ACTA HUMANA • 2017/2. 43–60.

Nemzeti konzultáció és adatvédelem

JULIEN ROSSI

Just like it was the case with previous, similar polls organised by the government, the 2015 Hungarian national consultation on "immigration and terrorism" arose significant data protection related worries in the public opinion. Indeed, governments organising such consultations are given an opportunity to collect political data on their citizens, and store them into a database. Yet, such experiments in digital direct democracy are increasingly frequent. For example, last year, the French government launched a large-scale Internet consultation on a proposed Bill on digital rights. This paper studies the compliance of Hungarian and French governmental consultation practices with data protection requirements, both legal and technical. Are the personal data of citizens handled in conformance with national and European regulations? This paper describes the tools and methods currently implemented to protect citizens' political data in public consultations, and explores ideas derived from computer science and legal literature in order to improve the level of data protection in digital democracy.

A 2015-ös nemzeti konzultáció a „bevándorlásról és a terrorizmusról" adatvédelmi aggályokat keltett. Amikor a kormány a saját állampolgárait kérdezve közvélemény-kutatást tart, lehetősége van adatbázis készítésére, amelyben rögzíti állampolgárai véleményét. Az ilyen típusú konzultáció egyre sűrűbben fordul elő és egyre gyakrabban elektronikus úton történik. 2015-ben a francia kormány szintén indított egy nagyszabású internetes konzultációt az egyik törvényjavaslatáról. E tanulmány elemezni kívánja a magyar konzultáció adatvédelmi gyakorlatát jogi és technikai szempontok alapján, összehasonlítva azt a francia gyakorlattal. Mennyire felel meg a nemzeti, valamint európai jogszabályoknak a magyar és francia kormányok adatkezelési gyakorlata? Az elemzés kitér arra, hogy milyen eszközök vannak most használatban, hogy milyen fejlesztési lehetőségeket nyújtanak az információbiztonság új kutatási eredményei ahhoz, hogy minél erősebb elektronikus adatvédelmi szintet lehessen elérni az ilyen típusú konzultációk folyamán.

Bevezetés

2015. április 24-én Kovács Zoltán, Magyarország kormányszóvivője bejelentette, hogy nemzeti konzultációt fognak tartani a „bevándorlásról és a terrorizmusról”[1] egy 12 kérdésből álló kérdőív formájában. A kérdőívet a Miniszterelnökség minden 18. évét betöltött állampolgárnak kipostázta, egyébként a kérdéssor az interneten is kitölthető volt a következő linken: http://nemzetikonzultacio.kormany.hu.

A postán kiküldött változat két oldalból állt össze, az első lapon a Miniszterelnök által aláírt bevezető beszéd, a másodikon pedig maguk a kérdések voltak.

A kérdések tartalma körül nagy politikai vita tört ki. Társadalomtudományi és kutatási szempontok alapján a kérdőív valóban egy kitűnő illusztrációja a Pierre Bourdieu által fogalmazott véleménykutatási kifogásoknak és annak módszertani korlátainak, miszerint, „a véleménykutatás jelenleg pusztán a politikai tevékenység egyik eszköze”.[2] Jelen tanulmánynak ugyanakkor nem témája a konzultáció tartalmának tárgyalása vagy esetleges bírálata.

A közvetlen kapcsolat az állampolgár és a döntéshozó között a közvetlen demokráciának fontos eleme. Ez utóbbi típusú demokrácia gyakorlati bevezetése ellen eddig az az érv szólt, hogy anyagilag nem volt megoldható az athéni *agora* megvalósítása, azaz hogy minden egyes állampolgár jelen tudjon lenni a döntéshozatalnál egy helyen és egy időben. Az informatika egyik gyakran említett ígérete az, hogy bár virtuális formában, de végre valósággá válhat a közvetlen népszuverenitás utópiája. Ha az állampolgár mostantól akár otthonról is szavazhat bármilyen ügyről, akkor technikailag már nincs akadálya egy korlátlan számú referendumnak korlátlan számú témáról.

Egyre több civil szervezet,[3] politikai párt[4] és cég[5] támogatja a digitális, közvetlen vagy legalább résztvevő demokráciát. Ez a tendencia megfigyelhető mind a jobb-, mind a baloldali pártoknál. Ráadásul olyan országokban is, amelyekre nem is gondolnánk, például Oroszországban, a Change.org petíciós portál az ötödik legnagyobb nemzeti felhasználói csoport.[6]

Nagyon valószínűnek tűnik, hogy egyre több ilyen típusú konzultációra fog sor kerülni a jövőben. Így kiemelten fontos nemcsak azon gondolkodni politika-filozófiai szempontok alapján, hogy örvendetesek-e az ilyen konzultációk, hanem arról is, hogy ha már úgyis léteznek, akkor megfelelő körülmények között történjenek.

1 www.kormany.hu/hu/a-kormanyszovivo/hirek/elo-kozvetites-kormanyszovivoi-sajtotajekoztato-konzultacio, 2016 június 23.

2 Pierre Bourdieu: L'opinion publique n'existe pas. *Questions de sociologie,* Párizs, Les Editions de Minuit, 1984. 222.

3 Például Youth decides Tunéziában, G0V Tajvanban.

4 Franciaországban létezik egy új regisztrált politikai párt „Baztille” néven, amely azt ígéri szavazóinak, hogy mandátumhoz jutása esetén azokat a döntéseket fogja képviselni, amikről az állampolgárok közvetlenül egy okostelefonos alkalmazáson szavazhatnak (www.baztille.org).

5 Például Voxe.org, Cap-Collectif, GOV, Change.org, Bluenove.

6 Forrás: Benjamin Des Gachons, a Change.org Franciországi országos igazgatója. Első Szeminárium a Digitális Demokráciáról, Párizs, Nemzetgyűlés, 2015. 11. 05.

A Snowden-ügy nagy erővel hangsúlyozta a magánélet védelmének fontosságát az állami megfigyelés ellen. Bebizonyította, hogy az állampolgárok átfogó megfigyelése nemcsak diktatúrákban fordul elő, hanem liberális demokráciákban is.

A nemzeti konzultáció során a végrehajtó hatalom politikai véleményadatokat gyűjt a saját állampolgárairól. Ezért fontos vizsgálni, hogy ezeket az adatokat hogyan kezeli, és milyen lépéseket tud tenni az ilyen típusú adatkezelés folyamatos javítása érdekében.

Jelen tanulmány több részből áll. Elsősorban vizsgálja a jelenlegi magyar nemzeti konzultáció gyakorlatát, és összehasonlítja azt a 2011-es szociális konzultációval. Ezt követően tárgyalja, hogy külföldön, különösképpen Franciaországban milyen gyakorlatok léteznek. A végén kísérletet tesz arra, hogy jogász- és politológusszemmel tekintsen az informatikai tanulmányokra a témában.

A jelenlegi magyar gyakorlat

Jelen tanulmányban három magyar nemzeti konzultációt elemzünk: a 2011-es szociális konzultációt (a továbbiakban: szociális konzultáció), a 2015-ös konzultációt a bevándorlásról és a terrorizmusról (a továbbiakban: bevándorlási konzultáció), valamint a 2015-ös, csak az interneten lefolytatott, internetről szóló konzultáció (a továbbiakban: internetes konzultáció).

A fent felsorolt magyar nemzeti konzultációk keretében lezajlott adatkezeléseket két hatályos jogszabály fényében fogjuk vizsgálni: az első a magyar 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.), a másik 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 (a továbbiakban: adatvédelmi irányelv).

A fenti jogszabályokat három doktrínaforrás segít majd értelmezni: a 29. cikk szerinti munkacsoport véleménye, ami az európai adatvédelmi hatóságoknak a brüsszeli közös tanácsadó testülete (a továbbiakban: 29-es Munkacsoport), a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) döntései és véleményei és különösen a NAIH 2015-ös ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről.

Háttérinformációként fontos megemlíteni, hogy a 2011-ben folytatott szociális konzultációt számos politikai és jogi vita övezte, ami magyarázza azt, hogy máig magas politikai és médiaérdeklődés létezik a konzultációk adatvédelmi kérdései iránt. A konzultációt ugyanis dr. Jóri András adatvédelmi biztos megtiltotta, és az összegyűjtött adatok törlésére szólította fel az adatkezelőt.[7] Amikor ez a döntés és felszólítás megtörtént, már folyamatban volt a magyar adatvédelmi intézmény reformja, hiszen a Parlament már megszavazta az új Infotv.-t, ami a régebbi adatvédelmi törvény (a továbbiakban: Avtv.) helyett lépett hatályba 2012. január 1-jén. E törvény többek

7 ABI-1642-9/2011/H.

között függetlenítette az adatvédelmi intézményt az ombudsmani rendszertől, amihez az adatvédelmi biztos tartozott. Így jött létre a NAIH mint új autonóm igazgatási szerv. A köztársasági elnök a miniszterelnök javaslatára nem Jóri András választotta a NAIH elnökének, hanem dr. Péterfalvi Attilát, aki korábban maga is adatvédelmi biztos volt. Végül az Európai Unió Bírósága (a továbbiakban: EUB) 2014-ben megállapította, hogy Magyarország Jóri András adatvédelmi biztos mandátumának idő előtti megszakításával megsértette az adatvédelmi biztos függetlenségének követelményét,[8] amely az adatvédelmi irányelv 28. cikkében elő van írva. Az ügy azóta már politikailag is lezárult a magyar kormány és az Európai Bizottság között: a magyar kormány kártérítést fizetett Jóri Andrásnak.[9]

Az adatvédelmi biztos számos ponton kritizálta a szociális konzultáció adatkezelését. A több mint tíz oldalas döntés összes érvét nem lehet itt részletesen felsorolni, de röviden összefoglalva a fő kifogás az volt, hogy nem megfelelő az érintett személy (ideértve: a részt vevő állampolgárok) tájékoztatása. A 3.2.8. bekezdés szerint: „Sem a hozzájáruló nyilatkozat szövegében, sem máshol nincs – még jogszabályra hivatkozás szintjén sem – az érintettek Avtv.-beli[10] jogaira és jogorvoslati lehetőségeire (Avtv. 11–15. és 17–18. §) vonatkozó tájékoztatás."

A Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (a továbbiakban: KEK KH), ami egy kormányhatározat alapján a szociális konzultáció adatkezelője volt,[11] az adatvédelmi biztos döntésének bírósági felülvizsgálatát kérte. A perre soha nem került sor, mert Péterfalvi Attila – mint a NAIH elnöke – 2012. január 1-jén megkezdte mandátumát, és egy újabb határozattal[12] módosította az adatvédelmi biztos korábbi döntését. Míg az előző döntés *minden* adat megsemmisítését írta elő, a NAIH már csak azoknak a későbbi kapcsolattartást szolgáló kontaktadatoknak a megsemmisítését kérte, amelyekhez az érintett személy a kitöltendő íven nem adott hozzájárulást. A kormány a NAIH előírásait követve változtatott az adatvédelmi gyakorlatán.

A bevándorlási konzultáció papír alapú változata már nem tartalmazza azt az ívet, amin az érintett személy a személyes adatait fel tudná tüntetni. A feltett kérdésekre viszont az interneten is lehetett válaszolni, és aki részt akart venni, annak ki kellett tölteni a személyes adatait. Fontos megemlíteni, hogy ugyan kötelező volt a személyes adatok megosztása, az internetes kérdőív tartalmazott adatvédelmi tájékoztatót. Továbbá, mivel a postai úton kiküldött kérdőív már semmilyen lehetőséget nem adott arra, hogy a válaszoló állampolgár személyes adatot vezessen rá, ezért e cikkben először a bevándorlási konzultáció weboldalának[13] adatvédelmi tájékoztatóját fogjuk vizsgálni.

8 EUB 2014. április 8. „Európai Bizottság kontra Magyarország" C-288/12.
9 Europe Direct Contact Centre információi alapján (Case ID: 1062957/1471337).
10 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.).
11 Szociális konzultációval összefüggő feladatok ellátásáról szóló 1137/2011. (V. 6.) kormányhatározat.
12 NAIH-5638-1/2012/H.
13 http://nemzetikonzultacio.kormany.hu/, 2015. július 28.

Önmagában változást jelent az, hogy van csatolt adatvédelmi tájékoztató, bár e tájékoztatót – a láthatóság és egyértelműség érdekében – érdemes lett volna úgy elhelyezni, hogy a weboldalt böngésző érintett személy ne tudjon továbblépni, ne tudja elküldeni személyes adatait anélkül, hogy legalább lássa az adatvédelmi tájékoztatót. Ez utóbbi javaslat ugyan meghaladná a törvény előírásait, de mégsem lenne fölösleges az érintett személy tájékozottsága érdekében, főleg egy ilyen esetben.

Az Infotv. 20. §-a előírja, hogy milyen információnak kell szerepelnie egy adatvédelmi tájékoztatóban. Az adatvédelmi irányelv nem tartalmaz explicit felsorolást, viszont a 29-es Munkacsoport 10/2004. számú véleménye kimondja, hogy az Európai Unió adatvédelmi hatóságai szerint mik a kötelező kellékek.

A fent említett két listát a bevándorlási konzultáció webes változatának adatvédelmi tájékoztatójával az alábbiakban hasonlítjuk össze:

	Előírt információ a 29-es Munkacsoport szerint	**Előírt információ a magyar Infotv. 20. §-a szerint**	**Bevándorlási konzultáció internetes adatvédelmi tájékoztatója***
Adatkezelő neve	x	x	Miniszterelnökség
Adatfeldolgozó neve		x	Damit Informatikai Kft.
Adatkezelés célja	x	x	„A konzultáció célja, hogy Magyarország Kormánya nevében a Miniszterelnökség megismerje a bevándorlásról és a terrorizmussal kapcsolatos véleményét.”
Adatkezelés jogalapja		x	Hozzájárulás.
Adatok megismerésére jogosultak	x	x	Magyarország Kormánya: csak a kontaktadatok, és csak akkor, ha ehhez hozzájárult az érintett személy.
Adatvédelmi nyilvántartási szám		x	Hiányzó adat.
Az adat megadásának kötelező vagy fakultatív jellege	x	x	Meg van jelölve, hogy milyen adat kötelező vagy fakultatív jellegű ahhoz, hogy az érintett részt vehessen a konzultációban.
Az adatok esetleges továbbítása vagy annak kizárása	x		Nincsen ugyan explicit módon leírva, de a szövegből egyértelmű, hogy kizárt.

* A teljes szöveg sajnos már nem elérhető a neten, és az Archive.org sem őrzött belőle másolatot. Az adatvédelmi tájékoztató ezen a címen volt elérhető: http://nemzetikonzultacio.kormany.hu/, 2015. július 28.

Az érintettek jogainak ismertetése	x	x	Az érintettek jogaik érvényesítéséhez postai úton fordulhatnak az adatkezelőhöz, illetve a NAIH-nál tehetnek panaszt.
Az adatkezelés időtartama		x	A konzultáció végéig, vagy – ha az érintett személy hozzájárult ahhoz, hogy további kapcsolattartás érdekében tovább kezeljék az adatait – addig, amíg hozzájárulását nem vonta vissza.

A fenti táblázatból kiolvasható, hogy a bevándorlási konzultáció adatkezelésének egyetlen fontosabb hiányossága az, hogy nincsen feltüntetve a pontos NAIH nyilvántartási szám. Továbbá vannak olyan hiányzó részletek (mint az adatfeldolgozó pontos szerepe[14]), amiknek megjelölése a NAIH-nak az előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlása szerint jó gyakorlatnak minősülne. Ezek olyan részletek, amelyek az adatvédelmi tájékoztató minőségét javítanák, de hiányuk – ami tulajdonképpen inkább szabály a gyakorlatban, mint kivétel – nem eredményezi a teljes tájékoztató törvénytelenségét.

Példák a francia gyakorlatból

Franciaországban nem létezik nemzeti konzultáció ugyanabban az értelemben véve, mint Magyarországon. Viszont ott is vannak, habár más formában, konzultációs gyakorlatok. Ebből kettőt választottunk ki: a Nemzeti Közvita Bizottság (Commission nationale du débat public, a továbbiakban: CNDP) vitáit, valamint a 2015-ös internetes konzultációt a digitális köztársaságról szóló törvényjavaslatról[15] (a továbbiakban: digitális konzultáció).

A CNDP egy független igazgatási szerv,[16] mely létrejöttével az 1970-es évek végén világszerte elterjedt New Public Management elv szerint megkívánt pártpolitikai semlegességet kívánja biztosítani bizonyos technikai döntések terén. Ennek két célja van: egyrészt a döntések technikai minőségének javítása szakemberek bevonásával a döntési folyamatba, másrészt az államhatalom korlátozása.[17] Az elvet természetesen kritizálják is, hiszen gyakran ellentétbe kerülhet a demokrácia elvével és a választások legitimációs rendszerével. De amennyiben gyakorlattá válna a rendszeres nemzeti

14 A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről: „A Hatóság elvárja, hogy az adatkezelő a tájékoztatóban jelölje meg, hogy az adatfeldolgozó pontosan milyen tevékenységet lát el az adatkezelő számára." Letölthető: http://naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf

15 Projet de loi pour une république numérique.

16 Autorité administrative indépendante.

17 L. Allen Schick: *Les agences à la recherche de principes*. Revue de l'OCDE sur la gestion budgétaire, 2/1, 2002. 7.

konzultáció, érdemes lenne a CNDP modelljét kiindulási pontként tekinteni, hiszen ez növelhetné az állampolgárok bizalmát a konzultációs folyamatban. Egy másik érv egy ilyen megoldás mellett az lehetne, hogy így nem közvetlenül a kormány, hanem egy autonóm szervezet kezelné a személyes adatokat.

Nyilvánvaló, hogy nem lenne észszerű közvetlenül átvenni egy külföldi mintát. Példának okáért: a CNDP kizárólag helyi infrastrukturális befektetésekről írhat ki közvitát vagy konzultációt. Ennek következtében nincs róla külön törvény, pusztán csak a Környezetvédelmi Törvénykönyv[18] egy cikkelye említi meg. Az erről folytatott kutatások jól mutatják, hogy helyi fórumokon a résztvevők nem annyira politikai kérdésekre, mint inkább személyes vagy kifejezetten helyi kérdésekre fókuszálnak, ami a CNDP missziói keretében ugyan releváns,[19] de nem terjeszthető ki a magyar nemzeti konzultáció céljaira. Emiatt nem lehet összehasonlítást végezni a magyar nemzeti konzultáció és a francia CNDP konzultációi között.

A digitális konzultáció viszont már jobban hasonlít a magyar konzultációs gyakorlatra, hiszen ugyanúgy országos politikai kérdésekről szól. A honlapján megtalálható, a digitális köztársaságról szóló törvényjavaslat több témát is érint. Ezek többek között: a személyes adatok védelme, az internet semlegessége, a forgalomirányító szolgáltatások szabályozása, valamint az információszabadság és az Open Data.

A weboldalon bárki tehetett javaslatot egy új szakaszra vagy egy szakasz módosítására. Ezekről a javaslatokról (beleértve a törvényjavaslat eredeti szövegét is) mindenki szavazhatott. A résztvevők indokolhatták is voksukat, és így vita is keletkezhetett a résztvevők közt.

A digitális konzultáció 2015. szeptember 26-tól október 18-ig tartott. A 21 330 regisztrált felhasználó 147 710 szavazatot adott le és 8501 bejegyzést írt.[20] A regisztrált felhasználók nagy része magánszemélyként regisztrált, azonban több, a digitális szabadságban érdekelt civil szervezet (pl. Quadrature du Net, APRIL), ipari érdekképviselet (pl. Medef, ami egy országos ipari és munkaadói képviselő szövetkezet), illetve cég (pl. Tripadvisor) is megtalálható volt a regisztráltak között. Volt olyan is, aki a konzultációban magánszemélyként vett részt, de tagja egy civil vagy egy érdekképviselői szervezetnek.

A két csoport – tehát a civil szervezetek és az érdekképviseleti szervezetek – egymástól eltérő stratégiát alkalmaztak. A civil szervezetek főleg ajánlásokat tettek, *agenda setting* céllal. Egyes javaslatokat a digitális gazdaságért felelős államtitkárság be is vett a törvényjavaslatba. Ilyen volt többek között a Quadrature du Net ajánlása

18 Art. L-121-1 du Code de l'environnement.

19 Clément Mabi: *Le numérique pour favoriser l'inclusion des publics?* Etude des logiques d'équipement des débats publics CNDP. 2015.

20 Forrás: République Numérique: www.republique-numerique.fr/consultations/projet-de-loi-numerique/consultation/consultation.

arra, hogy a francia adatvédelmi hatóság hivatalos célkitűzései közé tartozzon a titkosítási módszerek népszerűsítése.[21]

A másik csoport később kezdett regisztrálni a portálon. Így az Alliance Française des Industries du Numérique (Francia Digitális Iparágak Szövetsége, a továbbiakban: AFNUM) csak október 14-én regisztrált, pár nappal a konzultáció vége előtt. Stratégiájuk főleg arra összpontosított, hogy ellenezzék azokat a hivatalos javaslathoz tartozó részeket, amik ütköznek érdekeikkel.

A regisztrációhoz három módszer állt az állampolgárok rendelkezésére: egyszerű regisztráció, Facebook-os regisztráció, valamint Google Plus-os regisztráció.

Az egyszerű regisztrációhoz a következő adatokat kérte a weboldal: a regisztrált felhasználó típusa (magánszemély, cég, egyesület stb.), a teljes név, az e-mail-cím, valamint a jelszó. Minden adat kitöltése kötelező volt. A név mezőt a „nom complet" (teljes név) felirat jelezte, így a rendszer láthatóan a felhasználó valódi nevét kérte. A gyakorlatban viszont sok felhasználó álnevet választott magának, hiszen a regisztrált név nyilvánosan elérhető volt a weboldalon, csakúgy, mint a felhasználó összes szavazata, javaslata és egyéb bejegyzései.

Ha a felhasználó a Facebook API-n keresztül regisztrált, akkor a nyilvános profilt és az e-mail-címet is eléri a konzultációs rendszer. A Facebook nyilvános profilja a következő adatokat tartalmazza: név, profilkép, korcsoport, nem, nyelvpreferenciák, a felhasználó országa, valamint „egyéb nyilvános adatok". Ezek az adatok messze túlmennek a kijelölt célon, és semmi nem indokolja azt, hogy a digitális konzultáció szervere több adatot kérjen azoktól, akik a Facebook-on keresztül regisztrálnak, mint azoktól, akik az egyszerű regisztrációt választják.

A digitális konzultáció formai adatvédelmi szabályai betartásának szintjét tovább rontják az adatvédelmi tájékoztató hiányosságai. Az 1978. évi 78–17. törvény az informatikáról és a szabadságjogokról[22] (a továbbiakban: francia adatvédelmi törvény) 32. §-a írja elő, hogy mit kell tartalmaznia egy adatvédelmi tájékoztatónak (hasonlóan a magyar Infotv. 20. §-ához). A jogszabályi előírásokat szintén összehasonlítottuk a konkrét adatvédelmi tájékoztatóval.

21 Az új szakasz megtalálható az Államtanácshoz küldött törvényjavaslat verziójában: Art. 25, Projet de loi pour une République Numérique: www.republique-numerique.fr/project/projet-de-loi-numerique/step/projet-de-loi-transmis-au-conseil-d-etat.

22 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

	Előírt információ a 29-es Munkacsoport szerint	**Előírt információ a francia adatvédelmi törvény 32. §-a szerint**	**Nemzeti konzultáció internetes adatvédelmi tájékoztató***
Adatkezelő neve	x	x	A tájékoztató csak a Cap Collectif céget azonosítja, ami valójában nem az adatkezelő, hanem az adatfeldolgozó.
Adatkezelés célja	x	x	„A weboldal működtetése" (de ezen a célon túlmegy az adatok gyűjtése, főleg ha Facebook-on keresztül regisztrál a felhasználó).
Adatok megismerésére jogosultak	x	x	„A Kormány az adatok egyetlen címzettje."
A adatok megadásának kötelező vagy fakultatív jellege	x	x	Elő van írva, hogy milyen adat megadása kötelező/fakultatív.
Az adatok esetleges továbbítása vagy annak kizárása	x	x	A francia törvény szerint ezt csak akkor kell jelezni, ha történik ilyen adattovábbítás.
Az érintettek jogainak ismertetése	x	x	Az előírtak szerint az érintett személy megadhat egy e-mail-címet, ami az adatfeldolgozóhoz tartozik. Erre a címre írva gyakorolhatja többek között hozzáférési, módosítási és törlési jogait. Nincs viszont semmi utalás arra, hogy az adatvédelmi hatósághoz is fordulhat.
Adott esetben, tájékoztatni kell az érintett személyt arról, hogy milyen következményekkel jár, ha tagadja a válaszadást		x	Nincs következmény, ha az érintett személy nem kíván valamilyen adatot közölni, így az adatvédelmi tájékoztató nem tér ki erre.

* Az adatvédelmi tájékoztató két részből áll. A „Confidentialité" című oldalon a cookie-k használatáról tájékoztatják a felhasználót. A „Charte" című oldalon pedig egy paragrafus található, ami adatvédelmi tájékoztatóként szolgál.

Két következtetés vonható le a fenti elemzés alapján. Az első az, hogy a magyar joghoz képest a francia adatvédelmi jog követelményei viszonylag lazábbak az adatvédelmi tájékoztatást illetően. Álláspontunk szerint az egyik fő hiányosság az, hogy az érintett fél nem tudja, adatait meddig kezelik. Ez ugyan nem ütközik a 29-es Munkacsoport már korábban említett, 10/2004. számú véleményével, de mégis hiányosságnak minősíthető, amit azonban az új európai adatvédelmi rendelet 14. § 2. a) paragrafusa pótolni kíván.[23]

A másik észrevétel az, hogy még ha pontosan meg is lett volna jelölve az adatkezelő és az adatfeldolgozó, akkor is csak minimálisan teljesülnek a tájékoztatási kötelezettségek, és nincsen összhangban a kijelölt céllal mindaz a sok adat, amit a Facebook-tól kér a rendszer. Ez arra mutat, hogy a weboldal fejlesztői vélhetően kevés gondot fordítottak az adatvédelemre.

Ebből az következik, hogy a francia digitális konzultáció esetében mindenki, akinek van internetkapcsolata, megtudhatja, ki hogyan szavazott. Noha a felhasználók titkolni tudták valódi nevüket, az adatkezelő mégis tudhatja, hogy ki van az álnév mögött, hiszen minden esetben ki kell tölteni egy helyes e-mail-címet. Ráadásul az adatfeldolgozó http-szervere biztonsági okokból tárolja azt a naplót, amin megtalálhatóak az érintettek IP-címei. Ezek egyrészt személyes adatoknak minősülnek (ahogy az EUB már többször is kimondta[24]); másrészt összeköthetők az oldalra feliratkozott felhasználókkal, hiszen megteremthető a kapcsolat aközött, hogy egy IP-cím mikor töltött le egy oldalt és hogy mikor érkezett a rendszerbe egy bizonyos felhasználó szavazata. Ráadásul ezekről az adatokról nem tudjuk, hogy meddig tárolja a kormány, illetve a feldolgozó.

Ennek ellenére, habár adatvédelmi szempontból javítandó, a digitális konzultáció egy érdekes kísérlet arra, hogyan lehet átlátható módon bevonni a civil társadalmat, az állampolgárokat, valamint az érdekképviseleteket egy online konzultációba, ami túlmutat egy egyszerű kérdőíven, hiszen lehetőséget nyújt például javaslatok tételére.

Az adatvédelem technikai oldala

Eddig csak az adatvédelem formai követelményeit vizsgáltuk – ami fontos ugyan, de nem elegendő. A szakirodalom bőséggel tárgyalja, hogy miben különböznek az adatvédelemmel kapcsolatos jogi és informatikai elképzelések.[25] Eredetileg a jogi megkö-

23 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 (általános adatvédelmi rendelet).

24 EUB 2008. január 29., „Promusicae" C-275/06, illetve EBU 2011. november 24., „Scarlet kontra SABAM" C-70/10, § 51.

25 Lásd többek között: Sergio Mascetti – Anna Monreale – Annarita Ritti – Andrea Gerino: *Anonimity: A Comparison Between the Legal and Computer Science Perspectives.* In: Serge Gutwirth – Ronald Leenes – Paul De Hert – Yves Poullet (eds.): *European Data Protection: Coming of Age.* Dordrecht, Springer, 2013. 85.

zelítés szerint egy személyes adat elvileg vagy személyes, vagy nem.[26] Egy ilyen megközelítés alapján nem személyes adat egy anonimizált adat. Több informatikai tanulmány azonban kimutatta, hogy – Paul Ohm szavai szerint – az erős anonimizáció (*robust anonimity*) csupán „mítosz"[27]

Nem lenne helyénvaló azonban azt állítani, hogy a jogi koncepciók egyáltalán nem veszik figyelembe az informatikai szempontokat. Az adatvédelmi irányelv 17. §-a, valamint a magyar Infotv. 7. §-a például az adatbiztonság informatikai, technikai követelményeit írja elő. Az utóbbi 6. paragrafusa magában foglalja: „Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek." Ezt az elvet a magyar bevándorlási konzultáció esetében nem sikerült teljes mértékben átültetni a gyakorlatba, a konzultáció honlapja ugyanis a HTTPS-protokollal nem, csak a sokkal kevésbé biztonságos http-protokollal volt elérhető. A HTTPS bevezetése ma már standard eljárás, hiszen – amellett, hogy kevés erőforrást igényel – nem követel meg a felhasználótól semmiféle külön feladatot. Bár a francia digitális konzultáció honlapjára http-protokollal is lehetett csatlakozni, ebben az esetben az rögtön átirányított egy https://-al kezdődő címre.

A magyar bevándorlási konzultáció adatvédelmi tájékoztatója hangsúlyozta, hogy az adatok anonimizálva vannak, és hogy a véleményadatok nem kapcsolhatók össze a személyes kontaktadatokkal. Miután az adatkezelő elmulasztotta alkalmazni a bevett módszernek számító HTTPS-protokollt, felmerül a gyanú, hogy a konzultáció anonimizációs eljárása nem is volt annyira biztonságos gyakorlati és technikai szemszögből nézve, mint ahogy az a papíron állt.

A 29-es Munkacsoport 5/2014 számú számú véleménye, amely iránymutató a létező anonimizálási technikák tekintetében,[28] fontos különbséget tesz az anonimizálás és a pszeudonimizálás gyakorlata között. Az anonimizálás esetében az adat semmilyen módon nincs összekötve azzal a személlyel, akire vonatkozik. Ezzel szemben a pszeudonimizálás esetében az történik, hogy a nevet egy álnévre cseréljük. Az álnévből nem kereshető vissza az érintett személy, viszont a kialakított álnévvel minden olyan adatot azonosíthatunk, ami ehhez a személyhez fűződik.

26 Ez a koncepcionális különbség most már sokkal árnyaltabb. Az adatvédelmi törvények szerint is relatív a „személyes adat" fogalma, és attól függ, hogy mennyire képes az adott adatkezelő egy adatot a természetes személlyel összekapcsolni. Ennek ellenére a szakirodalomban és a gyakorlatban még egyaránt előfordulnak különbségek a jogi és az informatikai adatvédelmi koncepció között. Erről bővebben lásd: Mascetti, S. – Monreale, A. – Ricci, A. – Gerino, A.: *Anonimity: A Comparison Between the Legal and Computer Science Perspectives, i. m.* 85.

27 Paul Ohm: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review,* 57, 2010. 1701.

28 29. Cikk Szerinti Adatvédelmi Munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról.

A pszeudonimizálás sok esetben azért gyenge megoldás, mert általában marad olyan adat, ami visszakereshetővé teszi az adott személyt. Így – még ha el is tűnik a név – megmaradhat az adott személy neme, irányítószáma és születési dátuma. Ezek alapján bizonyos tanulmányok szerint az Egyesült Államok lakosságának a 80%-át azonosítani lehet.[29]

Egy másik, informatikabiztonsági szempontból fontos kérdés, hogy milyen fenyegetésekkel szemben kell védeni az adatokat. A bevándorlási konzultáció esetében három kockázattal kell számolni:

1. A végrehajtó hatalom valamelyik szerve meg akarja ismerni az állampolgárok személyes véleményét. Ez a fenyegetés tűnik a legvalószínűbbnek, és a szociális konzultáció esetében ez a veszély került a média érdeklődésének középpontjába.
2. Közepes kockázatnak minősül, hogy bizonyos személyek próbálhatják befolyásolni az eredményeket.
3. Kisebb – de abszolút elképzelhető és könnyen előforduló – kockázatnak minősül, ha valaki nem saját nevét, hanem egy másik személy adatait tünteti fel a konzultáció regisztrációs ívén.

Mivel a második kockázat szinte kizárólag informatikabiztonsági kérdés, amely inkább a statisztikai eredményt érinti, mintsem a személyes adatok védelmét, a továbbiakban az első és a harmadik veszélyre összpontosítunk. Hogyan védekezett az adatkezelő, valamint az adatfeldolgozó e kockázatok ellen? A NAIH segítségével ezzel a kérdéssel fordultunk a Miniszterelnökséghez, amelynek két névtelenséget kérő munkatársa 2015. október 2-án fogadott engem, valamint dr. Péterfalvi Attilát, a NAIH elnökét egy interjúra.

Az interjún – mivel erre kaptak engedélyt az informatikai szakértők – elsősorban az internetes konzultációról esett szó. Erre háromféleképpen lehetett regisztrálni:

1. Facebookon keresztül,
2. a kormány ügyfélkapuján át,
3. valamint egy sima regisztráción keresztül.

A Facebook-os regisztráció ellen a NAIH-nak csak egyetlen kifogása volt: ebben az esetben az a személyes adat, hogy az érintett személy részt vett a konzultáción, az Egyesült Államokba kerül. A NAIH ezért fontosnak tartotta, hogy más módon is lehessen regisztrálni. Ez elővigyázatos lépésnek bizonyult, ugyanis az EUB időközben visszamenőlegesen érvénytelennek nyilvánította a Safe Harbor-egyezményt, amely a Facebook jogalapjaként szolgált ahhoz, hogy személyes adatokat továbbíthasson az Egyesült Államokba.[30]

Ha a felhasználó a Facebook-on keresztül regisztrál, a Facebook egy kódot generál, amely a továbbiakban azonosítóként szolgál. Ez az azonosító teljesen egyedi: minden alkalmazás ugyanis, amely a Facebook API-n keresztül azonosítja felhasználóit,

29 Sweeney Latanya: Uniqueness of Simple Demographics in the U.S. Population. *Laboratory for Int'l Data Privacy Working Paper,* LIDAP-WP4s. 2000.

30 EUB 2015. október 6., „Schrems kontra Data Protection Commissionner" C-362/14.

egyedi számsort kap. Ez azt jelenti, hogy ha valaki a magyar internetes és a francia digitális konzultáción egyaránt a Facebook-on keresztül venne részt, akkor a magyar internetes konzultáció szoftvere más azonosító számsort kapna, mint a francia. Így sem a magyar, sem a francia fél nem tudná összekötni az adatait egymással a Facebook együttműködése nélkül. Ráadásul, a francia digitális konzultációval ellentétben – a megkérdezett miniszterelnökségi munkatársak szerint – a magyar adatkezelési rendszer kizárólag ezt az egyedi azonosítót kéri le a Facebook-ról, semmi egyéb személyes adatot.

Ha a felhasználó a kormány ügyfélkapuján keresztül azonosítja magát, akkor a konzultáció szervere egy egyedi kódot kap. Ezt a kódot az ügyfélkapu képezi négy különböző személyes adatból,[31] amelyekből hasítófüggvény használatával végzi el a pszeudonimizálást (amelynek a végeredménye az ún. *hash* kód). Ugyanez történik akkor is, ha a felhasználó a sima regisztrációt választja.

A hash kód elvileg nem visszafordítható, ami azt jelenti, hogy nem lehet visszafejteni a hashelt személyes adatokat. Az alábbi példa azt mutatja be, hogy mi történik a névvel, miközben keresztülmegy az MD5 függvényen:

- MD5(Csaladnév Béla) → 5d23d9ecdee872fc402d19d57c458de0
- MD5(Családnév Béla) → 70430fdaeeb478b9fd8ea4e291864124
- MD5(70430fdaeeb478b9fd8ea4e291864124) → 33bb9fc698221ae20b367820c3efe493

A hash rendszer viszont könnyen feltörhető, amennyiben az ellenfél ismeri:

- az alkalmazott függvényt: a függvények között kettő nagyon népszerű (az MD5 és az SHA-1), annak ellenére, hogy e kettő között egyik sem tekinthető teljesen biztonságosnak,[32]
- az eredeti adatokat: például annak ismeretében, hogy a hash-t a felhasználó családnevével és születési dátumával készítették, ami sok helyről beszerezhető és visszakereshető adat, vissza lehet keresni az adott személyt a hash adatok közül.

Egészében véve az állam mindkét információval rendelkezik. Ezért kifejezetten fontos annak lehetetlenné tétele, hogy az adatkezelő ismerje az algoritmust, amelynek segítségével az azonosító hash értékek létrejönnek. Ezt a célt szolgálhatja, ha a hash értéket képző szerver az ún. *salting* technikát is használja. Másrészt szervezeti értelemben megoldást kínálna az is, ha az adatkezelő a CNDP modellje alapján egy független szervezet lenne, amelynek nem érdeke összekapcsolni az adatokat és visszakeresni az érintett személyeket.

Tekintettel a fenti veszélyre, az internetes konzultáció rendszerét fejlesztő mérnökök a személyes adatok biztonságát azzal kívánták megerősíteni, hogy külön táblában

31 Az, hogy milyen adatról van szó, sajnos titkos maradt.

32 Agence nationale de la sécurité des systèmes d'information (ANSSI): Référentiel général de sécurité version 2.0. Annexe B1: Mécanismes cryptographiques. Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. Párizs, Premier Ministre, 2014: www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf (2016. június 30.). Jelenleg az amerikai National Institute of Standards and Technology szerint az SHA-3 algoritmust kell alkalmazni: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf (2016. június 30.)

kezelték a pszeudonimizált azonosító értékeket és a véleményadatokat, sőt az azonosító hash értékeket a konzultáció lezárása után törölték. Így a hash értéket a felhasználók válaszaival, tehát a véleményadatokkal sem lehetett összekötni – ami egy fontos és hatékony lépés volt az anonimitás lehető legnagyobb fokának biztosítása érdekében.

Maguk a véleményadatok (tehát a felhasználó által közölt válaszok) nem minősülnek személyes adatnak, mert e válaszokat olvasva lehetetlen visszakeresni a válaszok mögött álló személyt. Bár ez nem minden esetben állja meg a helyét, ezúttal a kérdések és a válaszok túl általánosak voltak ahhoz, hogy olyan egyedi válasz szülessen, amely alapján visszakereshető lenne az eredeti válaszadó.

Tekintettel a második veszélyre (arra, hogy valaki megpróbálja befolyásolni az eredményt), a konzultáció során egy ún. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) rendszert vezettek be, pontosabban a Google rendszerét, a reCAPTCHA-t. Ez a rendszer többek között az egérmozgások elemzésével képes elválasztani a felhasználókat a robotoktól, amelyek az eredmény befolyásolása érdekében például több ezer automatikus választ küldenek be. Így nem volt szükség a személyes adatoknak minősülő IP-címek kezelésére sem. Ez a megoldás azonban nem tudja kiküszöbölni a többszörös szavazás problémáját, amely megoldható úgy, ha valaki különböző Facebook-profilokat állít elő vagy különböző neveket használva jelentkezik be a sima regisztráción keresztül.

A harmadik veszélyre azonban nem született megoldás: a sima regisztráción keresztül a saját adatai helyett bárki be tudja ütni a szomszédjáét.

A Miniszterelnökség munkatársai szerint a bevándorlási konzultáció rendszere ugyanazokat az irányelveket követte, mint az internetes konzultáció, amelynek a technikai részleteit a fentiekben részleteztük.

Összefoglalásként: nem lehet tehát azt állítani, hogy a magyar konzultáció esetében az érintett személyek adatai nem megfelelő módon lennének kezelve. Az adatkezelők számára a véleményadatok egyedi személyekkel történő összekapcsolása (amely a hash adatok véleményadatokkal történő összekapcsolhatatlanságából következik) nehéz, ha éppen nem lehetetlen feladat. Mint láttuk azonban, bizonyos jelek arra utalnak, hogy van még mit javítani a rendszeren. Ez annál is inkább kívánatos volna, mivel egyre több ilyen típusú konzultációra kerül sor világszerte.

Azzal a dilemmával, hogy hogyan lehet egyszerre garantálni egy internetes szavazás vagy petíció anonimitását és a válaszok megbízhatóságát, az informatikai szakirodalom is foglalkozott. Jorn Lapon az ún. *anonymous identity credential* (anonim személyazonosság hitelesítés) rendszer bevezetését javasolta doktori disszertációjában.[33] Lapon javaslata – amelyet az informatikabiztonsági szakembereknek még tesztelniük kell, egy politológus vagy egy jogász ezt nem teheti meg – választ kínál arra a kockázati modellre, amelyet a fentiekben leírtunk, vagyis hogy 1. a konzultáció adatkezelője vagy a kormány összekapcsolhatja a véleményadatokat az érintett sze-

33 Jorn Lapon: *Anonymous Credential Systems: From Theory Towards Practice.* Doktori disszertáció. Leuven, Mérnöki kar, Leuveni Katolikus Egyetem, 2012.

mélyekkel, 2. egyesek megpróbálhatják tisztességtelenül befolyásolni a konzultációs folyamatot, 3. egy felhasználó egy másik személyként azonosíthassa magát a rendszerben, megszegve az adatok pontosságának elvét.

Az *anonymous identity credential* alapvetően egy olyan rendszer, amelyben a személyes adatok (amelyeken a hitelesítés alapul), valamint a felhasználói adatok (vagyis ez esetben a véleményadatok) külön vannak tárolva, és nemcsak külön táblában, hanem külön adatbázisban, sőt külön szerveren és külön adatkezelőnél. Az IBM *Identity Mixer* néven fejlesztett egy ilyen prototípust, amely azon az elven alapul, hogy a hitelesítést nem maga az alkalmazás végzi.

A hitelesítés folyamatát a következőképpen kell elképzelni. A konzultációs alkalmazásnak bizonyos személyes adatokra szüksége lehet, például megkövetelheti, hogy a felhasználók magyarok és nagykorúak legyenek. A személyes adatokat viszont nem a konzultációs alkalmazás fogadja be, hanem az ún. *Identity Provider* (személyazonosság-szolgáltató) szolgáltatja. Ha a felhasználó jelszóval vagy elektronikus személyigazolvány használatával[34] sikeres belépést hajt végre az *Idendity Provider*-en keresztül, az *Identity Provider* egy *identity credential* (azonosító levél) formájában átküldi a szükséges személyes adatokat a konzultációs alkalmazásnak, amely ez esetben két BOOLEAN-értékkel megoldható: magyar = TRUE [igaz] és nagykorú = TRUE [igaz]. A személy pontos korát nem szükséges átküldenie az alkalmazásnak.

A rendszer másik fontos pilléreként az *Identity Provider* szerverének természetesen megbízhatónak kell lennie. A magyar esetben a KEK KH lakcím-adatbázisa kínálhat a konzultációhoz megoldást. A 1992. évi LXVI. törvény szerint ugyanis:

> „(1) A Kormány által meghatározott ügyekben a kormányzati tevékenység összehangolásáért felelős miniszter
> a) a polgárok személyre szóló tájékoztatása, illetve
> b) a polgárok álláspontjának megkérdezése
> céljából a 17. § (2) bekezdés a) pontja szerinti adatok szolgáltatását jogosult kérni, a 11. § (1) bekezdés b), c), d), h) és k) pontjában meghatározott kiválasztási szempontok szerint."[35]

Jorn Lapon *PetAnon* nevű alkalmazásában a konzultációt szervező szerver is kér azonosító levelet az *Identity Provider*-től. Mind a felhasználó, mind a konzultáció azonosító levele egy aszimmetrikus kulcsú titkosítást alkalmaz. Ennek célja a két fél közötti kommunikáció biztonsága. A PetAnon, amelyről e tanulmány keretei között nem áll módunkban részletes leírást nyújtani, megoldást kínál a fenti kockázatokra, hiszen:

1. A véleményadatok és a személyes adatok teljesen szét vannak választva.
2. A *PetAnon* rendszer lehetővé teszi, hogy a felhasználó ellenőrizze: szavazata nem lett-e a szerveren módosítva, ezzel emelve a biztonsági és megbízhatósági szintet.

34 Jorn Lapon tanulmánya a belga eID elektronikus személyigazolvány rendszerén alapul.
35 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról, 19/A. §.

Ráadásul minden személy csak egyszer szavazhat, kizárólag abban az esetben, ha az *Identity Provider* szerver megerősíti az arra való jogosultságot.

3. Csak az szavazhat, akit az *Identity Provider* hiteles módon azonosít. Így egy felhasználó nem élhet vissza egy másik személy személyes adataival.

Az észt elektronikus szavazási rendszer, amelyet a 2005-ös önkormányzati választások után vezettek be, és amelynek segítségével minden észt állampolgár otthonról, az interneten keresztül szavazhat, részben hasonló eszközöket alkalmaz, mint Jorn Lapon anonim petíciós modellje. Fontos azonban megemlíteni, hogy bizonyos informatikai biztonsági szakértők szerint ennek a rendszernek is vannak riasztó hibái: „Az E-szavazás rendszernek fontos konstrukciós (*architectural*) és eljárási hiányosságai vannak, amelyek kockáztatják a választások integritását."[36] Ezért a jelenlegi próbálkozások – legyen szó a magyar, az észt vagy a különböző egyetemi kutatások keretében zajló kísérletekről – még csak kutatási fázisban tartanak. A megfelelő megoldás megtalálása érdekében e kísérletek elemzése és továbbfejlesztése, az informatikai kísérletek jogi szemszögből való folyamatos elemzése, valamint az interdiszciplináris párbeszéd ösztönzése elengedhetetlen feladat.

Összefoglaló és válasz a kutatás eredeti kérdésére

A kutatás, amin e rövid tanulmány alapult, abból a gyanúból indult ki, hogy a 2015-ös bevándorlási konzultáció *nem felel meg* az adatvédelmi jogszabályok előírásainak. De hamarosan nyilvánvaló lett, hogy bár lehet javítani az adatvédelmi tájékoztató minőségén – például a jogot nem jól ismerő állampolgár részére érthetőbb szöveg készítésével –, a médiabotrányt keltő 2011-es konzultációhoz képest sokkal jobban megfelel az előírásoknak. Sőt, elmondható, legalábbis ha a francia gyakorlattal vetjük össze, hogy a magyar gyakorlat nem tekinthető jogsértőnek vagy helytelennek az adatvédelmi jogok tekintetében.

Viszont nem elég, hogy egy adatkezelés *formálisan megfelelő* legyen. Hiszen még ha be is van jelentve az adatvédelmi hatóság nyilvántartásába és az érintett személyt megfelelően tájékoztatják, ettől még nem lehetünk biztosak abban, hogy az *informatikai műveletek megfelelőek* adatbiztonsági, illetve adatvédelmi szempontból. Több tanulmány jelent már meg arról, hogy mennyire távol állhat az anonimizálásról szóló jogi elképzelés a technikai valóságtól. Ezért egy másik fázisban új irányt vett a kutatás: hogyan oldották meg az állampolgár válaszainak anonimizálását technikailag?

Ehhez sok segítséget kaptam a NAIH-tól, különösen annak elnökétől, valamint a Miniszterelnökség munkatársaitól, akik válaszoltak technikai kérdéseimre. A válaszokból kiderült, hogy született egy olyan technikai megoldás, ami a megadott kockázat, illetve fenyegetési modellnek megfelelő anonimitást biztosít a válaszadók számá-

36 Zakir Durumeric – Travis Finkenauer – Alex J. Halderman – Harri Hursti – Jason Kitcat – Margaret Macalpine – Drew Springall: *Security Analysis of the Estonian Internet Voting.* Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS '14), november 2014.

ra. Az alkalmazott technika nem tökéletes: így maradnak kérdések a *hash* érték körül, és nem lehet biztosítani a jelenlegi rendszerrel, hogy egy adott személy ne írja be egy másik személy adatait, azzal például kizárva, hogy e másik személy részt vehessen a konzultációban.

A Jorn Lapon által kidolgozott e-petíció rendszere kísérletet tesz arra, hogy egy *anonymous identity credential* rendszer alkalmazásával az állampolgár biztonságosan, anonim és az adatkezelő szemszögéből tekintve megbízható módon tudja magát azonosítani egy internetes konzultáción. Ez a modell ráadásul elvileg ellenőrizhető, és biztosítja azt, hogy senki ne tudja magát más személyként azonosítani. Ezzel nemcsak növeljük a konzultáció folyamatának és eredményeinek társadalmi megbízhatóságát és elfogadottságát, hanem olyan rendszert alakítunk ki, ami jobban megfelel a személyes adatok pontosságát előirányzó törvényi rendelkezésnek (Infotv. 4. § 4. bekezdés).

Technikai szempontból tehát még van hová fejlődni, és érdemes lenne egy közös kutatási projektet indítani jogászok és informatikusok között, ami tesztelni tudná jogilag, valamint informatikabiztonságilag többek között a mostani magyar konzultációs programot, illetve a Jorn Lapon által kidolgozott megoldást.

Zárszóként azt is fontosnak tartom megemlíteni: ahhoz, hogy a nemzeti konzultáció valóban hozzájáruljon a közvetlen demokráciához vagy a Habermas-féle diszkurzív demokráciához, nélkülözhetetlen a bizalom a konzultációs folyamat semlegességében. A kérdés már nem pusztán jogi, hanem politikatudományi, ezért túlmutat jelen tanulmány keretein. Ennek ellenére személyes meggyőződésem, hogy ez egy kizárhatatlan kérdés és potenciális szakmai kutatási cél.

Irodalomjegyzék

29. Cikk Szerinti Adatvédelmi Munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról.

Agence nationale de la sécurité des systèmes d'information (ANSSI): *Référentiel général de sécurité version 2.0. Annexe B1: Mécanismes cryptographiques. Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.* Párizs, Premier Ministre, 2014.

Pierre Bourdieu: *L'opinion publique n'existe pas. Questions de sociologie.* Párizs, Les Editions de Minuit, 1984

Zakir Durumeric – Travis Finkenauer – Alex J. Halderman – Harri Hursti – Jason Kitcat – Margaret Macalpine – Drew Springall: *Security Analysis of the Estonian Internet Voting.* Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS '14), november 2014.

Jorn Lapon: *Anonymous Credential Systems: From Theory Towards Practice.* Doktori disszertáció. Leuven, Mérnöki kar, Leuveni Katolikus Egyetem, 2012.

Sweeney Latanya: Uniqueness of Simple Demographics in the U.S. Population. *Laboratory for Int'l Data Privacy, Working Paper,* LIDAP-WP4s. 2000.

Clément Mabi: *Le numérique pour favoriser l'inclusion des publics?* Etude des logiques d'équipement des débats publics CNDP. 2015.

Sergio Mascetti – Anna Monreale – Annarita Ritti – Andrea Gerino: *Anonimity: A Comparison Between the Legal and Computer Science Perspectives.* In: Serge Gutwirth – Ronald

Leenes – Paul De Hert – Yves Poullet (eds.): *European Data Protection: Coming of Age.* Dordrecht, Springer, 2013.

National Institute of Standards and Technology: FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions and Revision to the Applicability Clause of FIPS 180-4, Secure Hash Standard, 2015. augusztus 5., http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf (2016. június 30.)

Paul Ohm: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review,* 57, 2010. 1701–1777.

L. Allen Schick: Les agences à la recherche de principes. *Revue de l'OCDE sur la gestion budgétaire,* 2/1, 2002.

Bírósági döntések

EUB 2008. január 29., „Promusicae" C-275/06, illetve EBU 2011. november 24., „Scarlet kontra SABAM" C- 70/10.

EUB 2014. április 8., „Európai Bizottság kontra Magyarország" C-288/12.

EUB 2015. október 6., „Schrems kontra Data Protection Commissionner" C-362/14.

Hatósági döntések

ABI-1642-9/2011/H

NAIH-5638-1/2012/H

Jogszabályok

1. Európai Unió

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 (adatvédelmi irányelv).

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 (általános adatvédelmi rendelet).

2. Franciaország

Code de l'Environnement (Környezetvédelmi Törvénykönyv).

Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (francia adatvédelmi törvény).

3. Magyarország

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.).

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról.

Szociális konzultációval összefüggő feladatok ellátásáról szóló 1137/2011. (V. 6.) kormányhatározat.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).