Amint arra a fenti dalszöveg utal, az önrendelkezés korlátozása sem tesz jót nekünk. A kérdés az, hogy a garanciarendszerben hogyan lehet azt a problémát feloldani, hogy ugyan alkotmányos jogánál fogva, egyéni szinten magának mindenki árthat[4] – ez egyéni probléma –, de a tömeges ostobaság[5] nem tömeges egyéni jogsérelmet okoz, hanem magát a demokráciát veszélyezteti. Szinte csak egy hajszál választja el a digitális totalitarizmust a demokrácia 2.0-tól – a döntés a miénk.

Mind az állami, mind a magánjogi információs hatalmasságok[6] által folytatott információgyűjtés a kellő jogi garanciák megléte nélkül az alapjogok súlyos megsértésével jár a rohamosan fejlődő technológiák – a Big Data jelenség – adta kifinomult és betolakodó megfigyelést is biztosító lehetőségek miatt. Így a demokrácia megingatására is képes mechanizmusok idézhetők elő, például a prediktív profilírozás módszerével akár a demokratikus választások szabadsága is befolyásolható. Az, ha egy magáncég vagy magánszemély az információs hatalmi pozícióját a közhatalom befolyásolására használja, igazolja, hogy a közhatalommal nem bíró, magánjogi szereplőkkel szemben is kikényszeríthető az információs önrendelkezési jog.

A Big Data által megvalósítható személyiségprofil-alkotás, predikciók és manipuláció önkényes eszközeinek gátat szabhatna egy effektív adatvédelmi szabályozás, amelyben olyan intézményes garanciák szerepelnek, amelyek elejét veszik a demokráciaromboló mechanizmusoknak. Az új technológiák viszonylatában azonban a jogalkotás számos nehézségbe ütközik így nem biztos, hogy a megszületendő jogszabály teljeskörű válaszokat tud majd adni a technológiai kihívásokra. Amennyiben a jog önmagában nem tudja megakadályozni azt, hogy az egyének folyamatos alapjogsérelemnek legyenek kitéve, figyelembe kell venni más, a jogon kívüli lehetőségeket is. A technológia megoldást nyújthat azokon a területeken, ahol a jog erre nem képes, így ez az út megfontolandó szempont az új adatvédelmi garanciák kialakítása során.

A dolgozatban Magyarországra és az Európai Unióra fókuszálok. Egyrészt azért, mert az európai – és ezen belül az általunk is követett német – modell képviseli a legmagasabb védelmi

[4] Önmagának mindenki árthat, s vállalhat kockázatot, ha képes a szabad, tájékozott és felelős döntésre [21/1996. (IV. 17.) AB határozat].
[5] Ostobaság alatt nem feltétlenül csak a „természetes", emberek saját hibájából eredő butaságot értem, hanem benne foglaltatik a Big Data jelenség által fokozódó buborék hatás (Filter Bubble) is, ami olyan intellektuális izolációhoz vezet, mely a demokratikus vitatér szempontjából igencsak kedvezőtlen.
[6] Voltaképp bárki, aki kellőképp ért a Big Datához, így hatalmi erőeltolódást előidézve.

szintet és a legjobban kidolgozott dogmatikát az adatvédelem területén, amihez a globalizálódó világban másoknak is viszonyulniuk kell. Másrészt pedig a dolgozat terjedelme nem engedi meg, hogy más szabályozási modelleket is elemezzek, ugyanakkor tisztában vagyok vele, hogy ez elengedhetetlen lenne egy teljességre törekvő, igényes monográfia kidolgozásához.

A dolgozat három fő részre osztható. Kezdésként az adatvédelem alkotmányos alapjait ismertetem, majd a magyar és közösségi jogi szabályozásban történt jelentős, tendenciális változásokra térek ki. A következő nagyobb egység a Big Data technológiai, társadalmi és jogi aspektusait foglalja magában. Nélkülözhetetlennek tartom részletesebb példákkal szemléltetni a Big Data adta – az egyén önrendelkezése és a demokrácia szempontjából kedvezőtlen – technológiai lehetőségeket, mert ezáltal derülhet fény az alapjogvédelmi mechanizmusok hiányosságaira. Végül a jogi megoldáskeresés elveit exponálom, ami során arra jutok, hogy a jog önmagában véve képtelen adekvát válaszokkal szolgálni, így egy lehetséges technológiai megoldást javaslok a felvetett problémákra.

II. Az adatvédelem alkotmányos alapjai

Az adatvédelem a XX. század utolsó harmadában a számítástechnikában rejlő veszélyekre adott válaszként jelent meg.[7] Már az 1989-es Alkotmányban is nevesített jog volt,[8] s az Alaptörvényben is az alapjogok egyikeként szerepel.[9] A természetes személyek személyes adatainak védelméhez való joga Európai Uniós szinten is alapvető jogként van rögzítve, hiszen az Alapjogi Charta,[10] és az Európai Unió működéséről szóló szerződés[11] is deklarálja.

Ugyan megjelenésének ideje alapján harmadik generációs alapvető jog, azonban természetét tekintve alanyi alapjog. Szabadságjogi jellegét bizonyítja, hogy az államtól elsősorban tartózkodást vár el, az egyéni autonómia védelmének jegyében korlátozza a polgárokra vonatkozó adatok kezelését. Erre azért van szükség, mert az információs társadalomban az egyének személye virtualizálódik,[12] online és offline is rendkívüli mennyiségű adatot osztunk meg magunkról nap mint nap, akár szándékosan, akár akaratunkon kívül, ami a személyiség védelmében hatalmas kihívásként jelenik meg. A személyes adatok védelméhez való jog

[7] Emberi jogok. Szerk. Halmai Gábor és Tóth Gábor Attila. Osiris Kiadó, Budapest, 2008. 580-582. o.
[8] Alkotmány 59. § (1) bekezdés.
[9] Alaptörvény VI. cikk (3) bekezdés.
[10] Az Európai Unió Alapjogi Chartája 8. cikk (1) bekezdése.
[11] Az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikk (1) bekezdés.
[12] Szabó Máté Dániel: Az alapjogok információs jogi rétege. In: Jogi tanulmányok 2010. Ünnepi Konferencia az ELTE megalakulásának 375. évfordulója alkalmából. Budapest, ELTE ÁJK, 2010. I. kötet, 106. o.

személyiségvédelemben gyökerező mivoltát Sólyom László fogalmazta meg először az első generációs alapjog információs társadalomra történő konvertálódásaként.[13]

Magyarország magas adatvédelmi standardot állított fel a rendszerváltás után, hiszen a totalitárius rezsim eltörlésével, ahol az állampolgár átlátható, az állam pedig átláthatatlan volt, történeti vívmányként jelent meg az átlátható állam és átláthatatlan polgár koncepciója. A személyes adatok védelme mint alapjog az egyén kiismerhetőségéből adódó kiszolgáltatottságot hivatott megakadályozni, védi az egyéni autonómiát, a magánszférát. A magánszféra átvilágíthatóságával ugyanis az egyén személyisége kibontakozásának, a cselekvési és döntési szabadságának esélyei beszűkülnek. Az Alkotmánybíróság is úgy érvel, hogy „megalázó az olyan helyzet, és lehetetlenné teszi a szabad döntést, amelyben az egyik fél nem tudhatja, hogy partnere milyen információkkal rendelkezik róla."[14] A személyiségi jogok sérelmén túl tehát az emberi méltósághoz való jog megsértésében is megtestesül az alkotmányos adatvédelmi szabályok áthágása. Ennélfogva a magyar adatvédelmi szabályozási modell középpontjában az emberi méltóság mint alkotmányos érték, védendő alapjog jelenik meg az információs jogok igazolásaként.[15]

Az adatvédelem tartalmában európai értelmezés[16] szerint nemcsak az adatok védelme, a jogosulatlan hozzáférés tilalma[17] jelenik meg, hanem az adatalany[18] megóvása a cél. A magánszféra-oltalom[19] lényegi fogalmi eleme, hogy az érintett akarata ellenére mások ne tekinthessenek be a privát terébe.[20] Az, hogy kinek hol húzódnak a magánszféra határai, egyénileg eltérhet. Ez szükségképpen azt eredményezi, hogy az alapjogi jogosult döntheti el, hogy személyes adatait más egyáltalán megismerheti-e, s ha igen, akkor ki és meddig. Az alapjog tehát tevőleges magatartást vár el az egyéntől, ami speciális jelleget biztosít a személyes adatok védelméhez való jognak: az nem csak hagyományos védelmi jog, hanem létezik egy aktív oldala is, ez az információs önrendelkezési jog.[21]

[13] Sólyom László: A személyiségi jogok elmélete. KJK, Budapest, 1983. 45-127. o.
[14] 15/1991. (IV. 13.) AB határozat.
[15] Szigeti Tamás: Az információs hatalom korlátozása tengeren innen és túl. In: Infokommunikáció és jog, HVG-Orac, 2009. 159. o.
[16] Az amerikai adatvédelmi felfogásban (csak) az adatbiztonság érvényesül elsődleges fókuszként. Idézi: Szigeti, 2009. 162. o.
[17] Ez az adatvédelem tartalmán belül az adatbiztonság elve.
[18] Adatalany az, akire az adat vonatkozik, más szóval: érintett.
[19] A személyes magánszféra egésze (nemzetközi kifejezéssel privacy) tágabb fogalom, mint a személyes adatok védelme, noha a mai világban szinte mindennek van adat-vonatkozása.
[20] 36/2005. (X. 5.) AB határozat.
[21] 15/1991. (IV. 13.) AB határozat.

II. 1. Az információs önrendelkezési jog

A német alkotmánybíróság (BVG) 1983-ban hozott népszámlálás-határozata alapozta meg a személyes adatok védelméhez való jogon belül az információs önrendelkezés logikáját. Az alkotmányellenesnek nyilvánított népszámlálásról szóló törvény rendelkezései közt szerepelt, hogy az állampolgárok azonosító adatain kívül a foglalkozási, munkahelyi és lakóhelyi adatait is fel kellett volna mérni. A személyes adatok összekapcsolhatóságából és továbbíthatóságából adódó alapjogsérelem veszélyét azzal a jogtechnikai eszközzel oldotta fel a BVG, hogy az egyén kezébe adta „azt a jogot, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról",[22] vagyis az adatvédelem fundamentumaként határozta meg az információs önrendelkezést. Rögzítette, hogy az önrendelkezés kényszerű közérdekből korlátozható, valamint megfogalmazta a célhoz kötöttség elvét, a tájékoztatáshoz való jogot, továbbá a garanciális eljárás részeként az adatalany felvilágosításhoz való jogáról és – amennyiben az adatkezelés célja teljesült – az adattörlés kötelezettségéről is szólt.[23]

Az adatvédelmi jog BVG szerinti értelmezése nagy hatással volt a nemzetközi alapjogfelfogásra. A magyar Alkotmánybíróság a 15/1991. (IV. 13.) AB határozatával átemelte a magyar alkotmányjogba a német mintát.[24] Az Alkotmánybíróság értelmezésében a személyes adatok védelméhez való jog immanens része az információs önrendelkezési jog, amely alapján a főszabály az, hogy az érintett előzetes beleegyezése szükséges bármiféle adatkezeléshez, kivételesen azonban törvény is elrendelheti a személyes adatok kiadását, de csakis alkotmányos keretek között, mert ez korlátozza az információs önrendelkezési jogot. A törvényi jogalapú adatkezelés úgy történhet alkotmányosan, ha az a szükségességi-arányossági tesztnek megfelel.[25] Az önrendelkezés így erős jogvédelmi eszköz (volt),[26] amelyet az egyén a kezébe kapott, hogy részt vegyen személyes adatai alkotmányosan történő kezelésének biztosításában.

Az Alkotmánybíróság értelmezésében az információs önrendelkezési jog két alappillére, egyben konjunktív feltétele a célhoz kötöttség, illetve az adattovábbítás és az adatok nyilvánosságra hozatalának korlátozása.[27] A célhoz kötöttség a legerősebb garanciája az alapjog érvényesülésének, mert rögzíti az előre meghatározott, jogszerű, bejelentett és

[22] BVerfGE 65, 1 – Volkszählung (1983).
[23] Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése c. PhD dolgozata. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, 2009. 25-28. o.
[24] Uo. 27. o.
[25] 15/1991. (IV. 13.) AB határozat.
[26] A későbbi fejezetekben éppen az információs önrendelkezési jog válságáról írok.
[27] 15/1991. (IV. 13.) AB határozat.

közhitelűen rögzített cél nélküli adatkezelés alkotmányellenességét. Ez a szabály az adatkezelés minden egyes szakaszára mérvadó. Az érintettet adatai felhasználásának céljáról megfelelően kell tájékoztatni, hogy megfontolt döntést tudjon hozni adatainak kiadásáról, valamint arról is tudnia kell, hogyan tudja jogait érvényesíteni, ha a személyesadat-kezelés során eltérnének a céltól, s azt jogszerűtlenül használnák fel.[28] Ha az adatkezelés során új cél fogalmazódik meg, arról is megfelelően kell tájékoztatni az érintettet. Az alkotmánybírák levonják a következtetést ebből: „a meghatározott cél nélküli, „készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes".[29]

További alapfeltétele az információs önrendelkezésnek az adattovábbítás és az adatok nyilvánosságra hozatalának korlátozása. Adattovábbítás alatt szűkebben lehet érteni az adat adatkezelő[30] általi kiadását *meghatározott* harmadik személynek, illetve tágabban az adatok nyilvánosságra hozatala azt jelenti, hogy *bármely* harmadik személy számára hozzáférhetővé teszi az adatkezelő a személyes adatot. Harmadik személy csak akkor jogosult tudomást szerezni az adatról, ha „minden egyes adat vonatkozásában az adattovábbítást megengedő összes feltétel teljesült,"[31] vagyis az célhoz kötött, továbbá vagy konkrét törvényi felhatalmazással rendelkezik a harmadik személy, vagy az érintett hozzájárulását beszerezte.[32] Látható tehát, hogy e két, egymásból következő, alapvető fontosságú, sajátos garancia az információs önrendelkezési jog testőre, hiszen, ha minden feltétel teljesül az adatkezelés során, elméletileg az érintett személyes adatai kellőképp védve vannak.

II. 2. Az adatvédelem jogi szabályozásának tendenciái

E fejezetben az adatvédelem alkotmányos alapjaihoz mérten vizsgálom a különböző jogi megfogalmazásokat. Kérdés, hogy az Alkotmánybíróság 1991-ben fikciót fogalmazott-e meg az információs önrendelkezési jog alapjogi értelmezésekor. Mennyiben tartható még az általuk lefektetett alkotmányos idea? A magyar és európai uniós adatvédelmi joggyakorlat áttekintésével szemléltetem, hogy az origótól, vagyis a 15/1991. (IV. 13) AB határozattól

[28] 15/1991. (IV. 13.) AB határozat.
[29] 15/1991. (IV. 13.) AB határozat.
[30] A 15/1991. (IV. 13.) AB határozatban még az „adatfeldolgozó" kifejezést használják, de a zavartalanabb érthetőség érdekében én a hatályos Infotv. szerinti „adatkezelő" szót használom a szövegben, mert a hatályos jogi dogmatikának így lesz megfeleltethető. A 15/1991. (IV. 13.) AB határozat szerint „aki az adatfeldolgozó számára annak megbízásából – rendszerint hivatás- vagy üzletszerűen – végzi az adatfeldolgozás szorosan vett fizikai vagy számítástechnikai teendőit, nem számít "adatfeldolgozónak"(...)." Vagyis a hatályos jog adatfeldolgozó-fogalmára mondta ki az Alkotmánybíróság 1991-ben, hogy ő nem adatfeldolgozó.
[31] 15/1991. (IV. 13.) AB határozat.
[32] 15/1991. (IV. 13.) AB határozat.

mennyire tért el a jogalkotó, azaz a felvázolt követelményeket hogyan puhította fel majd' harminc év alatt. Először a magyar adatvédelmi jogi szabályozásban elért, s az erre hatással lévő mérföldköveket azonosítom, majd olyan faktorokat jelölök ki, amelyek alapján vizsgálhatók a tendenciák az adatvédelem jogi kodifikálásában és gyakorlati megvalósulásában.

A mérföldkövek kijelölésekor egy kronológiát vázolok fel, amelyben helyet kap a 15/1991. (IV. 13.) AB határozat után a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Avtv.), ezt követi a jogharmonizációs EK irányelv 1995-ből,[33] majd a 2011-es Infotv., végül a 2018. május 25-én hatályba lépett, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR),[34] s ennek keretében az Infotv. módosítása kerül fel az idővonalra. Ezekben a jogszabályokban az összehasonlításhoz szükséges faktorok a következők: a jogalap meghatározása, a célhoz kötöttség követelményének érvényesülése, ehhez kapcsolódóan az adattovábbítás korlátoltságának vizsgálata indokolt, majd szólok az egyének jogairól. Ezen kívül jelentős az intézményrendszeri változások feltérképezése, a jogvédelem szervezeti alakulása.

[33] 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 (továbbiakban: EK irányelv).

[34] Az Infotv. viszonya a GDPR-ral feltétlenül tisztázandó. A GDPR közvetlenül hatályosuló jogi aktus [Alaptörvény E) cikk (3) bekezdés], de a rendelet tárgyi hatálya nem minden adatkezelésre vonatkozik, mert a GDPR meghatároz egy pozitív hatályt [GDPR 2. cikk (1) bekezdés], s ez alól kivesz egyes adatkezeléseket, melyek esetében az Infotv. lesz irányadó [GDPR 2. cikk (2) bekezdés]. Ezek alapján a GDPR kiterjed az adatvédelmi szektorok közül az automatizált adatkezelésre (vagyis az automatizált eszköz – általában elektronikus eszköz, számítógép – útján történő adatkezelésre) és a manuális adatkezelés tekintetében a nyilvántartási célú adatkezelésre (a GDPR 4. cikk 6. pontja a nyilvántartás foglamát nagyon tágan fogalmazza meg, így arra, hogy ez valójában mit is takar, még nincs joggyakorlat). A pozitív hatály alól kivett adatkezelésekre – általában – az Infotv. hatálya terjed ki; ilyennek minősül a nem európai uniós hatáskörbe tartozó adatkezelés (pl. nemzetbiztonsági adatkezelés), a más uniós pillérre tartozó ügyek (kül-és biztonságpolitika), a természetes személyek személyes és otthoni célú adatkezelése, illetve a bűnüldözési adatkezelés – ez utóbbira irányelvi rendelkezések irányadók (a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló (EU) 2016/680 európai parlamenti és tanácsi irányelv). Mindez szükségképp azt eredményezi, hogy egy tagállamon belül több – minimum kettő – adatvédelmi rezsim van, melyek nem is függetlenek egymástól. Azon adatkezelésekre, melyekre a GDPR az irányadó, arra az Infotv. szabályait a GDPR-ban meghatározott kiegészítésekkel kell alkalmazni: a GDPR paragrafusszámra rögzíti, mely rendelkezések minősülnek együtt alkalmazandónak. A GDPR meghatároz területi hatályt is, mely innovatív elemként értékelhető (GDPR 3. cikk): a hatály kiterjed minden olyan adatkezelőre és adatfeldolgozóra, mely tevékenységi hellyel rendelkezik az Európai Unión belül, vagy ennek hiányában itt nyújt árut és szolgáltatást vagy itt megfigyeli az ittlévő embereket (pl. cookie-k).

A jogalapot vizsgálva kitűnik, hogy a 15/1991. (IV. 13.) AB határozatban lefektetett dogmatika teljesen átalakult. Fejlődésnek tekinthető, hogy különbséget tesz minden vizsgált joganyag a személyes adat és a különleges (szenzitív) adat között, utóbbit minden esetben többletvédelemmel ellátva.[35] Ugyanakkor a jogalapok köre már az Avtv.-ben tágulásnak indult, mikor a törvényen kívül – az alkotmányosságot erősen megkérdőjelezve – megjelent a helyi önkormányzati rendeletben történő alapjogkorlátozás lehetősége is. Az érdekmérlegelés a jogalkotó kötelezettsége volt tehát: törvényt – vagy önkormányzati rendeletet – alkotott, és ebben felhatalmazást adott a szükségességi-arányossági tesztnek megfelelően személyes adatok kezelésére.

A GDPR két szempontból gyökeresen megváltoztatta az önrendelkezési logikát a jogalapok tekintetében.[36] Először is kijelenthető, hogy a GDPR már nem az önrendelkezés talaján áll, mert a hozzájárulás[37] csak egy a sok jogalapból.[38] A jogalapbővülés nem minden esetben jelent feltétlenül rosszat.[39] Azonban a jogos érdek[40] is alapja lehet az adatkezelésnek, ami az addigi alapjogvédelmi sztenderdhez képest egyértelműen lerontásként értékelhető:[41] ha az adatkezelőnek jogos érdekében áll, akkor – az információs önrendelkezést sértve – elméletileg jogszerűen kezelhet személyes adatokat. Ezzel kapcsolatban a GDPR második fő nézőpontváltása az, hogy az érdekmérlegelési teher átkerült a jogalkotóról az adatkezelőre, vagyis ő maga határozhatja meg, mi minősül jogos érdeknek. Ebben az esetben a szükségességi-arányossági teszt alkalmazásakor már nem alapjog vagy alkotmányos érték áll tehát alapjoggal szemben, hanem egy másik magánszemély érdeke. Elég nehéz elképzelni, hogy létezik olyan magánérdek, ami miatt alkotmányosan megengedhető lenne egy alapjog korlátozása. Ezért a

[35] Avtv. 3. § (2) bek., EK irányelv 8. cikk, Infotv. 5. § (2) bek., GDPR 9. cikk (1)-(2) bek.
[36] Igaz, már az EK irányelv is szinte ugyanazokat a jogalapokat sorolta fel, mint a GDPR, ám míg előbbi a nemzeti jogba jogszabályban átültetendő jogharmonizációs célzatú norma, addig a GDPR egy rendelet, mely közvetlenül és hatálybalépését követően azonnali hatállyal alkalmazandó uniós jogi aktus.
[37] GDPR 6. cikk (1) bek. a) pont.
[38] A hozzájárulás jogalapja mellett szerepel a vélelmezett hozzájárulás, vagyis a szerződés teljesítése érdekében történő adatkezelés [GDPR 6. cikk (1) bek. b) pont]. Míg a jogi kötelezettség teljesítésén alapuló adatkezelés nem csak közhatalmi szervek általi kötelezést jelenthet, addig a közhatalmi tevékenység érdekében végzett adatkezelés csak közhatalmi jogosítványon alapulhat. [GDPR 6. cikk (1) bek. c) és e) pont]. A létfontosságú érdek vészhelyzetek, például életek megmentése esetén kaphat fontos szerepet [GDPR 6. cikk (1) bek. d) pont].
[39] Nem múlhat minden adatkezelés az érintett hozzájárulásán, és a jogalkotó válláról is levették a terhet, hogy folyamatosan törvényben (önkormányzati rendeletben) korlátozza az információs önrendelkezési jogot a szükségességi-arányossági tesztnek megfelelően.
[40] GDPR 6. cikk (1) bek. f) pont. Egyébként már az EK irányelvben [7. cikk f) pont] és a 2011-es Infotv. 6. §-ában is megjelent a jogos érdek.
[41] "Olyan nagy" lerontás azonban mégsem történt, mert a GDPR kivételként rögzíti a közhatalmi szektort a jogos érdek alól, így e jogalap csak magánszemélyek egymás közti adatkezelésére vonatkoztatható.

legitim cél tesztjénél lényegében meg is bukik az alapjogkorlátozás alkotmányossága, a jogos érdek nem tekinthető alkotmányos jogalapnak.

További aggodalomra ad okot a rapid módon módosított Infotv., mely a hagyományos dogmatikához képest szintén jelentős eltérést mutat. Úgy tűnik, hogy az eddig kivételként meghatározott törvényben – vagy önkormányzati rendeletben – elrendelt (kötelező) adatkezelés lett a főszabály.[42] Ennek hiányában beszélhetünk csak a hozzájárulásról mint jogalapról, ami egyébként már nem „tiszta" hozzájárulás, ugyanis azt az érintett csak az adatkezelő törvényben meghatározott feladatainak ellátásához szükséges adatkezelésnél adhatja meg.[43] E szerint nem tudok olyan adatkezeléshez hozzájárulni, melyre az adatkezelőnek nincs szüksége. Ez nyilvánvalóan korlátozza az önrendelkezést, de úgy is megközelíthető, hogy a törvény beépít egy plusz feltételt a hozzájárulás jogalapjába, ami implicite célhoz kötöttségként is értékelhető. További jogalap az adatkezelésre a létfontosságú érdek,[44] valamint az, mikor az érintett kifejezetten nyilvánosságra hozta a személyes adatait[45] (például közszereplés, telefonkönyv, bejegyzések olyan társas oldalakon, mint a Facebook). E két utóbbi jogalap alapján történő adatkezelés csak akkor tekinthető jogszerűnek, ha az a szükségességi-arányossági tesztnek megfelel.

A célhoz kötöttség megfogalmazásának tekintetében nem történtek jelentős változások, sőt, ha összeolvassuk az AB dogmatikáját a hatályos Infotv.-nyel, ugyanazt a definíciót kapjuk.[46] Az információs önrendelkezés másik alapvető garanciájánál, az adattovábbítás korlátozásánál ez azonban már nem mondható el. Az adattovábbítást a 15/1991. (IV. 13.) AB határozat célhoz köti, és jogszerűségéhez törvényi felhatalmazás vagy az érintett hozzájárulása szükséges. Ezt az Avtv. még követte a belföldi és külföldi adattovábbítás tekintetében is,[47] ám az EK irányelv már behozott a harmadik országba[48] történő adattovábbítás esetén egy új kritériumot, a megfelelő védelmi szintet.[49] A megfelelő védelmi szint hiányában csak meghatározott feltételek mellett[50] (többek között az érintett hozzájárulásával) történhetett meg a személyes

[42] Infotv. 5. § (1) bekezdés. Felmerül a kérdés, hogy a magánadatkezelők esetében hogyan történhet meg a jogalap kiválasztása, hiszen esetükben nincs törvényben meghatározott feladat, vagyis elméletileg a módosított Infotv. szerint az érintett nem adhat hozzájárulást.
[43] Infotv. 5. § (1) bek. b) pont.
[44] Infotv. 5. § (1) bek. c) pont.
[45] Infotv. 5. § (1) bek. d) pont.
[46] Infotv. 4. § (1)-(2) bek.: „Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának", és a szükségességi-arányossági tesztnek.
[47] Avtv. 8-9. §.
[48] Minden nem EGT-állam (bővebben: Infotv. 3. § 23-24. pont).
[49] EK irányelv 25. cikk.
[50] EK irányelv 26. cikk.

adatok harmadik országba való továbbítása. Idáig tehát érvényesülhettek az önrendelkezési elemek az adattovábbítás korlátozása kapcsán. Ám az Infotv. 2011-ben elkezdte az adatkezelőre róni a terheket, amit aztán a GDPR és a módosított Infotv. nyomatékosított. Harmadik országba történő adattovábbítás esetén a megfelelő védelmi szint[51] és a megfelelő garanciák[52] szigorú alkalmazása is feltétel. A tételesen meghatározott védelmi és garanciális faktorok az önrendelkezés rovására az adatbiztonságra helyezték a hangsúlyt, és az adatkezelő felelőssége is jelentősen megnőtt.[53] Emellett a megfelelő garanciák hiánya esetén is számos jogalapot biztosít a hatályos jog az adattovábbításra,[54] amelyek közül csak a hozzájárulás biztosítja az önrendelkezést az érintett számára, a többi esetén az adatkezelő többletkötelezettségei tűnnek ki.

Mindamellett az egyének jogai körében bővülő tendenciák is felfedezhetők.[55] A GDPR-ban kifejezetten nagy hangsúlyt kapnak az egyes jogosultságok,[56] s megjelennek újabb jogok is.[57] Az erősödő részvételi jogosultságok valamennyire kiegyensúlyozzák az önrendelkezési jog jelentőségének csökkenését, vagyis a jogalapoknál az egyéntől elvett önrendelkezés itt, az egyéni jogosultságoknál helyrebillenhet.

A szervezeti változások rendkívül jelentősek voltak. Az Avtv. alapján felállított adatvédelmi biztos[58] ombudsman típusú, az Országgyűlésnek alárendelt szerv volt.[59] Később a biztos a jogharmonizáció miatt hatósági jogköröket kapott.[60] Az adatvédelmi biztos 2005-től tehát mint

[51] A megfelelő védelmi szint biztosítása a Bizottság kiemelt feladata (GDPR 45. cikk).
[52] GDPR 46. cikk.
[53] Például kötelező erejű és kikényszeríthető magatartási kódex szerint kell eljárnia [GDPR 46. cikk (1) bek. e) pont], vagy a GDPR 35. cikk (1) bekezdése alapján adatvédelmi kockázatelemzés és hatásvizsgálat szükséges olyan adatkezelések esetében, ahol feltételezhető, hogy magas kockázattal jár az adatkezelés (pl. gyermekek esetében, vagy ha sok embert érint). Ezt az adatkezelőnek dokumentálni kell, egyeztetnie kell az adatvédelmi hatósággal, hogy egyáltalán megkezdhető-e az adatkezelés [GDPR 36. cikk (1) bek.].
[54] GDPR 49. cikk (1) bekezdés: ilyen alap lehet az érintett hozzájárulása és vélelmezett hozzájárulása (kivétel: közhatalmi szervek tevékenysége esetén), uniós vagy tagállami jog által elismert fontos közérdek, jogérvényesítés vagy jogvédelem, létfontosságú érdek cselekvőképesség esetén, és a nyilvánosan hozzáférhető nyilvántartás. Ezeken kívül egyedi esetekben is alapot nyújt a rendelet az adattovábbításra.
[55] A tájékoztatáshoz való jog, a helyesbítéshez való jog, a törléshez való jog már az Avtv.-ben is jelen volt, ehhez csatlakozott az EK irányelvvel a tiltakozáshoz való jog és a zároláshoz való jog, melyeket az Infotv. is beépített, s ezek ma is hatályos egyéni jogosultságként vannak nevesítve.
[56] Például a tájékoztatáshoz való jog is erősödik, mert az adatalanynak a tájékoztatást „tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva" kell megkapnia [GDPR 12. cikk (1) bekezdés], ami eddig nem volt jellemző. A törléshez való jog (GDPR 17. cikk) is cizelláltabb értelmezést kap, de kérdés, és ezen jogosultság kritikus pontja maga a megvalósíthatóság, vagyis, hogy az elfeledtetés technológiailag végrehajtható-e.
[57] Ilyen innovatív elem például az adathordozhatósághoz való jog (GDPR 20. cikk).
[58] Avtv. 23-27. §.
[59] Sólyom László: Adatvédelem és személyiségi jog. Világosság, 1988. január. 57. o.
[60] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról szóló 2005. évi XIX. törvény értelmében az Avtv. 25. § (4) bekezdése sajátos, hatósági jogköröket rögzített: „az adatvédelmi biztos határozatban elrendelheti a jogosulatlanul kezelt adatok zárolását, törlését, vagy

kvázi hatóság léphetett fel, ami azt is jelentheti, hogy megszűnt ombudsmannak lenni, hiszen az ombudsmannak hatósági jogkörei nincsenek.[61] Ebből fakadóan intézményi és szerepfelfogási feszültségek is keletkeztek, majd az alkotmányos változások keretében az országgyűlési biztos megszűnt, helyébe hatóság lépett:[62] az autonóm államigazgatási szervként működő[63] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH).

Összességében a hagyományos információs önrendelkezési jogi dogmatika eróziója figyelhető meg a jogi szabályozásban. A szabályozás immár nem alapjogi logikát követ.[64] A GDPR-ban vannak ugyan önrendelkezési jogot biztosító elemek, de nem ez a vezérelv, hanem az adatkezelő elszámoltathatósága. A személyes adatokat kezelni kell, mert anélkül nem működne a gazdaság, a társadalom. Az egyén így háttérbe szorult, ellenben hatalmas hangsúlyt kapott az adatbiztonság, és ezzel együtt nőtt az adatkezelő kötelezettsége, felelőssége. Az adatvédelem európai tendenciáit vizsgálva jól kirajzolódik egyfajta őrségváltás: az információs önrendelkezés logikájában hangsúlyosan az érintett kezében volt a fegyver, mellyel védi személyes adatait és a magánszféráját, ám a hatályos jog az adatkezelőre telepíti a védelmi terhet. A védelem irányának megfordulása jelentősen csorbítja az egyén önrendelkezését. Az 1991-ben lefektetett alkotmányos alapokhoz képest ez végső soron az alapjogvédelmi garanciák gyengüléseként értékelhető.

II. 3. Az adatvédelem horizontális hatálya

A klasszikus alapjogi jogviszony állam és egyén között áll fenn. Azonban a személyes adatok védelméhez való jog tekintetében – a magyar és európai alapjogi gondolkodás szerint – kivétel tehető: magánszemély és magánszemély közt is létesülhet alapjogi jogviszony, de csak akkor, ha a két államon kívüli jogalany közt aszimmetrikus hatalmi elosztás van.[65] A jogrendszer az alapjogok közvetlen horizontális hatályával válaszol erre a helyzetre.[66] A személyes adatok védelméhez való jog kötelezettje így magánjogi jogalany is lehet. A horizontális kötelezés

megsemmisítését, megtilthatja a jogosulatlan adatkezelést vagy adatfeldolgozást, továbbá felfüggesztheti az adatok külföldre továbbítását. A határozat ellen (...) jogorvoslatnak nincs helye."

[61] Majtényi László: Az adatvédelmi ombudsmann – az adatvédelmi törvényhozás. Magyar Közigazgatás, 8. sz. 1990. 30. o.

[62] Infotv. V-VI. Fejezet.

[63] Infotv. 38. § (1) bek.

[64] A GDPR nem tekinthető alapjogi jogszabálynak, mert nem minden hatálya alá tartozó jogviszony alapjogi jogviszony. Bizonyos esetekben szolgálhatja az alapjog érvényesülését, de egyébként az egységes piacot szolgálja.

[65] Az alapjogi jogviszony deklarálásához tehát mindenképp szükséges, hogy a jogalanyok közt kialakuljon a hatalmi erőeltolódás, így az egyik fél a másikkal szemben gyengébbnek kell, hogy minősüljön. Ha viszont a két fél egyenlő hatalmi pozícióban van, nem beszélhetünk alapjogi jogviszonyról.

[66] Halmai-Tóth, 2008. 98-102. o., Gárdos-Orosz Fruzsina: Az emberi jogok alkalmazásának lehetőségei a rendes bíróságokon különös tekintettel a magánjogi jogvitákra. Doktori értekezés, Győr, 2010. 91-98. o.

magyarázatául[67] szolgál az a körülmény, hogy az egyénnel szembeni alapjogsértést az államon, a közhatalom képviselőin kívül gazdálkodó vagy egyéb szervezetek, sőt magánszemélyek is véghez vihetnek,[68] amennyiben olyan információs többlettel rendelkeznek az egyénről, ami az egyént kiszolgáltatottá teszi velük szemben.

Az információs társadalomban a hatalmi viszonyokat az adatgazdagok és adatszegények közti választóvonal határozza meg, és e viszonyok dinamikusan változnak. Információs hatalomnak nevezzük azt a speciális hatalmi viszonyrendszert, amelyben a hatalmi pozícióban elhelyezkedő féllel szemben a többiek – az ismeretek aszimmetrikus allokációja miatt – védtelenek.[69] Az ismeretet birtokló és az ismerethiányban szenvedő fél közt vertikális erőeltolódás figyelhető meg, így a hatalmat birtokló a hatalmi eszközeit – így a megfigyelést, és ennek lehetőségét, az elrejtőzést, vagyis a hatalmi pozícióban lévő megfigyelhetetlenségét, illetve a hatalmasság által birtokolt információs monopóliumot – bevetve gyakorolja hatalmát az alávetettek felett.[70] Az aszimmetrikus hatalmi viszonyból következő kiszolgáltatottság előrevetíti az egyén cselekvési és döntési szabadságának korlátozását.

Az adatfeldolgozási technológia jelenlegi szintjén *bárki* gyakorolhat információs hatalmi fölényt mások felett. Vagyis már nemcsak a klasszikus hatalmi ágak mint közhatalommal felruházott állami szervek képesek az egyéneket hatalmuk alá vonni, hanem egyes magánjogi jogalanyok is rendelkeznek ilyesfajta fegyverkészlettel. Az információs hatalmak befolyása túlnyúlik a nemzeti jog által szabályozott területeken és a nemzeti szintű intézmények jogérvényesítési lehetőségein.[71] Ezt mi sem bizonyítja jobban, mint a szakirodalom által „Little Brothers"-ként, kis testvérekként emlegetett információs magánhatalmak kiemelt pozíciója.[72] A Google, az Amazon, a Facebook, az Apple, a mobilszolgáltatók, a bankok, a biztosítók stb. olyan transznacionális és multinacionális vállalatok, amelyek közhatalmi eszközök megléte nélkül is képesek ügyfeleiken „uralkodni", akár közfunkciókat ellátni, ám ezt mind az állam

[67] Érdekes gondolat, hogy a közvetlen horizontális hatály mögött nincs igazolás, csak utólagos magyarázat. A magyar alapjogi szemléletben 1992 óta létezik az adatvédelem horizontális kikényszeríthetősége, mert benne volt az Avtv.-ben, azonban soha nem tettük fel a kérdést, hogy miért. Lényegében a kiterjesztés mögé tettük az igazolást (ti. információs hatalmak miatt), de ez nem jelenti azt, hogy az információs hatalmi helyzetből következik a kiterjesztés. Felmerül a kérdés tehát, hogy van-e igazolásunk azt mondani, hogy a személyes adatok védelméhez való jog magánjogi jogalannyal szemben is kikényszeríthető. Én úgy gondolom, hogy a válasz igen, és ezt a fejezetben írtakkal bizonyítom.

[68] Chronowski Nóra: Üzlet és emberi jogok – nemzetközi törekvések és alkotmányjogi korlátok. In: JURA, 2013. 2. szám, Pécs, 9. o. https://jura.ajk.pte.hu/JURA_2013_2.pdf.

[69] Szabó Máté: Az információs hatalom alkotmányos korlátai, Miskolc, 2012. 13. o.

[70] Uo. 13-14. o., 15-23. o.

[71] Éppen a joghatóság kérdésére próbálnak választ adni a nemzetközi jogi dokumentumok.

[72] Ennek előzménye az államra metaforaként használt orwelli Big Brother, vagyis a Nagy Testvér, aki mindent lát, de őt senki sem látja.

keretein kívül teszik. E magáncégek kezében immár államszintű hatalom összpontosul, hiszen ők rendelkeznek az információs monopóliummal, többet tudnak rólunk, mint maga az állam.[73] Emellett speciális kérdést vet fel, mikor az állam összefog a kis testvérekkel: egyrészt kiszervezi az állami adatkezelési feladatokat, másrészt együttműködik különféle magánszervezetekkel, biztosítókkal stb., így az egyén egy információs hatalmi koalícióval találhatja magát szemben.

Alkotmányosan hogyan ítélhetők meg tehát az információs hatalmak? Egyes nézetek szerint – amelyekkel mélységesen egyetértek – az információs hatalom már nemcsak hatalomgyakorlási instrumentum, hanem egy különálló, közhatalomtól is levált hatalmi ág.[74] A Montesquieu-féle hatalommegosztás[75] már Bibó István szerint is meghaladottá vált.[76] Bibó leírása alapján a hatalomkoncentráció új veszélyei a bürokráciában jelennek meg. A bürokrácia mindenhatósága két társadalmi réteget különít el: a szűk nagyon képzett, szakértő réteget és az annál sokkal népesebb képzetlen átlagot. Utóbbi – lustaságából adódóan – fejet hajt az őket irányító, túlracionalizált nagyüzem szervezőinek. Így emberi szabadságukat feladván utat engednek az önkény eluralkodásának.[77] Ezt vizionálja Bibó, ugyanis akkoriban még csak körvonalazódott a probléma ilyen szempontból való megközelítésének létjogosultsága. Ma viszont alappal állítható, hogy egy újfajta, digitális bürokratizálódás folyamatába léptünk. Az erőviszonyok újrarendeződése figyelhető meg, amelyben a fejlődés irányainak meghatározása, az adatok jelentős része és a feldolgozói tudás és kapacitás szinte kizárólag a fent említett magánvállalatok kezében van. Ez azt is jelenti, hogy az állam funkcióit nagy részben átvették a nem állami szervezetek, így azok a nemzetállamot egyre inkább destabilizálják, zárójelbe teszik.

A társadalom felismerte, hogy az egyén szabadságára az államon kívüli szereplők, a kis testvérek is ugyanolyan – sőt, bizonyos esetekben nagyobb – függőséget jelentenek, mint az állami szervek.[78] Mindez megalapozza a fékek és ellensúlyok intézményeinek közhatalom határain túlmutató létjogosultságát. Először is egyre inkább szükségessé válik a kis testvérek

[73] Például azt, hogy hol vagyunk, mennyit alszunk, mit eszünk, kikkel beszélünk, miket vásárolunk, hogy szolgál az egészségünk; lényegében mindannyian a kis testvérek által birtokolt adatokká konvertálódunk.
[74] Szabó, 2012. 24. o.
[75] Charles Montesquieu: A törvények szelleméről. Budapest, Osiris–Attraktor, 2000. 245 o.
[76] Bibó István: Az államhatalmak elválasztása egykor és most. In: Válogatott tanulmányok, Második kötet, 1947. http://mek.oszk.hu/02000/02043/html/290.html.
[77] Uo.
[78] Szabó, 2012. 26-27. o.

átláthatóságának megkövetelése. Ez eredetileg az állammal szemben került megfogalmazásra,[79] de a közhatalmon kívüli szereplők államszintű hatalmának kibontakozása indokolttá tette a velük szembeni transzparencia igényét is.[80] Az átláthatóság követelményén túl szükség van az információs hatalmi helyzetet korlátozó jogi eszközökre, így például az információs szabadságjogok az információs hatalmi helyzet ellensúlyaként funkcionálnak. Az információs hatalommegosztás fogalma is megjelenik, amely alatt azokat a jogi eszközöket kell érteni, amelyek gátat szabnak az információs hatalom egy kézben történő összpontosulásának.[81] Erre példaként említhető a személyes adatok védelméhez való jog alapjogként történő elismerése. Az adatvédelmi szabályok megakadályozzák, hogy az információ egy kézben koncentrálódjon, és ezzel olyan hatalmat gyakoroljanak az egyének felett, ami kiüresíti az egyéni autonómiát – legalábbis a hagyományos dogmatika ezt feltételezi.

Az információs önrendelkezési jog alapjogi deklarációja rendkívül jelentős esemény az adatvédelem történetében, azonban nem tekinthető végső lépésnek.[82] A cél az, hogy ne csak elméletben létezzen az információs önrendelkezés, hanem a gyakorlatban is megvalósulhasson, hiszen ez az előfeltétele annak, hogy saját életünket szabad döntéseinkkel, felelősen alakíthassuk.[83] Az önrendelkezési logika alapvető eleme az érintett hozzájárulása. Tekintve, hogy az adatkezelő – alapjogi kötelezettként – gazdasági és információs erőfölényben van, az adatalany a kedvezőtlenebb alkupozíciójából hajlamos minden esetben megadni a hozzájárulást. Így a hozzájárulás feltételei, vagyis annak önkéntessége,[84] határozottsága[85] és a megfelelő tájékoztatáson való alapulása[86] is megkérdőjelezhető. Ez azt eredményezi, hogy az információs önrendelkezés már kevésbé minősül a magánszférát védő mechanizmusnak.[87] Az

[79] Az átlátható állam, átláthatatlan polgár eszményét az Alkotmánybíróság kényszerítette ki az információs hatalom megosztásáról szóló határozataival [pl. 15/1991. (IV. 13.) AB határozat].
[80] Szabó, 2012. 25. o.
[81] Uo. 9. o.
[82] Jóri, 2009. 38. o.
[83] Will Democracy Survive Big Data and Artificial Intelligence? In: Towards Digital Enlightenment. Essays on the Dark and Light Sides of the Digital Revolution. Szerk: Dirk Helbing. Springer, 2018. 78. o.
[84] Vagyis az, hogy az az érintett szabad és befolyásmentes akaratán, saját döntésén alapul, és létezik tényleges választási lehetőség bármiféle negatív jogkövetkezmény nélkül. (A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv 29. cikke szerint létrehozott Adatvédelmi Munkacsoportnak [Munkacsoport] a hozzájárulás fogalom-meghatározásáról szóló 15/2011. számú véleménye [Vélemény] 12. o.)
[85] Az érintett félreérthetetlen beleegyezését jelenti az adatkezelésbe, azaz egy konkrétan meghatározott adatkezeléshez, adatkezelési művelet(ek)hez járul hozzá (és nem egy blanketta elfogadó nyilatkozatot ír alá) tevékeny módon, igazolhatóan. (Vélemény 34. o.)
[86] Azt feltételezi, hogy az érintett a jogairól és az adatkezelés következményeiről teljes és reális képet kapott az adatkezelőtől. Ehhez egyszerű, szakzsargon használata nélküli, érthető szöveg szükséges, melyet az átlagember is el tud érni közvetlenül (az nem elég, hogy az információ „valahol elérhető"). A tájékoztatásnak jól láthatónak, feltűnőnek és minden részletre kiterjedőnek kell lennie. (Vélemény 21. o.)
[87] Jóri, 2009. 38-39. o.

új technológiáknak – a Big Data jelenségnek is – köszönhetően egyes nézetek szerint a magánszféránk már egyébként is elillant.[88] Ez valóban így lenne? Pontosan mivel áll ma szemben az egyén, s beszűkült – vagy nem létező – magánszférája?

III. Big Data jelenség

A Big Data jelenség egy 2014-es NAIH nyilatkozat[89] szerint az adatot új szemszögből közelíti meg, a segítségével olyan információkat nyerhetünk ki a hatalmas adatmennyiségből, amelyekhez korábban nem, vagy csak igen nehezen lehetett hozzáférni. A Big Data jelenséget az alapozza meg, hogy az információs társadalomban szinte már mindennek[90] azonnal (valós időben)[91] digitális nyoma marad, vagyis így mérhetetlen adatmennyiség[92] jön létre nap mint nap. De nem a méret a lényeg, hanem a korlátlan növekedési képesség és az adatelemzés. A Big Data a generált adathalmazokat összekapcsolja, s ezáltal olyan következtetések és predikciók előtt nyitja meg a kaput, amelyekkel akár beleláthatunk az emberek legbelsőbb gondolataiba is.[93] A Big Data olyan, eddig nem ismert módszereket, algoritmusokat alkalmaz az adatok kezelésénél, amelyek lehetővé teszik az egymástól szinte teljesen különböző adatállományok közti összefüggések vizsgálatát, az adatok újrafelhasználását. Az adatokat úgy tudja összekötni, rendszerezni, hogy ez alapján akár jövőbeli eseményeket, tevékenységeket is képes előre jelezni, ami kétségtelenül a technológiában rejlő hatalmas potenciál – s egyben hatalmas veszélyforrás és kihívás az adatvédelmi jog számára.

III. 1. A Big Data és a pszichometria

Hogy kirajzolódhasson a Big Data által okozott paradigmaváltás az adatkezelés terén, célszerű valós példával[94] megvilágítani, hogy a Big Data alapú elemzések milyen szociálpszichológiai

[88] „Már most sincs magánszférájuk. Lépjenek túl ezen." („You already have zero privacy – get over it.") – fogalmazott Scott McNealy, a Sun Microsystems vezérigazgatója 1999-ben. Idézi Schwartz 2002. 77. o.

[89] Nyilatkozat a Nemzetközi Adatvédelmi Biztosítási Konferenciák keretében a Big Data-ról, 2014. https://www.naih.hu/files/Nyilatkozat-Big-Data.pdf.

[90] A Big Data 3 V-vel leírható jellemzői közül ez a „Variety": az összes online és offline tevékenység növeli az ember digitális lábnyomát (pl. online aktivitás monitorozása, CCTV, GPS, IoT [Internet of Things], banki tranzakciók, stb.).

[91] A Big Data 3 V jellemzői közül ezt hívják „Velocity"-nek.

[92] Ezt szokták a Big Data-ra jellemző 3 V-ből a „Volume"-ként emlegetni, miszerint az addig felhasználhatatlan adatok is hirtelen felhasználhatókká válhatnak, ha minél több adat áll rendelkezésre, mert így a korreláció esélye nő. A mennyiség – nem a minőség - határozza meg, hogy a begyűjtött adatok információvá válhatnak-e vagy sem.

[93] Ződi Zsolt: Privacy és a Big Data, Fundamentum, 2017. 1-2. szám, 19. o. http://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf.

[94] Hannes Grassegger, Mikael Krogerus: The Data That Turned the World Upside Down. How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election, Motherboard 2017. frissítve: 2018. március 17. https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.

hatásokat képesek előidézni. Mindenekelőtt elengedhetetlen az OCEAN modell megértése. A pszichometria a pszichológia adatok által vezérelt ágazata, mely pszichológiai jellemvonásokat, például a személyiséget méri. A Big Five öt személyiség-típust jelöl: nyitottág (*openness*), lelkiismeretesség (*conscientiousness*), extrovertáltság (*extroversion*), alkalmazkodó képesség (*agreeableness*) és érzelmi labilitás (*neuroticism*). Ezen dimenziók alapján összeállítható egy viszonylag pontos értékelés az elemzett alany személyiségéről. A Big Data megjelenése előtt a módszer nehézsége az adatok begyűjtése volt, hiszen általában igen hosszú és bonyolult személyiségi teszteket kellett kitöltetni a résztvevőkkel, hogy legyen miből dolgozni. Azonban a Cambridge-i Egyetem Pszichometria Központjában kidolgoztak egy rendkívül hatékony és gyors metódust, amellyel a személyiségek kielemezhetők. Egy alkalmazást fejlesztettek, mely a MyPersonality nevet kapta.[95] A felhasználók különböző pszichometriai kérdőíveket tölthettek ki az egyre népszerűbbé váló applikációban, a kiértékelés során kaptak magukról egy személyiség-profilt (egyéni Big Five értékeket), majd hozzájárulásos alapon megoszthatták a kutatókkal a Facebook-profil adataikat.

A pszichometriai értékeket a Facebook-profilokkal összekapcsolva rendkívül megbízható következtetéseket lehet levonni, főleg, ha több ezer individuális adatpontot kombinálnak a Big Data segítségével. Például 2012-ben Kosinski bebizonyította, hogy átlagosan 68 Facebook like alapján 95 %-os pontossággal megállapítható a felhasználó bőrszíne, 88 %-os pontossággal a szexuális orientációja és 85 %-os pontossággal az, hogy a Demokrata, vagy a Republikánus Párt nézeteit osztja.[96] 70 like alapján többet tudtak az adott felhasználóról, mint annak barátai, 150 like után a szülőket, és 300 like után az illető partnerét is beelőzték. Ennél több like begyűjtésével pedig jobban ismerhették a felhasználót, mint ő saját magát.[97] Nemcsak like-okról van azonban szó. A kutatócsoport már ki tudta elemezni a Big Five értékeket csupán az alapján, hogy a felhasználónak hány profilképe vagy ismerőse van.[98] A Facebook platformján kívül számos online tevékenység által feltérképezhető az egyén személyisége: Google-keresések, blogbejegyzések, Twitter üzenetek, Instagramon megosztott képek stb. Ezen felül az offline tevékenységek is indikátornak számítanak a profilalkotás során: a mobiltelefonban

[95] Yoram Bachrach, Michal Kosinski, Thore Graepel, Pushmeet Kohli, David Stillwell: Personality and Patterns of Facebook Usage – Proceedings of the ACM Web Science Conference, 2012. 36-44. o. http://www.alanuk.com/wp-content/uploads/attachments/Personality_and_Patterns_of_Facebook_Usage.pdf.
[96] Michal Kosinski, David Stillwell, Thore Graepel: Private traits and attributes are predictable from digital records of human behavior. In: Proceedings of the National Academy of Sciences, vol. 110, no. 15., 2013. április 9. 5802-5805. o. http://www.pnas.org/content/pnas/110/15/5802.full.pdf.
[97] Wu Youyou, Michal Kosinski, David Stillwell: Computer-based personality judgments are more accurate than those made by humans. In: Proceedings of the National Academy of Sciences, vol. 112, no. 4., 2015. január 27. 1037-1040. o. http://www.pnas.org/content/pnas/112/4/1036.full.pdf.
[98] Yoram Bachrach, Michal Kosinski, Thore Graepel, Pushmeet Kohli, David Stillwell, 2012. 39. o.

lévő mozgásérzékelő méri, milyen gyorsan és milyen messzire mozgunk, hol vagyunk, hová utazunk.

Fontos kiemelni, hogy a korábbi statisztikai módszerekkel ellentétben a Big Data már nem az egyének véleményeit kérdezi meg, hanem a viselkedésüket monitorozza, és nem érdekli a rendszert, hogy mi miért történik, csak gyűjti az adatokat. Ehhez társul a prediktív adatelemzés: a profilokat felállítva rendkívül pontos előrejelzések tehetők az érintett jövőbeli döntéseivel kapcsolatban, vagyis az egyén digitális lábnyoma már előre konstruált, és tudják, hogy bele fog lépni, mert tudják előre, mit fog csinálni.

Hasznos célokra is fordítható lenne a módszer,[99] de kérdés, hogy mennyire van összhangban az egyének önrendelkezésével. Ezen túlmenően: mi történne akkor, ha valaki tömeges manipulációra használná fel? Létezhet a Big Data világában még szabad akarat? A kép sajnos elég borúsan fest. Egy 2017-es kutatás[100] kimutatta, hogy a profilok alapján személyre szabott targetálás alkalmas arra, hogy tömegeket győzzön meg valamiről – például arról, hogy a választásokon kire szavazzanak.[101] Eszerint mindenkit lehet irányítani – akár a saját érdekeik felé (például meggyőzni őket arról, hogy egészségesebben étkezzenek), akár a saját érdekeik ellen (például meggyőzni őket, hogy szerencsejátékosok legyenek). Egy, még ennél aggasztóbb szcenárióról is szól a kutatás, miszerint minél jobban ki tudják ismerni a felhasználói viselkedést valós időben, annál inkább lehetséges lesz, hogy szituációs kontextusba helyezzék az egyének pszichológiai jellemvonásait: az ember kedvéhez mérten választhatják ki azt az időszakot, mikor számít a legmeggyőzhetőbbnek. Ha az embernek jobb a kedve, hamarabb rábeszélhető például egy termék megvásárlására. A modern demokráciákban egyébként mindig is meg akarták győzni a pártok és politikusok a választóikat; a mostani különbséget az okozza,

[99] Például terrorizmus elleni küzdelem elősegítése, egészségügyi célok, közlekedés optimalizálása, hatékonyabb energiapolitika, egyéniesített marketing (könnyebben eladhatóvá válnának a termékek és szolgáltatások), a toborzók egyszerűbben megtalálnák a megfelelő jelöltet egy pozícióra (de persze itt kérdésessé válik az egyenlő bánásmód követelménye), a kutatók anélkül vehetnének fel primer adatokat, hogy hosszas kérdőívekkel, fókuszcsoportos beszélgetésekkel háborgatnák a résztvevőket, stb. Egyszóval az emberek életében minden gyorsabban, hatékonyabban működne az automatikus, adatok által vezérelt döntések világában (Wu Youyou, Michal Kosinski, David Stillwell, 2015. 1039. o.).

[100] S. C. Matz, Michal Kosinski, Gideon Nave, David Stillwell: Psychological targeting as an effective approach to digital mass persuasion. In: Proceedings of the national academy of sciences, vol. 114, no. 48, 2017. november 28. http://www.pnas.org/content/pnas/114/48/12714.full.pdf.

[101] Megtörtént példaként említhető a Cambridge Analytica botrány: Trump, Brexit és a fake news. Erről bővebben: Hannes Grassegger, Mikael Krogerus: The Data That Turned the World Upside Down. How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election, Motherboard 2017., frissítve: 2018. március 17. https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.

hogy nincs idő arra, hogy a választók kialakítsák a véleményüket, mert valós időben kapnak személyre szóló befolyásolást.

III. 2. A demokrácia-deficit két dimenziója

Már az internet és különböző online platformok megjelenésével, jóval a Big Data jelenség előtt elkezdődött a demokrácia és a jogállam erodálódása, ám ezt a Big Data újabb dimenzióba helyezte. A demokrácia-deficit két vetülete a Big Data korszak előtti és utáni technológiai és ebből következő társadalmi hatások összessége. A demokrácia-fogalom azon tágan értelmezett jelentését használom, miszerint a demokratikus döntéshozatal a tájékozott, információhoz alacsony költségen hozzáférő, plurális véleményeket ismerő, gondolkodó választópolgár ideáján alapul. Cass R. Sunstein a demokrácia két alapvető követelményét említi:[102] először is fontos, hogy az egyének találkozzanak a sajátjuktól eltérő nézőpontokkal, mert így elkerülhető a szélsőségek felé fordulás; emellett szükség van a közös élményekre és tapasztalatokra, amelyek társadalmi összetartó erőként funkcionálnak. A pluralitás, a vélemények különbözősége kreatív erőként hat a deliberatív vitára, hiszen, ha mindenki egyetértene, nem lenne miről beszélni. Ennélfogva az állampolgároknak nem szabadna elszigetelni magukat mások eltérő véleményétől, mert az szélsőségesedéshez vezethet.[103]

III. 2. 1. Az első dimenzió: Filter Bubble[104]

Az internet megkönnyíteni hivatott az emberek közti véleménycseréket, hiszen térben és időben korlátlan platformot nyújt, ezáltal egymáshoz közelebb hozhatja az embereket. Első látásra tehát a demokrácia nagyobb térnyerését segíti elő. Ám Sunstein felhívja a figyelmet arra, hogy a különböző szűrési lehetőségek által – amelyek egyébként nélkülözhetetlenek az információkkal túltelített, zavaros világban – a felhasználók könnyen beleesnek abba a hibába, hogy csak olyan tartalmakat követnek, olvasnak, ismernek meg, amelyek nekik tetszenek, az ő egyéni ízlésükhöz közel állnak. Így a hasonló gondolkodású emberek könnyebben egymásra találnak, és ezáltal elszigetelik magukat az eltérő véleményű csoportoktól. A zárt csoporton belül az azonos vélemények visszhangozása kedvezőtlen a demokrácia szempontjából, mert a korlátozott érvkészletű belső vita után a csoport tagjai ugyanazt fogják gondolni, amit korábban, de szélsőségesebb formában. Ez a csoportpolarizáció jelensége, ami komoly

[102] Cass R. Sunstein: Republic. com 2.0. Budapest, Complex, 2014. 18. o.
[103] Sunstein, 2014. 46. o.
[104] A fogalom Eli Parisertől származik 2011-ből. Eli Pariser: The Filter Bubble: What The Internet Is Hiding From You. Penguin Books Limited, 2011.

társadalmi veszélyeket rejt magában. Ehhez társul a társadalmi- vagy kiberkaszkádok elterjedt jelensége, ami a történések gyorsaságát adja, vagyis, mikor az információt (beleértve a hamis információt is: fake news) milliók terjesztik szét egyetlen kattintással.[105] A fenti jelenségek összefoglalása a Filter Bubble (visszhangkamra, buborékhatás, véleménybuborék), ami intellektuális izolációhoz vezet, és ez kétségtelenül kedvezőtlen hatással van a demokratikus vitára.

III. 2. 2. A második dimenzió: prediktív profilírozás

A Sunstein által felvázolt probléma már önmagában véve aggodalomkeltő a demokrácia szempontjából, azonban a Big Data megjelenésével a demokráciát ugyancsak csorbító, ám egészen más természetű veszélyek keltek életre. A mérhetetlenül pontos személyes profilok kialakítása, és az ezek alapján történő predikciója az emberi viselkedésnek az egyén irányíthatóságához, elszemélytelenedéséhez vezet. Ezt azért tartom másnak, mert ebben az esetben már nem emberek győzik meg egymást valamiről, mint a Filter Bubble esetében, hanem tulajdonképpen egy algoritmus vezérli az embert. Ez sokkal nagyobb veszélyeket rejt magában, mint az első dimenziós jelenség, mert nincs – vagy csak minimális az – emberi tényező, vagyis nincs olyan jogalany, akit el lehetne számoltatni, felelősségre lehetne vonni. Az algoritmikus irányítása az embereknek a fenti példák alapján kifejezetten hatékonynak bizonyulhat, ami azt támasztja alá, hogy a Big Data korszakban az egyéni autonómia, a szabad akarat elillanni látszik. Ha nincs szabad akarat, nincs szabad döntés sem, vagyis megdől a paradigma, miszerint a jog az egyén szabad döntésére alapoz, így gyakorlatilag az információs önrendelkezési jog működésképtelenné válhat. Ha pedig az alapvető jogok nem tudnak érvényesülni, a demokrácia sem tud – jól – működni.[106]

Az információs önrendelkezési jog megerősítése egy lehetséges orvoslása lehet a Big Data (és korábban a Filter Bubble) okozta demokrácia-deficitnek. Ehhez a jognak korlátoznia kell az „algoritmus-alapú kormányozhatóságot”[107] és újra kell értelmeznie az adatvédelmi dogmatikát. Ez utóbbi szükségességét a következő fejezetben részletezem néhány példa szemléltetésével, amelyek jól mutatják, hogy a Big Data az adatvédelem eddig ismert alapfogalmait gyökeresen átalakította.

[105] Sunstein, 2014. 46-96. o.
[106] Helbing, 2018. 78. o.
[107] A kormányozhatóság fogalmáról ld. Michel Foucalt: La gouvernementalité. In Dits et écrits, t.II, Paris, Gallimard, Quarto, 1994. 635–657. o.

III. 3. Adatvédelem a Big Data érájában

Amennyiben elfogadjuk, hogy megdőlt az önrendelkezés magjaként interpretált szabad döntés eszméje, az alapjogi katalógusból egyszerűen kihúzható lenne az információs önrendelkezési jog, ami végzetes hibának bizonyulna az alapjogvédelem és a demokrácia szempontjából. Jelen fejezetben felvázolom az adatvédelem Big Datára specializált dogmatikáját. Az elemzés szándékosan nem teljeskörű, csak azokat a fogalmakat emelem ki, amelyek – azon kívül, hogy jól szemléltetik a hatályos jog elavultságát – a később megoldásként javasolt technológia megértéséhez elengedhetetlenek.[108] Az elemzés alapján a klasszikus fogalmak egy része átértelmezésre szorul a technológiai fejlődés jegyében, bizonyos dogmatikai elemek létjogosultsága pedig a Big Data korban már megkérdőjelezhető.

III. 3. 1. Személyes adat

A személyes adat fogalma több szempontból is újragondolásra szorul. A személyes adatok védelméhez való jog már a nevében is sejteti, hogy csak a személyes adatokra fókuszál, csak akkor beszélhetünk az alapjogról, ha személyes adatokról van szó. A jelenlegi definíció így hangzik: „az érintettre vonatkozó bármely információ".[109] Vagyis nem minden adat személyes adat, annak az érintettre (természetes személyre) kell vonatkoznia. A Munkacsoport 2014-es véleménye szerint az anonimizált információ kiesik az adatvédelmi szabályozás alól,[110] ami tételesen megjelenik a GDPR-ban is.[111] A Big Data kontextusában azonban figyelembe kell venni, hogy a személyes adat és anonimizált adat közti különbség elmosódik, hiszen a Big Data – az anonimizálás ellenére – bármikor újra azonosíthatóvá tudja tenni az adatalanyt. Ennélfogva az anonim adatokat is személyes adatként kellene kezelni Big Data alapú adatkezelés esetén.[112]

Ezen felül az anonimitás már azért sem számít elégséges garanciának a felhasználó viselkedésének monitorozása, ez alapján történő profilírozása és a predikció ellen, mert a Big Data metaadatok felhasználásával lehetővé teszi a személyes profil felállítását az adott egyén személyazonosító adatai nélkül is. Ez azt jelenti, hogy az adott egyén kapcsolati hálójának adatai alapján – a saját személyazonosító adatai nélkül – ugyanolyan precíz profil állítható fel,

[108] Ld. IV. 2. fejezet.
[109] Infotv. 3. § 2. pont, de a GDPR 4. cikk 1. pont lényege is ez.
[110] Opinion 05/2014 of the Article 29 Working Party on Anonymisation Techniques.
[111] GDPR (26) bek.
[112] Antoinette Rouvroy: Of Data and Men. Fundamental Rights and Freedoms in a World of Big Data, Council of Europe, Directorate General of Human Rights and Rule of Law, Strasbourg, 2016. 20-22. o.

mintha csak az adott egyént néznék.[113] Így már nem az érintett személyes – vagy más, anonim – adatai adnak alapot egy profil kiépítésére, hanem az algoritmikus formákban történő személytelen kategorizációja az emberek viselkedésének. Ez nem a személyes érintettségen keresztül, hanem a metaadatok közti korrelációk keresése által teszi – akár szenzitív – információvá az olyan adatot,[114] amelyről addig személyes adat mivolta a hatályos dogmatika szerint elképzelhetetlen lett volna.[115]

A hagyományos definíció tehát elavult. Újra kell értelmezni a személyes adat fogalmát annak figyelembevételével, hogy az érintettre vonatkozó adaton kívül az összefüggő – kollektív – metaadatok is személyes adatnak minősülhetnek. A fogalomzavar tisztázása azért szükséges, hogy eldönthető legyen, milyen adatok kezelése esetén szorul alapjogi védelemre az adatalany, ezáltal új garanciák mihamarabbi megfogalmazására kerülhessen sor az alapjogvédelmi katalógusban.

III. 3. 2. Különleges adat

A különleges adatokat a jog kezdetektől fogva többletgaranciákkal látta el.[116]A különleges (szenzitív) adatok tételesen vannak felsorolva a hatályos jogszabályokban: „faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok".[117] Látható tehát, hogy már létező – statisztikai, társadalmi, kulturális és egyéb – kategóriákba vannak sorolva a szenzitívnek számító adatok, vagyis az egyének deduktív módszerrel kerülnek kategorizálásra, így lesznek tagjai egy bizonyos csoportnak.

A Big Data ezt az elgondolást is felborította. A deduktív kategorizáció helyett klaszteranalízist alkalmaz, mellyel korábban nem ismert – szociálisan és vizuálisan nem érzékelhető – kategóriákat lehet megjeleníteni. Ezek az új csoportok vagy kategóriák automatikus eredményei egy statisztikai adatfeldolgozásnak, ami puszta tényeken (adatokon) alapszik,

[113] Minden adat személyes, ha az alannyal kapcsolatba hozható, nemcsak a személyazonosító adatai.
[114] Ződi Zsolt: Platformok, robotok és a jog. Gondolat Kiadó, Budapest, 2018. 41-42. o.
[115] Rouvroy, 2016. 22. o.
[116] Például a jogalap tekintetében már az Avtv. is szigorúbb rendelkezéseket írt elő [Avtv. 3. § (2) bek.], az EK irányelv 8. cikkében főszabályként kimondta, hogy megtiltható a különleges adatok kezelése, és kivételeket sorolt fel; a GDPR pedig ténylegesen megtiltja a különleges adatok kezelését, de 10 kivételt említ a tiltás alól [GDPR 9. cikk (1)-(2) bek.].
[117] Infotv. 3. § (3) bek., GDPR 9. cikk (1) bek.

vagyis nem már eleve létező politikai, kulturális, esztétikai, ideológiai folyamatok által születnek meg – mint amiről eddig, a különleges adatok kategóriáinak jogszabályi szövegezése esetén szó volt. Lehetséges, hogy a klaszteranalízissel társadalmilag, politikailag, ideológiailag neutrálisabb kategóriák állíthatók fel, és az eddigi „elfogult" kategóriák meghaladhatók lesznek.[118] A társadalmilag kialakított kategóriák kétségtelenül diszkriminatívak. A Big Data jelenség itt kifejezetten előnyös hatásokat implikál az egyenlőségnövelő és diszkriminációt csökkentő, megelőző klaszterek kialakításával.[119]

További szempont, hogy a Big Data korban kifejezetten leegyszerűsödött a szenzitív adatokhoz való hozzáférés. A technológia biztosította korrelációs technikák lehetővé teszik olyan adatok szenzitívvé konvertálását, melyeknek önmagukban nem tulajdonítható jelentőség, de ha a nagy adathalmazban összekapcsolódnak más – hasonlóan nem releváns – adatokkal, különleges adatok derülhetnek ki az egyénről. Például a Netflixen történő filmválasztás politikai és vallási nézeteket is elárul rólunk, a vásárlási szokások kiváló indikátorai az egészségi állapotunknak, vagy a Facebookra feltöltött kép alapján könnyen lehet következtetni etnikai és faji hovatartozásunkra.[120] Ahogyan azt fentebb említettem, a like-okból is leszűrhető az ember szexuális orientációja, politikai véleménye.[121]

Felmerül a kérdés, hogy mi szükség van a személyes adatok kiemelt védelemben részesített kategóriáira. Az eredeti cél a diszkrimináció megelőzése és csökkentése volt, de ma már megkérdőjelezhető, hogy a különleges adatok tételes felsorolása és némi többletgaranciával ellátása valóban hatékony eszköz lenne erre. Egyrészt azért felesleges a különleges adatok kezelését szigorúbban szabályozni, mint a „sima" személyes adatok kezelését, mert a Big Data segítségével bármilyen – addig személyesnek sem mondható – adat szenzitívvé formálható (vagyis a létező szenzitív adatkategóriák egyikébe besorolható lesz). Másrészt az emberek közti különbségtétel a Big Datával sokkal finomabban, diszkriminációmentesebben is történhet (például az egyéni életvitel szempontjából), mint a történelmileg kialakult védendő csoportokba

[118] Rouvroy, 2016. 26-29. o.
[119] Tal Zarsky: Governmental Data Mining and its Alternatives. Penn State Law Review, Vol. 116, No. 2. 2011.
[120] Rouvroy, 2016. 27. o.
[121] Ld. III. 1. fejezet.

sorolás.[122] Ezek alapján úgy gondolom, hogy a különleges adatok kategóriáira a Big Data korban nincs már szükség.

III. 3. 3. Hozzájárulás

A Big Data korban az érintett hozzájárulása rendkívül alacsony védettségi szintet biztosít az alapjognak. Már korábban is szóltam az érdemi hozzájárulás érvényesíthetőségének korlátairól,[123] ami nem véletlen. A hagyományos dogmatika alapján a hozzájárulás volt a legerősebb alapjogvédelmi eszköz az egyén kezében, de mára alappal állítható, hogy ez lett a leggyengébb. Az interneten manapság minden úgy van konstruálva, hogy ne legyen átlátható.[124] Egyszerűen nem várható el senkitől, hogy elolvassa a nyolc-tíz – vagy több – oldalas adatkezelési tájékoztatót minden egyes alkalmazás letöltésekor és honlap megnyitásakor,[125] s e szcenário alapján az sem elvárható tőle, hogy tájékozott döntést hozzon. A hozzájárulás ekképpen az adatvédelmi jog fikciójává vált.[126] Éppen ezért erősítette meg a GDPR az adatkezelők kötelezettségeit, és vezette be a privacy by design és by default követelményeit.[127]

Ám az információs önrendelkezés intézményes korlátozása – azért, mert jogilag képtelenek a gyakorlatban megvalósíthatóvá tenni az érdemi hozzájárulás érvényesülését – nem megoldás, hiszen a folyamatos alapjogsérelem nem kompatibilis a demokráciával. Nyomatékos jelentősége van tehát annak, hogy a hozzájárulás alapú adatkezelést újragondolja a jogalkotó. Olyan új meghatározásra van szükség, melyben figyelembe veszik a digitális média különböző szereplőinek adatkezelésben való részvételét is, és mindenekelőtt azt, hogy ezen szereplők érdekei ne kapjanak túlzott hangsúlyt.[128] (Ennek a tézisnek ellentmond a hatályos szabályozásban foglalt jogos érdek jogalapként történő elismerése.) Az új szabályozásban Rouvroy szerint sokkal tisztábban kellene meghatározni az önkéntes, határozott, megfelelő tájékoztatáson alapuló hozzájárulás kritériumait, s kifejezetten ki kellene térni arra, hogy az

[122] Rouvroy, 2016. 29. o.
[123] Ld. 15-16. o.
[124] Erre egyszerű példa a cookie-k alkalmazása. Két típusuk van: az első a webböngésző működését gyorsítja (legtöbbször nem tartalmaz személyes adatot), a második típus felhasználói szokásokat érint, vagyis valójában csak személyes adatokat termel a Big Data adatbázisokba. Vannak olyan honlapok, melyek be sem engednek, ha nem hagyom jóvá a sütiket, vagy nem enged továbblépni, vagy a felhasználói élményt csökkenti. Egyszóval úgy van kalkulálva a rendszer, hogy az ember rögtön leokézza, és tovább mehessen. Az automatikus okézgatás elveszi a hozzájárulás értelmét, hiszen az nemhogy nem tájékozott, de nem is önkéntes, hiszen a hozzájárulás nélkül nem tudnánk megnyitni az oldalt. Ez nagyon jól mutatja, hogy a Big Data korban a hozzájárulás mivé változott.
[125] Ződi, 2018. 84-85. o.
[126] Erről bővebben ld. A. Mantelero: The future of consumer data protection in the EU. Rethinking the "notice and consent" paradigm in the new era of predictive analytics. Computer Law and Security Review, 2014. 643-660. o.
[127] GDPR 25. cikk.
[128] Rouvroy, 2016. 24. o.

adatkezelők garantálják, hogy az egyén választása egy tényleges, valódi döntés legyen, amellyel az érintett vagy megadja a hozzájárulását az adatkezeléshez, vagy nem.[129] Továbbá az opt-in rendszereket kell előnyben részesíteni az opt-out rezsimmel szemben, hogy a hozzájárulás határozottsága megerősítést nyerjen.[130]

III. 3. 4. Adatminimalizálás és célhoz kötöttség

A Big Data típusú adatkezelés logikája teljesen ellentétes az adatminimalizálás követelményével és a célhoz kötöttség elvével. Az adattakarékosság paradoxiális jellege a Big Datával nem szorul különösebb magyarázatra, hiszen a technológia alfáját és omegáját, a „Volume"-ot, azaz a mennyiséget tennék semmissé, ha a hatályos jog szabályait[131]alkalmaznák a Big Data típusú adatkezeléskor. Nem beszélve arról, hogy az adatminimalizálás a mesterséges intelligencia tanításának (machine learning) gátját is jelenti, amivel a fejlődést akadályozná meg, s ezért feleslegesnek bizonyul a garanciarendszerben.

A célhoz kötöttséggel már kissé más a helyzet. Annak ellenére, hogy a Big Data rendszerek működésének szempontjából kedvezőtlen, mert akadályozza az innovációs folyamatokat, elengedhetetlen elem a személyes adatok védelméhez fűződő alapvető jog érvényesülése szempontjából.[132] Ha nem lenne az adatkezelés célhoz kötött, az adatvédelem alapjogi minősége szűnne meg. Azonban a jelenlegi dogmatika itt is elavult, hiszen előír egy egyértelműen meghatározott, jogszerű célt, melynek az adatkezelés minden szakaszában meg kell felelni, s mindennek a szükségességi-arányossági tesztnek megfelelően kell történnie.[133] Ezzel szemben a Big Data lényege a parttalan és cél nélküli adatgyűjtés, hiszen a korreláció keresése annál hatékonyabb, minél több adat van az adatbázisban, s ezek az adatok nem jogszerű célból, más alapjog érvényesítése érdekében kerülnek begyűjtésre, hanem az optimalizáció miatt. Ezért alakulhatnak ki a precízebbnél precízebb személyes profilok, ezért képes a technológia a mikrotargetálásra és predikcióra, amik az egyén szempontjából

[129] Például a hozzájárulás megadásáért bármiféle előny ígérésének kizárásával, valamint annak a megtiltásával, hogy a választási architektúrát a hozzájárulás megszerzése végett bármilyen módon megzavarják. (Rouvroy, 2016. 24. o.)
[130]Rouvroy, 2016. 24. o.
[131] GDPR 5 cikk (1) bek. c) pont.
[132] Ezt a Munkacsoport is megerősítette, ám nem alapjogi indokolással. A célhoz kötöttség megtartását a tisztességes piaci verseny fenntartása céljából látja elengedhetetlennek: a mamutcégek ne juthassanak aránytalan előnyökhöz az új vállalkozásokkal szemben annál fogva, hogy ők már rég kiépítették a Big Data adatbázisukat. (Statement of the Article 29 Working Party on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU).
[133] Infotv. 4. § (1)-(2) bek., de a GDPR 5. cikk (1) bekezdés b) pontja nem írja elő a szükségességi-arányossági-teszt alkalmazásának követelményét, de szól a közérdekű archiválás, tudományos és történelmi kutatás, statisztikai célból történő adatkezelés további garanciáiról.

veszélyforrást jelentenek. A célhoz kötöttség elve tehát nagyon határozott átalakításra szorul, – ahol szükséges – a személyes adatok anonimizált verziójára is kiterjesztett értelmezésével.[134]

III. 3. 5. Automatizált döntéshozatal, adatkezelő

A GDPR[135] megtartotta az EK irányelv[136] automatizált döntéshozatalra vonatkozó szabályát, de azt még a profilalkotásra is kiterjesztette. A szabályozásnak már az eleje is betarthatatlan a Big Data korban, mely szerint az egyénnek joga van arra, hogy ne terjedjen ki rá az automatizált döntés hatálya.[137] Mivel a szomszédom[138] adata is ugyanolyan hasznos a Big Datának, mint az enyém, én kérhetem ugyan, hogy töröljék[139] a rám vonatkozó összes adatot, de az önrendelkezési jogom nem terjed ki a szomszédomra, így, ha ő nem kéri, az ő adatai alapján még mindig visszaállítható a rólam alkotott profil a saját (személyazonosító) adataim nélkül is.[140] A GDPR szerint az adatkezelőnek kell biztosítani, hogy az egyén jogai érvényre juthassanak,[141] ami szintén elképzelhetetlen a Big Data kontextusában, mert ha egy öntanuló algoritmus kiszámíthatatlan eredménye az automatizált döntés, az adatkezelőnek ahhoz már semmi köze nincs, hiszen nem tud befolyással lenni rá. A legfeleslegesebb rendelkezések a szabályozásban pedig az egyén jogai[142] tekintetében azok, hogy az érintettnek érthetően magyarázzák el az automatizált döntés során alkalmazott logikát, illetve azt is, hogy az adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.[143] Ismételten hangsúlyozom, hogy a machine learning algoritmusai olyan bonyolultak, hogy még egy szakértőnek is nehézséget okoz – ha nem lehetetlen – a megértése. Annak, hogy egy átlagembernek, az adatalanynak elmagyarázzák az automatizált döntés mögött húzódó logikát nincs értelme, mert soha nem fogja megérteni, és ennél fogva nem jelent semmilyen garanciát a személyes adatok védelmében.

Ha a személyes adatok alapján történő automatizált döntések öntanuló vagy machine learning algoritmusok eredményei, felmerül a kérdés, hogy ki számít adatkezelőnek. A hatályos jog szerint adatkezelő „az a természetes vagy jogi személy, illetve jogi személyiséggel nem

[134] Rouvroy, 2016. 26. o.
[135] GDPR 22. cikk.
[136] EK irányelv 15. cikk.
[137] GDPR 22. cikk (1) bek.
[138] Szomszéd alatt az egyénhez (napi szinten) közel álló kapcsolati hálót kell érteni.
[139] Az megint más kérdés, hogy a törlés gyakorlatban kivitelezhető-e.
[140] Rouvroy, 2016. 33. o.
[141] GDPR 22. cikk (3) bek.
[142] Tájékoztatáshoz való jog, hozzáféréshez való jog.
[143] GDPR 13. cikk (2) bek. f) pont, 14. cikk (2) bek. g) pont, 15. cikk (1) bek. h) pont.

rendelkező szervezet, aki vagy amely (...) önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (...) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja."[144] A személyi hatályba egyértelműen nem illik bele az algoritmus, de egy automatizált döntést az algoritmus hoz meg, így a tárgyi hatálynak ki kellene terjednie rá. Azonban hogyan lehetne felelősségre vonni egy gépet, egy algoritmust? A kérdés jól érzékelteti a diszkrepanciát a Big Data és a hatályos szabályozás között. A Big Data alapú adatkezelés átláthatatlansága bizonyítja, hogy az öntanulás és gépi tanulás miatt nem szabad arra az adatkezelőre hárítani a terhet, aki megírja az algoritmust.

IV. Megoldási javaslatok

IV. 1. A jogi megoldások keresésének elvei

A korábban kifejtettek alapján az információs önrendelkezési jog elveszíti jelentőségét mind a jogi szabályozásban, mind pedig a Big Data által átformált technológiai és társadalmi környezet tekintetében. A hatályos európai uniós és magyar adatvédelmi jog anakronisztikusnak titulálható, mert paradigmaváltásszerű változásai ellenére sem képes megfelelő garanciákat nyújtani a személyes adatok védelméhez való jog tényleges érvényesüléséhez. A Big Data alapú adatkezelések folyamatos alapjogsérelmeket okoznak, hiszen a prediktív profilírozás hatására az egyén egyre inkább eljelentéktelenedik, elszemélytelenedik. Éppen ezért olyan új, a Big Datára is reflektáló – nem technológia-semleges[145] – garanciákkal tűzdelt jogi szabályozás szükséges, mely nem gátolja meg a technológiai fejlődést. Ha a jog – a személyes adatok védelméhez való jog védelmében – egyenesen az innováció útjába lép, a tudományos kutatás szabadságát is akadályozza, ami szintén szóban forgó alapjog.[146] Ezért minden esetben a szükségességi-arányossági teszt elvégzésére is szükség van. Az új jogi szabályozást úgy kell kialakítani, hogy a jogrendszer egyrészt biztosítsa, hogy az adatalany ismét jelen lehessen, rendelkezhessen magáról, másrészt meg kell akadályoznia azt, hogy egyszerű profilokba zárják

[144] Infotv. 3. § 9. pont, de a GDPR szövege is ugyanezt rögzíti (GDPR 4. cikk 7. pont).
[145] Ivan Szekely, Mate Daniel Szabo and Beatrix Vissy: Regulating the future? Law, ethics, and emerging technologies. Journal of Information, Communication & Ethics in Society, Vol. 9, No. 3, (Special issue: Emerging technology and ethics – Guest Editor: Kutoma Wakunuma), 2011. 183. o.
[146] Ivan Szekely: Building our future glass homes: An essay about influencing the future through regulation. Computer Law & Security Review 29, 2013. 547-548. o.

az egyént, aki ily módon semmit nem tud tenni a róla szóló, de őt kikerülő döntések meghozatalakor.

IV. 1. 1. Fogalomtisztázás és új fogalmak bevezetése

A III. 3. fejezet rámutatott arra, hogy a hagyományos adatvédelmi dogmatikai keretek elavultak, így az alapfogalmak újragondolása és technológiai változásokkal való összehangolása szükséges. Ez szükségképpen magában foglalja új fogalmak bevezetését is. Rouvroy két új kiegészítő adatvédelmi jogi kodifikációs javaslatot tesz a Big Data kontextusában. Az első az engedetlenséghez való jog mint garanciális eszköz bevezetése. Ez a jogalanynak azt a képességet adja a kezébe, hogy ellen tud állni az algoritmusnak, vagyis nem mindig azt teszi, amit az algoritmus megjósol, hogy tenni fog vagy tennie kellene. A második az önmagunkért és cselekedeteinkért, döntéseinkért, szándékainkért való felelősség vállalásának jogi kötelezettsége, annak ellenére, mit ajánl az algoritmus a személyes profilunk alapján. A jognak ösztönöznie kellene az egyének elhajlását a spontaneitás és kiszámíthatatlanság felé, ami olyan liberális szemléletmódot tükröz, melyben az egyén kifejezheti azokat a véleményeit, ötleteit, melyek az algoritmusok által megjósolhatatlanok.[147]

IV. 1. 2. Az időzítés fontossága

Rouvroy javaslatai a Big Datára specializált irányba mutatnak, de még mindig csak a sötétben tapogatózik, hiszen a jövő komplex társadalmi és technológiai környezete megjósolhatatlan. Ugyanakkor a Big Data alapú adatkezelés okozta folyamatos alapjogsérelmek útjába minél előbb fel kell állítani a stop-táblát. Felmerül a kérdés, hogy hogyan fogalmazhatók meg új garanciák, ha tulajdonképpen még azt sem tudjuk, mivel állunk szemben. A Big Datában rejlő lehetőségek csak egy apró részletét tudtam bemutatni, hiszen exponenciális fejlődési képességénél fogva a jövőbeli társadalomra gyakorolt hatásai még nem ismertek. A jogalkotás így nagy eséllyel nem tudja majd elérni a kívánt hatásokat, és a hatályos szabályozáshoz hasonló inadekvát rendelkezéseket fog megállapítani. Ennek ellenére a jogi szabályozás új technológiákra hangolását minél hamarabb el kell kezdeni.[148] Ha megvárná a jogalkotó, hogy az új technológiák használata széleskörűen elterjedjen a társadalomban, már túl késő lenne azon gondolkozni, hogyan védjük meg azokat az alapértékeinket, alapjogainkat, melyeket az új technológiai berendezkedés hatására társadalmilag már kevésbé tartanak fontosnak. Például a

[147] Rouvroy, 2016. 36-37. o.
[148] Szekely, Szabo, Vissy, 2011. 189. o.

ma „túlértékelt" információs önrendelkezés és magánélethez való jog feladása is megtörténhet a jövőben a kényelemért cserébe.[149]

IV. 1. 3. Szabályozási szint

A Big Data jelenség okozta problémák a világon mindenhol jelen vannak, globálisak, így felmerül a kérdés, hogy milyen szinten lehetne a leghatékonyabb a szabályozás. Természetesen az univerzális szint bizonyulna optimális megoldásnak, azonban ennek számos akadálya van. A közeljövőben a globális jogi szabályozottság esélye rendkívül alacsony, tekintve, hogy a nemzetállamok szuverenitási korlátjába ütközik. A legjobb variáns így csak a nemzetközi egyezmények minél több ország általi ratifikációja lehet.[150] Ám az európai integráció olyan szupranacionális alapelveket fektetett le, melyeket az Alapjogi Charta kötelező erejénél fogva minden tagállamnak be kell tartani. Ezért az Európai Unió alapjogvédelmi sztenderdjei mindig is magasabbak lesznek, mint a világ többi régiójában.[151]

IV. 1. 4. A szabályozás prediktív tanuló modellje[152]

A Big Data okozta alapjogi és demokráciát csorbító problémákra, ha van is jogi megoldás, az még biztosan nem tökéletes. Hogyan lenne mégis kialakítható egy hatékony, garanciális szabálycsomag? A Székely Iván által javasolt modell, a szabályozás prediktív tanuló modellje az egyik járható út lehet. A prediktív tanulás az informatikából ismert módszer, ami a jogalkotásra analóg módon alkalmazható. Először az összes elérhető információt felhasználva elképzelik a jövőbeli életfeltételeket, melyeket jogilag szabályoznának, a jelen értékeivel összhangban. Ezután kialakítják azokat a szabályokat, amelyeket alkalmasnak ítélnek az elképzelt életfeltételek szabályozására. Ezt a szabályok hatásainak és alkalmazhatóságának tesztelése követi az elképzelt szcenáriók alapján. Az eredmények kielemzése után megváltoztatják a szabályokat, és újra lefuttatnak egy tesztet, amelyet újra kiértékelés követ.[153] A módszer állandó visszajelzéseket igényel. Kissé utópisztikusnak tűnhet, de a leghatékonyabb

[149] Szekely, 2013. 544-545. o.
[150] Uo. 544. o.
[151] Uo. 544. o.
[152] Uo. 549-550. o.
[153] Uo. 550. o.

jogi szabályozás elérése szempontjából sokkal praktikusabb, mint a jelenlegi jogalkotási procedúrák.[154]

IV. 2. Blockchain - egy lehetséges út

Az új technológiák (például Big Data, majd az abból kibontakozó mesterséges intelligencia) jogi szabályozása a fentiek alapján elengedhetetlen. Azonban a jogi megoldáskeresés elveinek áttekintése alapján kétségesnek tűnik, hogy a jogalkotó és általában véve a jelenlegi jogrendszer erre fel lenne készülve. Láthattuk az akadályokat: a fogalmi tisztázás nehézkes a jövő ismeretlensége miatt, a jogalkotás gyorsasága kritizálható, globális szinten még nem képzelhető el jogi szabályozás. Elfogadván tehát azt a tételt, hogy a jog mindig is le lesz maradva a technológiai fejlődéshez képest,[155] az is állítható, hogy pusztán jogi eszközökkel nem lehet szabályozni a mostani világot. A demokrácia védelme érdekében viszont minél hamarabb lépni kell. Ha jogi megoldás nem áll rendelkezésre, megfontolandó, hogy a technológia adhat-e választ a problémákra.

Lawrence Lessig már 1999-ben kimondta, hogy az információs társadalomban a kód de facto a jog („code is law"[156]): mindegy, mi van a jogban, a (kiber)valóság aszerint fog alakulni, ahogy azt az informatikus lekódolja. Ezt sok módon lehet befolyásolni. Ha például a fejlesztőknél sikerül elérni, hogy ágyazzanak bele a kódba olyan garanciákat, melyek az eddig lefektetett alkotmányos értékeket védik (például a személyes adatok védelméhez való jogot), a technológia jelenleg anarchikusnak tűnő jövőképe megelőzhető. Már ma is léteznek erre irányuló, jogban kodifikált törekvések,[157] de széleskörű jogi alkalmazásuk még nem nyert teret. A technológia viszont képes a jog belépése[158] előtt kizárni a jogsérelmi lehetőségeket. Számos privátszférát erősítő technológia (PET technológia) létezik,[159] melyek közül a blockchaint

[154] Több probléma is felmerül, többek között a jogalkotók hozzá nem értése, így a szakértők bevonásának kényszere okozta lassúság, valamint ha inadekvátként szabályok születnek, a személyi hatálya alá tartozó jogalanyok passzív rezisztanciája is szóba jön (Szekely, 2013. 548. o.).
[155] Szekely, 2013. 548. o.
[156] Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 1999.
[157] Ilyen, legalább 20 éves törekvés a beépített adatvédelmi funkció (privacy by design), miszerint úgy kell tervezni a rendszereket, hogy eleve benne legyenek azok a megoldások informatikailag, melyeket az adatvédelem megkövetel. (Bővebben: Ann Cavoukian: Privacy by Design. The 7 Foundational Principles. 2009. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf) A GDPR 25. cikkében az alapértelmezett adatvédelemmel együtt szerepel (privacy by default, mely lényege, hogy szükséges és elégséges funkcionalitása legyen az eszköznek eladáskor, és az opt-in logikának megfelelően a felhasználó iratkozhasson fel különböző helyekre), de kógenciájuk megkérdőjelezhető.
[158] Akár jogalkotással, akár jogalkalmazással.
[159] A teljesség igénye nélkül többek között ide sorolható az egyedi technológiáktól kezdve (webpoloskák detektálása) a rendszerszerű megoldásokon át (pl. private credentials: privát tanúsítványok rendszere, mely a célhoz kötöttség elvét hangsúlyozva csak a szükséges és elégséges mennyiségű adatot kezeli) a különböző

emelem ki, mert ez egy kimagaslóan jó és működőképes megoldás. Ezt a dolgozatban tárgyalt adatvédelmi problémák feloldásával szemléltetem.

A Big Data jelenséggel kapcsolatban négy, az információs önrendelkezési joggal összeférhetetlen problémát véltem felfedezni, melyekre a blockchain[160] – magyarul blokklánc – technológia alkalmazása válasszal szolgálhat. A következőkben ezeken a példákon keresztül mutatom be, hogy valójában takar ez a forradalmi, határokon átnyúló innováció, mellyel akár egy teljesen új társadalmi kontrollviszony is megteremthető.[161]

a) *Átlátható egyén – átláthatatlan algoritmus*: A Big Data alapú adatkezelés az egyént teljes mértékig kiismerhetővé tette, az algoritmus viszont annyira bonyolulttá vált, hogy az még a szakértők számára is (például a gépi tanulás folytán) átláthatatlan. Ahogyan azt az állam és egyén viszonylatában már a rendszerváltáskor megfogalmazták,[162] ennek pont a fordítottja lenne ideális. Ha az állam fogalmát rávetítjük a Big Data rendszerek alkalmazóira, nekik egyértelműen transzparensnek kellene lenniük. A blokklánc rendszerekben létezik egy megosztott főkönyv (az összes tranzakció regisztere), ami minden egyes tagnak a rendelkezésére áll, így egymást ellenőrizni tudják, és a láncolatban további műveletek csak konszenzusos formában hajthatók végre. Ezért a blokkláncban minden tag átlátja a többiek műveleteit, vagyis a rendszer transzparenciája adott. Az egyén átláthatatlanná tétele is kivitelezhető, mert az adatok egy ún. hash-kód (karakterek hosszú sora) által hitelesítve keringenek, és csak akkor válnak mások számára is láthatóvá, ha az adatalany privát kulcsával ezt engedélyezi. Létezik ugyanis egy kulcspár, melyből az egyik publikus (ez bárki számára elérhető), a másik privát (amiből kizárólag egy van, az adatalany birtokában).[163] A hash-kóddal

vizualizációs- (szteganográfia) és az egyén identitását elrejtő technológiák (THOR), valamint léteznek obfuszkációs technikák is, melyek az összezavaráson alapulnak.

[160] A blockchainről egyből a bitcoinra asszociálunk, azonban a technológia alkalmas arra, hogy ne csak pénz, hanem például szoftverek, ingatlanok, tudományos tartalmak, szavazatok vagy akár személyes adatok áramlásának regisztere legyen (Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly, 2015).

[161] Z. Karvalics László – Nagy Gábor Dániel: Prokrusztész nélküli világ? Blokklánc és társadalmi makroevolúció. Információs Társadalom, XVII. évf. 3. szám, 2017. 7. o.

[162] Az átlátható állam, átláthatatlan polgár eszményét az Alkotmánybíróság kényszerítette ki az információs hatalom megosztásáról szóló határozataival [pl. 15/1991. (IV. 13.) AB határozat].

[163] Az adatvédelem tekintetében a privát kulcs lehetne például biometrikus, az egyén ujjlenyomata, amiből biztosan csak egy van.

hitelesített személyes adatok csak akkor oldhatók tehát fel, ha azt mindkét kulccsal kinyitják. Az egyén önrendelkezési joga ennél fogva újra megerősítést nyerhet.

b) *Hatalomkoncentráció*: A Big Data technológiát alkalmazó adatkezelő kezében a hatalom koncentrálódik az érintett személyes profilja birtokában, melyet akár korlátlan manipulációs célokra is felhasználhat. Információs hatalmasság lévén neki az egyén ki van szolgáltatva, képtelen védekezni. A hatalmi góc megszüntethető a blokklánccal, ugyanis a rendszer a decentralizáción alapszik, vagyis nincs egy központi hitelesítő, kibocsátó, kormányzó szervezet, a „hatalom" (inkább kontroll) a tagok közt megoszlik. A blokkláncban a tagok egymást biztosítják, mindenki jelenléte fék és egyensúly is egyben.

c) *Elszámoltathatóság:* A Big Data rendszerekben az algoritmus gépi tanulás által önálló életre kelhet, vagyis az adatkezelőtől szinte teljesen független automatizált döntéseket tud meghozni. Felmerül tehát az elszámoltathatóság kérdése: ki vonható felelősségre az egyénnek okozott jogsérelemért, ha az az adatkezelőtől független algoritmus döntésén alapult? A GDPR egyértelműen az adatkezelőre hárította a terhet, de ez a szabály az automatizált döntések esetén tarthatatlan. A blokklánc erre a problémára is megoldást nyújt, mert minden egyes tag elszámoltatható a tranzakciók hitelesítéséért, érvényességéért, így mindenki egyetemlegesen felelősségre vonható. Mindenki tudja, ki hibázott, hiszen mindenki látja az összes műveletet, ezért a jogsértő magatartások száma nullára csökkenthető.

d) *Kikényszeríthetőség:* A Big Data alapú adatkezelés átláthatatlansága miatt az egyéni jogérvényesítés hatósági és bírósági útja nem lehet elég garancia az alapjogvédelemben, különös tekintettel arra, hogy a tömeges egyéni alapjogsérelem a demokratikus intézményrendszerre is negatív hatással lehet, tehát a probléma nem csak az egyes egyéneket érinti. A kikényszeríthetőség kérdése is megoldásra lel a blokklánc technológiákban, mert a rendszer úgy van tervezve, hogy önmagát hajtja végre. Létező példát nyújt erre az okosszerződés, amelyben a szerződésszegés kizárt, mert a rendszer mindegyik fél kötelezettségét automatikusan teljesíti, akár a felek mulasztása ellenére is.

A blokklánc alapú társadalom illúziónak tűnhet, számos érv hozható fel működőképessége mellett és ellen. Ellene szól, hogy mindig is voltak, és valószínűleg mindig is lesznek központi vagy globális gócok, amivel a blokklánc logikája ellentétes, hiszen szükségképpen kikerül a központi irányítás alól. Léteznek azonban olyan nézetek is, melyek azt vizionálják, hogy a

blokklánc forradalma szükségtelenné, illegitimmé teheti a nemzetállamot.[164] Kétségtelen, hogy bizonyos pontokon, ahol a jog képtelen adekvát választ adni, és csak kullog a technológiai fejlődés után, hatékonyabb megoldást biztosít a technológia. Ezáltal e pontokon ki is kapcsolhatja az állami kontroll szükségességét. Az állam végleges megszűnése ennek ellenére utópisztikus elképzelés. Jól jelzi azonban, hogy elindultunk egy olyan úton, melynek a vége beláthatatlan. Ezen az úton az adatvédelem garanciáinak blokklánccal történő biztosítása egy apró, ám markáns lépés.

Székely Iván az ohridi házak metaforájával írta le a blokklánc technológiát. A macedóniai Ohridi-tó környéke földrengések által veszélyeztetett terület. Ezért úgy épültek a házak, hogy a mestergerenda hosszabb, mint maga a ház, és belelóg a szomszédos házba. Így az egész utca össze van láncolva mestergerendákkal, amelyek egymást tartják, mikor remeg a föld.[165] A blokklánc is így működik, a peer-to-peer láncolat tartja össze az egészet, ez adja a rendszer erejét, stabilitását. Meggyőződésem, hogy blokklánc valódi megoldás a Big Data jelenség okozta adatvédelmi krízisre.

A demokrácia 2.0 számomra azt jelenti, hogy az állampolgárok részt vesznek a társadalom működésének elősegítése érdekében a társadalmi diskurzusokban, ők töltik fel tartalommal a rendszert. A blokklánc alapú társadalmi berendezkedés ezt megköveteli, hiszen csak akkor tud működni, ha minél többen részt vállalnak benne. Nemcsak a személyes adatok védelméhez való jog tényleges érvényesülésének lehetőségét adja tehát vissza, hanem a demokrácia újbóli virágzásához is vezethet.

[164] Marcella Atzori: Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Virtus Interpress, 2017. 49. o.
[165] Székely Iván, személyes közlés: 2018. október 26.

Hivatkozások

Felhasznált irodalom

A Nemzeti Adatvédelmi és Információszabadság Hatóság nyilatkozata a Nemzetközi Adatvédelmi Biztosítási Konferenciák keretében a Big Data-ról, 2014. https://www.naih.hu/files/Nyilatkozat-Big-Data.pdf

A. Mantelero: The future of consumer data protection in the EU. Rethinking the "notice and consent" paradigm in the new era of predictive analytics. Computer Law and Security Review, 2014. 643-660. o.

Antoinette Rouvroy, Thomas Berns: Le nouveau pouvoir statistique – Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps 'numériques'. Multitudes, No. 40, 2010. 88-103. o.

Antoinette Rouvroy: Of Data and Men. Fundamental Rights and Freedoms in a World of Big Data, Council of Europe, Directorate General of Human Rights and Rule of Law, Strasbourg, 2016.

Bibó István: Az államhatalmak elválasztása egykor és most. In: Válogatott tanulmányok, Második kötet, 1947. http://mek.oszk.hu/02000/02043/html/290.html

Charles Montesquieu: A törvények szelleméről. Budapest, Osiris–Attraktor, 2000. 245 o.

Chronowski Nóra: Üzlet és emberi jogok – nemzetközi törekvések és alkotmányjogi korlátok. In: JURA, 2013. 2. szám, Pécs, 9. o. https://jura.ajk.pte.hu/JURA_2013_2.pdf

Eli Pariser: The Filter Bubble: What The Internet Is Hiding From You. Penguin Books Limited, 2011.

Emberi jogok. Szerk. Halmai Gábor és Tóth Gábor Attila. Osiris Kiadó, Budapest, 2008.

Gárdos-Orosz Fruzsina: Az emberi jogok alkalmazásának lehetőségei a rendes bíróságokon különös tekintettel a magánjogi jogvitákra. Doktori értekezés, Győr, 2010. 91-98. o.

Hannes Grassegger, Mikael Krogerus: The Data That Turned the World Upside Down. How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election, Motherboard 2017., frissítve: 2018. március 17. https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

Ivan Szekely, Mate Daniel Szabo and Beatrix Vissy: Regulating the future? Law, ethics, and emerging technologies. Journal of Information, Communication & Ethics in Society, Vol. 9, No. 3, (Special issue: Emerging technology and ethics – Guest Editor: Kutoma Wakunuma), 2011.

Ivan Szekely: Building our future glass homes: An essay about influencing the future through regulation. Computer Law & Security Review 29, 2013. 540–553. o.

Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése c. PhD dolgozata. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, 2009.

Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 1999.

Majtényi László: Az adatvédelmi ombudsmann – az adatvédelmi törvényhozás. Magyar Közigazgatás, 8. sz. 1990. 30. o.

Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly, 2015.

Michael Haupt: “Data is the New Oil” — A Ludicrous Proposition, Medium Corporation, Medium, 2016. május 2. https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294

Michal Kosinski, David Stillwell, Thore Graepel: Private traits and attributes are predictable from digital records of human behavior. In: Proceedings of the National Academy of Sciences, vol. 110, no. 15., 2013. április 9. 5802-5805. o. http://www.pnas.org/content/pnas/110/15/5802.full.pdf

Michel Foucalt: La gouvernementalité. In Dits et écrits, t.II, Paris, Gallimard, Quarto, 1994. 635–657. o.

Paul M. Schwartz: Privacy, Participation, Cyberspace: An American Perspective. In

Baeriswyl–Rudin. 2002. 77. o.

Sólyom László: A személyiségi jogok elmélete. KJK, Budapest, 1983.

Sólyom László: Adatvédelem és személyiségi jog. Világosság, 1988. január. 57. o.

Szabó Máté Dániel: Az alapjogok információs jogi rétege. In: Jogi tanulmányok 2010. Ünnepi Konferencia az ELTE megalakulásának 375. évfordulója alkalmából. Budapest, ELTE ÁJK, 2010. I. kötet

Szabó Máté: Az információs hatalom alkotmányos korlátai, Miskolc, 2012.

Szigeti Tamás: Az információs hatalom korlátozása tengeren innen és túl, In: Infokommunikáció és jog, HVG-Orac, 2009.

Tal Zarsky: Governmental Data Mining and its Alternatives. Penn State Law Review, Vol. 116, No. 2. 2011.

Towards Digital Enlightenment. Essays on the Dark and Light Sides of the Digital Revolution. Szerk: Dirk Helbing. Springer, 2018.

Yoram Bachrach, Michal Kosinski, Thore Graepel, Pushmeet Kohli, David Stillwell: Personality and Patterns of Facebook Usage – Proceedings of the ACM Web Science Conference, 2012. 36-44. o. http://www.alanuk.com/wp-content/uploads/attachments/Personality_and_Patterns_of_Facebook_Usage.pdf

Z. Karvalics László – Nagy Gábor Dániel: Prokrusztész nélküli világ? Blokklánc és társadalmi makroevolúció. Információs Társadalom, XVII. évf. 3. szám, 2017.

Ződi Zsolt: Platformok, robotok és a jog. Gondolat Kiadó, Budapest, 2018.

Ződi Zsolt: Privacy és a Big Data, Fundamentum, 1-2. szám, 2017. http://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf

Felhasznált joganyag

Alaptörvény

Alkotmány

15/ 1991. (IV. 13.) AB határozat

21/1996. (IV. 17.) AB határozat

36/ 2005. (X. 5.) AB határozat

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

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

Az Európai Unió Alapjogi Chartája

Európai Unió működéséről szóló szerződés

BVerfGE 65, 1 (1983) – Volkszählung

A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv 29. cikke szerint létrehozott Adatvédelmi Munkacsoportnak a hozzájárulás fogalom-meghatározásáról szóló 15/2011. számú véleménye

Opinion 05/2014 of the Article 29 Working Party on Anonymisation Techniques

Statement of the Article 29 Working Party on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU)