

## Sandra Särav - Tanel Kerikmäe - Kasper Ágnes: Az e-polgárság mint a virtuális migráció eszköze Észtországban

### Hivatkozás/reference:

Sandra Särav - Tanel Kerikmäe - Kasper Ágnes, „Az e-polgárság mint a virtuális migráció eszköze Észtországban”, *Információs Társadalom*, XVI. évf. (2016) 2. szám, 8-31. old.

<http://dx.doi.org/10.22503/inftras.XVI.2016.2.1>

## Információs Társadalom

Sandra Särav – Tanel Kerikmäe – Kasper Ágnes:  
Az e-polgárság mint a virtuális migráció eszköze Észtországban

Galántai Zoltán:  
Big Data, tudomány, kauzalitás

Horatiu Dragomirescu – Michalis Vafopoulos:  
Az információtól a Webonomiáig: Hogyan alakítja az információs és kommunikációs technológia az információról, mint az üzleti tevékenység tárgyáról alkotott képünket?

2016. XVI. évfolyam 2. szám

2015-ben nemzetközi figyelmet keltett Észtország legújabb „találmánya” – az e-polgárság. Az Európai Unió eme kicsiny, de digitalizáltság szempontjából igen fejlett tagállama számára külön kihívást jelentett, hogy elmagyarázza a világ számára ez mit is takar, bár még nem reklámozták az e-polgárságot. Magyarország sem késlekedett érdeklődést mutatni az ötlet iránt, többek között azért sem, mert éppen a magyar e-kártya koncepciója volt kidolgozás alatt. Számos cikk jelent meg a sajtóban, amelyek beszámoltak az észt fejleményekről, bár gyakran a pontatlan fogalmazás miatt a valóditól eltérő képet festettek az e-polgárság mibenlétéről. Alapvetően az észt digitális személyazonosság vagy e-polgárság az észt állampolgársággal (vagy tartózkodási joggal/ engedéllyel) nem rendelkező személyek számára számos olyan jogot biztosít, amely többsége világszinten is ismeretlen, és lehetővé teszi az ország digitális szolgáltatásainak használatát a világ bármely pontjáról. Mindezek mellett az még kevésbé ismert, hogy milyen keret-szabály-rendszer biztosítja az „ország- mint-szolgáltatás” működését és hol vannak az e-polgárság problematikus, kiegyen-súlyozatlan vetületei. Jelen tanulmány célja az, hogy pontosítsa a magyar nyelven elérhető információkat és rámutasson arra, hogy az e-polgárság, bár technikai szem- pontból biztonságos, koncepciója még nem teljesen kiforrott és a közeljövőben számos buktatóval kell majd az észteknek szembesülniük. A szerzők reményei szerint eme tanulmánnyal hozzájárulnak ahhoz, hogy a magyar szakértők pontosabb képet kapjanak az észt gyakorlatról, beleértve a sikereket és nehézségeket is.

**Kulcsszavak:** e-polgárság, e-rezidens, Észtország, digitális személy-azonosság, e-kormányzat, virtuális bevándorlás

### The means of virtual migration – e-residency in e-Estonia

In 2015 the latest “invention” to come out of Estonia made it into the headlines. It was quite a challenge for this small, yet digitally advanced EU Member State, to explain to the world what e-residency really stands for, although they are not yet campaigning for it. There was no delay in Hungary expressing interest in the idea since the new concept of the Hungarian e-card was just under development at the time. Numerous media reports outlined the Estonian developments, however, the imprecise wording often gave the wrong impression about e-residency. In essence Estonian digital identity or e-residency bestows the right upon non-citizens (or nonresidents) to use the country’s numerous digital services from anywhere in the world. In addition the regulatory framework that ensures the functioning of this “country-as-a-service”, the problematic spots and unbalanced aspects of e-residency are even less well known. The aim of this study is to clarify the available information in Hungarian and point out that e-residency, although technically secure, is an incomplete concept and the Estonians will encounter certain pitfalls. The authors hope that this study will provide Hungarian experts with a more precise picture about the Estonian practice, including the successes and difficulties involved.

**Keywords:** e-residency, e-Stonia, Estonia, digital identification, e-government, virtual migration

A folyóiratban közölt művek a *Creative Commons Nevezd meg! - Ne add el! - Így add tovább! 4.0 Nemzetközi Licenc* feltételeinek megfelelően használhatók.

Sandra Särav – Tanel Kerikmäe – Kasper Ágnes

## Az e-polgárság, mint a virtuális migráció eszköze Észtországban

### Bevezetés

2014 októberében, arra adott válaszként, hogy az Apple bemutatta a PDF-dokumentumok trackpad használatával történő aláírásának lehetőségét, az Észt Köztársaság miniszterelnöke, Taavi Rõivas, a következő bátor hangú megjegyzést tette közzé Twitter-mikroblogján: „Kedves Apple, ha arra kíváncsiak, hogy a fájlokat hogyan kell a gyakorlatban digitális úton aláírni, lépjenek kapcsolatba bármelyik észt állampolgárral. Üdvözlettel, Taavi.”<sup>1</sup> Valóban, az észt nép tudatos internethasználó – a 2016. december 22-én fennálló helyzet szerint 1 279 293 észt lakos rendelkezett aktív személyazonossági kártyával, amelyeket 502 476 256 alkalommal használtak elektronikus hitelesítésre, 337 473 559 alkalommal pedig dokumentumok elektronikus úton történő aláírására.<sup>2</sup> Mivel Észtországnak hozzávetőlegesen 1 320 000 lakosa van, mindez azt jelenti, hogy az észt polgárok nagyjából 95%-a valóban tudja, hogyan kell egy okmányt elektronikus úton aláírni. Digitális személyi igazolványuk,<sup>3</sup> valamint az egyéb internetes megoldások használata révén az észttek ténylegesen a virtuális térben élnek – 2016-ban az adózók 96%-a nyújtotta be adóbevallását az interneten keresztül,<sup>4</sup> a banki tranzakciók 99,6%-át online bonyolították,<sup>5</sup> továbbá a szavazati joggal rendelkező polgárok 33%-a e-szavazatot adott le a 2015-ös országos parlamenti választáson.<sup>6</sup> Az állampolgároknak a rendszerbe vetett bizalmát továbbá szemmel láthatóan növeli az a tény is, hogy Észtország az internettel leginkább ellátott és technológiailag legfejlettebb orszá-

<sup>1</sup> Az észt miniszterelnök Twitter-blogja: [https://twitter.com/TaaviRoivas/status/523530893613617152?utm\\_source=fb&utm\\_medium=fb&utm\\_campaign=TaaviRoivas&utm\\_content=523530893613617152](https://twitter.com/TaaviRoivas/status/523530893613617152?utm_source=fb&utm_medium=fb&utm_campaign=TaaviRoivas&utm_content=523530893613617152)

<sup>2</sup> A digitális személyi igazolványok és mobil személyazonosító eszközök hivatalos ügyfélkapujától származó statisztikai adatok. <http://www.id.ee>

<sup>3</sup> Elektronikus személyazonossági kártya. E-Estonia.com Elérhető angolul a következő helyen: <https://e-estonia.com/component/electronic-id-card/>

<sup>4</sup> Észtország a 2000. évben ténylegesen bevezette az elektronikus adóbevallást; kezdetben az emberek 3%-a nyújtotta be adóbevallását az interneten keresztül, majd 15 év elteltével ez az arány 94%-ra emelkedett. Az adatok az észt Adó- és Vámhatóság hivatalos évkönyveiből származnak. Elérhető angolul és észt nyelven a következő helyen: <http://www.emta.ee/index.php?id=34149&tpl=1026> és <http://www.emta.ee/index.php?id=14595>

<sup>5</sup> Észt Informatikai Hatóság. Tények e-Észtországról. Elérhető angolul a következő helyen: <https://www.ria.ee/en/facts-about-e-estonia.html>

<sup>6</sup> Az észtországi internetes szavazási szokásokra vonatkozó adatok az Észt Nemzeti Választási Bizottságtól származnak. Észt Nemzeti Választási Bizottság. Statisztika az internetes szavazásról. Elérhető angolul a következő helyen: <http://vvv.vvk.ee/voting-methods-in-estonia/engindex/statistics/> További adatokért lásd például: Madise, Ü. és Vinkel, P. Internet Voting in Estonia, in: Constitutional Debate to Evaluation of Experience Over Six Elections. Regulating eTechnologies in the European Union. Normative Realities and Trends. T. Kerikmäe (ed.) Springer, 2014, pp. 53-72.

gok körébe tartozik<sup>7</sup>, ahol a szólás- és véleményszabadságot az alkotmány védi<sup>8</sup>, az internethez való hozzáférés pedig emberi alapjog.<sup>9</sup>

Miközben azon országok körébe tartozik, ahol a tartalomkorlátozás a legenyhébb, Észtország egyfajta digitális tündérmese birodalmának is tűnik – számos e-kormányzati szolgáltatásával<sup>10</sup> az ország „modellértékűnek minősül az internethez való szabad hozzáférés mint a társadalom fejlődését szolgáló eszköz”<sup>11</sup> vonatkozásában. Mindezt alátámasztják az Európai Unió Digitális Menetrendjének (Digital Agenda for Europe) országeredményei, amelyek a digitális közszolgáltatások kínálatát és használatát illetően Észtországot az élmezőnybe helyezik,<sup>12</sup> továbbá a fentieket megerősítik a legnevesebb nemzetközi médiumok is, amelyek szerint Észtország „technológiai vezető hatalom”, „egy olyan hely, ahol a digitális álom már valósággá vált”, továbbá „egy olyan ország, amely digitális infrastruktúrájáról híres.”<sup>13</sup> Más országok kormányai is vágnak arra, hogy átvegyék a legjobb észt eljárásokat – a 2014-es év végén közös megegyezéssel egy új megállapodás jött létre a Koreai Köztársaság, az Egyesült Királyság, Észtország, Új-Zéland, valamint Izrael között, amelynek rendeltetése egy D5 elnevezésű hálózat létrehozása a világ digitális szempontból legfejlettebb kormányzatainak részvételével, abból a közös célból, hogy egymás között megosszák a legjobb gyakorlatokat, továbbá hogy a résztvevő államok digitális kormányzati megoldásait még hatékonyabbá tegyék.<sup>14</sup> Észtországnak az e-eszközökkel és digitális infrastruktúrával kapcsolatos gyors fejlesztési tehát mások számára is tagadhatatlanul kívánatosak.<sup>15</sup>

<sup>7</sup> Freedom House: Az Internet szabadsága 2014. Észt országjelentés.

<sup>8</sup> Eesti Vabariigi põhiseadus, RT I, 15.05.2015, 2. Az Észt Köztársaság Alkotmányának 45. §-a.

<sup>9</sup> Uo. Az észt alkotmány 44. §-a értelmében mindenkinek joga van hozzáférni a nyilvános adatokhoz; a nyilvános és közérdekű adatokra vonatkozó törvény 33. §-a lefekteti, hogy „Mindenki részére biztosítani kell annak lehetőségét, hogy az Interneten keresztül hozzáférjen a nyilvános adatokhoz a könyvtárakban, a nyilvános könyvtárakra vonatkozó törvényben lefektetett eljárási szabályoknak megfelelően.”

<sup>10</sup> e-Észtország. A digitális társadalom. Elérhető angolul a következő helyen: <https://e-estonia.com/>

<sup>11</sup> Freedom House: Az Internet szabadsága 2015. Észt országjelentés.

<sup>12</sup> Az Európai Unió digitális menetrendje (Digital Agenda for Europe). Országokra lebontott előrehaladási jelentés. Észt eredmények. Elérhető a következő helyen: <https://ec.europa.eu/digital-agenda/en/scoreboard/estonia>

<sup>13</sup> Lásd például a „The Economist”-ot: How did Estonia become a leader in technology? The Economist. 2013. július 30., írta A.A.K, amely úgy írja le Észtországot, hogy „erős technikai kultúrával rendelkezik”. Lásd továbbá: “Digital identity cards. Estonia takes the plunge.” The Economist, 2014. június 28.; valamint Elisabeth Braw: “‘E-stonia’ Attempts to Become the Uber of Economies by Introducing Virtual Residency.” Newsweek, 2014. október 30. stb.

<sup>14</sup> „A D5 célzott fórumot biztosít a legjobb eljárások megosztására és annak beazonosítására, hogy a Résztvevők digitális szolgáltatásait hogyan lehetne továbbfejlesztetni, valamint lehetőséget biztosít a közös projektek keretében történő együttműködésre, továbbá támogatja növekedőfélyben levő digitális gazdaságunkat.” A D5 alapító okirata. A D5-ök alapító okirata: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/386290/D5Charter\\_signed.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386290/D5Charter_signed.pdf)  
[https://valitsus.ee/sites/default/files/news-related-files/ict\\_mou\\_fi-ee\\_10dec2013.pdf](https://valitsus.ee/sites/default/files/news-related-files/ict_mou_fi-ee_10dec2013.pdf)

<sup>15</sup> Egy további észt sikertörténetet jelent a “Data Exchange Layer X-Road”, amelyet 2001-ben vezettek be annak érdekében, hogy biztonságos internetalapú adatszerét tegyenek lehetővé az állam különböző informatikai rendszerei között. Ilves elnök kijelentette, hogy a rendszert pusztán csak azért vezették be, mert Észtország túl *szegény* volt ahhoz, hogy egyetlen központi szervere legyen.

2014. december 1-jén Észtország megnyitotta digitális határait<sup>16</sup> mindenki előtt, aki jogszerűen érdeklődik az ország e-szolgáltatásai iránt – az Európai Unió e kicsiny, de technikailag igen fejlett tagállama vált a világ első olyan országává, amely e-kormányzati szolgáltatásainak, valamint a magánszektor e-szolgáltatásainak bizonyos elemeit hozzáférhetővé tette az észt állampolgársággal nem rendelkező személyek részére is, egy „e-polgárság”-nak (e-residency) nevezett formában, a digitális személyazonosság észt megfelelőjének mintájára.<sup>17</sup> A 2016. október 10-én fennálló helyzet szerint 13 896 kérelmet nyújtottak be és 12 794 e-polgárságot bocsátottak ki. A kérelmek többsége Finnországból (2 364), Oroszországból (1 145), az Egyesült Államokból (894), Ukrajnából (749) és az Egyesült Királyságból (680) származott, az e-polgárság azonban a világ számos más pontján is nagy vonzerővel bírt – 134 országból nyújtottak be kérelmet, közöttük Nepál, Sri Lanka, valamint Vietnam. Magyar állampolgárok 175 esetben kérelmeztek e-polgárságot.<sup>18</sup>

E tanulmány célkitűzése az, hogy három különböző nézőpontból is megismertesse az olvasót az e-polgárság innovatív ötletével. A jelen tanulmány második részében bemutatott megközelítés magának a koncepciónak az áttekintését adja, beleértve a technológiai hátteret, az Észtország számára fontos célkitűzéseket, továbbá az e-polgárokkal szembeni elvárásokat is. A harmadik fő egység az e-polgárság megadásának szempontjából teszi vizsgálat tárgyává az észt nemzeti szabályozási rendszert; ezen belül az egyes alpontok bemutatják az e-polgárság és a hatályos észt jogszabályok közötti ütközési pontokat, valamint rámutatnak az e-polgárság és az EU adatvédelmi alapelvei közötti eltérésekre. A negyedik rész megkísérel választ adni arra a kérdésre, hogy vajon az e-polgárság jelenti-e az annyira vágyott megoldást a személyazonosítás globális szintű digitális kezelésében. A következő oldalak célja tehát nem az, hogy megoldásokat ajánljon az e-polgárság problémáinak különböző vetületeire, hanem sokkal inkább az, hogy kritikus hangvétellű vitát generáljon, valamint további elemzések kiindulási pontjaként szolgáljon.

## Az e-polgárság koncepciójának kiterjesztése

Ahogy ezt a fentiekben megállapítottuk, Észtország technikai fejlődésére nemzetközi szinten is felfigyeltek. Az észt állampolgárok és lakosok kiváltságos helyzetben vannak abból a szempontból, hogy legtöbb hivatalos és magánügyüket digitális úton tudják elin-

2013-ban Finnország és Észtország megállapodást kötött az informatikai területen történő együttműködés tárgyában; ennek egyik célkitűzése az volt, hogy az X-Road forráskódját a finnországi gyakorlatban is az országos szintű adatszere alapjaként alkalmazzák. További érdekességet jelent az a tény, hogy ugyanezen megállapodás volt az első olyan nemzetközi jogi dokumentum, amelyet a felek digitálisan láttak el aláírásukkal. Finnország és Észtország közötti, IKT-területen történő együttműködésre vonatkozó szándékmemorandum. Elérhető angolul a következő helyen: [https://valitsus.ee/sites/default/files/news-related-files/ict\\_mou\\_fi-ee\\_10dec2013.pdf](https://valitsus.ee/sites/default/files/news-related-files/ict_mou_fi-ee_10dec2013.pdf).

<sup>16</sup> Az Észt Köztársaság belügyminisztere, Hanno Pevkur, az Észt Köztársaság Kormányának 2015. február 5-én megtartott heti sajtóértekezletén. Csak észt nyelven elérhető: <http://meediaveeb.valitsus.ee/show.php?path=/2015/pressikonverents-2015-02-05-rnd32757.f4v>

<sup>17</sup> E-polgárság kérelmezése. Elérhető a következő helyen: <https://apply.e-estonia.com/>

<sup>18</sup> A kérelmek, továbbá a kibocsátott e-polgárságok számára vonatkozó statisztikák alapján. Az adatbázis elérhető a következő címen: <https://app.cyfe.com/dashboards/195223/5587fe4e52036102283711615553>

tézni. A terv, miszerint ezt a kiváltságot a világ többi részével is meg kellene osztani, az Észt Fejlesztési Alap<sup>19</sup> pályázatán került bemutatásra, a díjnyertes fejlesztési ötlet címe pedig így szól: „2025-re legyen 10 millió digitális észt.”<sup>20</sup> Megszületett az e-polgárság koncepciója, amelyet így a szélesebb nyilvánosság előtt is be kellett mutatni: „Az e-polgár egy olyan külföldi személy, akinek részére – a saját országában már létező személyazonosságára támaszkodva – Észtország digitális személyazonosságot hozott létre és digitális személyazonossági kártyát bocsátott ki: e-igazolványt egy e-polgár számára.”<sup>21</sup> Annak érdekében, hogy kézzelfoghatóbb kereteket adjanak az innovatív elképzelés számára, az Észtország Digitális Menetrendje 2020 stratégia a prioritást élvező kezdeményezések körében rögzítette azt, hogy Észtország „biztonságos és kényelmes szolgáltatásait” elérhetővé tegyék a külföldi állampolgárok számára is.

Ösztönzés Észtország számára? – Szemmel láthatólag az ország arra törekszik, hogy e-szolgáltatásai révén olyan hírnévre tegyen szert, mint Svájc a bankjainak köszönhetően.<sup>22</sup> Ennek megfelelően az Észtország Digitális Menetrendje 2020 rögzíti azt a szándékot, hogy az ország meg kívánja őrizni a technikailag rendkívül fejlett ország képét, az e-polgárság koncepciója kapcsán pedig kiemelésre került, hogy a fenti célkitűzés elérésében ez jelenti az egyik kulcsfontosságú tényezőt.<sup>23</sup> Mindazonáltal a digitális személyazonosságok kibocsátása nem csak Észtország jó hírnevéről szól, hanem annak összetett és többreüt hatása is van. Az észt e-szolgáltatások piaci népszerűsítésén túl az e-polgárság jogi alapját képező dokumentum – a személyazonossági okmányokról szóló észt törvény – az e-polgárság kibocsátásának céljaként az észt „gazdaság, tudomány, oktatás, illetve kultúra” fejlesztését jelöli meg „azáltal, hogy az észt digitális okmány révén hozzáférést biztosít az e-szolgáltatásokhoz,”<sup>24</sup> harmadsorban pedig, ahogyan ezt az Alapkoncepció is meghatározza, az e-polgárság programja hozzá kíván járulni az észt állampolgárokat és az észt kultúrát külföldön támogatni szándékozó „honfitárs-program” fejlesztéséhez.<sup>25</sup> Ezen a ponton még eldöntésre vár, hogy e kezdeményezések valóban egy szándékosan sokrétűként létrehozott program

<sup>19</sup> Estonian Development Fund. Elérhető angolul a következő helyen: <http://www.arendufond.ee/en/>.

<sup>20</sup> Az ötlet kidolgozóit Taavi Kotka, Ruth Annus és Siim Sikkut. Az Észt Fejlesztési Alap az országgyűlés alá rendelt intézmény, amely innovatív gazdasági társaságokba eszközöl befektetéseket annak céljából, hogy hozzájáruljon az észt gazdaság fejlődéséhez.

<sup>21</sup> „Digitális személyazonosság kibocsátása nem rezidens személyek részére: az e-polgárság megteremtése. Alapkoncepció. Az észt személyazonossági dokumentumokra, továbbá állami illetékekre vonatkozó törvénytervezet magyarázó kommentárjának függeléke. 1. sz. Függelék.” [Mitterresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptioon. Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu seletuskirja juurde. Lisa 1.] 2014. Csak észt nyelven elérhető; a továbbiakban „Alapkoncepció”.

<sup>22</sup> Észtország Digitális Menetrendje 2020 stratégia.

<sup>23</sup> Az Észtország Digitális Menetrendje 2020 a célkitűzések között szerepelteti azt, hogy megőrzésre kerüljön Észtország imázsa, amely szerint az ország technikailag előrehaladott, társadalma pedig fejlett információs alapú társadalom; továbbá célkitűzésként szerepel az is, hogy a világ figyelmét felhívják a digitális Észtországra.

<sup>24</sup> Az Észt Köztársaság személyazonossági okmányokra vonatkozó törvényének 20<sup>5</sup> §-a. Az e-polgárok digitális személyi igazolványa, a továbbiakban „IDA”.

<sup>25</sup> Az észt állampolgárok és az észt kultúra külföldön történő támogatása az Oktatási és Kutatási Minisztérium által vezetett nemzeti „honfitárs”-programon keresztül történik, amelyet a Művelődési Minisztériummal, valamint a Külügyminisztériummal együttműködésben valósítanak meg.

szisztematikusan megalkotott elemeit képezik-e, avagy az e-polgárság koncepcióját „be-gyömöszölték” több más, többé-kevésbé elfogadható ötlet közé azért, hogy létjogosultságát ilyen módon igazolják.

### *A technológiai háttér (PKI)*

Annak a ténynek köszönhetően, hogy Észtország már rendelkezik a digitális személyazonossági okmányok kezelését szolgáló, ténylegesen működő rendszerrel, nem voltak technikai akadályai annak, hogy megteremtsék a digitális személyi igazolványok biztonságos rendszerét az e-polgárok számára is.<sup>26</sup> Magát a digitális személyi igazolvány ötletét először 1998-ban vetették fel, 2003 januárjában pedig kibocsátásra kerültek az első digitális személyazonossági kártyák az állampolgárok részére.<sup>27</sup> Az állampolgárok számára kiadott személyazonossági kártyákba, és most már az e-polgárok számára kiadott kártyákba is beépített mikrocsip a titkosításra egy 2048 bites nyilvános kulcsot használ (a kártya régebbi változatai 1024 bites verziót használtak), amely az észt rendszerrel kompatibilis összes elektronikus rendszeren belül alkalmas a személyazonosság valódi és hiteles igazolására.<sup>28</sup> Mivel az e-polgár személyazonossági kártyája az állampolgárok és lakosok által használt személyazonossági kártyához hasonló módon szolgálja a hitelesítést, emiatt az állam által támogatott Nyilvános Kulcsú Infrastruktúra (Public Key Infrastructure, PKI) keretei között működik, amelynek révén az állam vállalja, hogy kötelezően szavatol a rendszer fennállásáért és működéséért.

A Nyilvános Kulcsú Infrastruktúra (PKI) jelenti a szó szerinti kulcsot a biztonságos személyazonosításhoz és az elektronikus aláíráshoz. A kulcsot egy bonyolult kódként képzelhetjük el, amelyet a személyazonossági kártyákba (az észt állampolgárok számára kiadott és az új e-polgárok részére kibocsátott digitális személyi igazolványokba egyaránt) beépített mikrocsip őriz.<sup>29</sup> Maga a kulcs további két részből, azaz egy kulcspárból áll: egy titkosítást szolgáló nyilvános kulcsból, valamint a visszafejtést lehetővé tevő magánkulcsból. Példának okáért az elektronikus aláírás a kettő kombinálásával jön létre – első lépésben az aláírás létrehozásához szükséges azon adatok használatával, amelyek az aláírást létrehozó, biztonságos eszközben vannak rögzítve: ez a titkosítást lehetővé tevő *magánkulcs*; második lépésben pedig az aláírás hitelességének ellenőrzését lehetővé tevő azon adatokat kell használni, amelyek egyedi módon megfeleltethetőek a magánkulcsnak – ez a dekódolást lehetővé tevő *nyilvános kulcs*.<sup>30</sup> A kártya kontaktsipjében vagy mikrocsipjében két tanúsítvány<sup>31</sup> található, amelyet a személyazonosság igazolására, valamint dokumentumok

<sup>26</sup> Alapkoncepció, lásd a fenti 16. lábjegyzetet.

<sup>27</sup> A személyazonossági kártyák bevezetésének időrendje a digitális személyi igazolványok és mobil személyazonosító eszközök hivatalos ügyfélkapujától származik.

<sup>28</sup> Az elektronikus személyazonossági kártyákra vonatkozó információ az E-Estonia webhelyről származik.

<sup>29</sup> Nyilvános Kulcsú Infrastruktúra. PKI. Észt Informatikai Hatóság.

<sup>30</sup> Az elektronikus aláírásokról szóló észt törvény 2(2) §-a.

<sup>31</sup> A tanúsítvány egy olyan elektronikus tanúsítványt jelent, amely a személyazonosság igazolásához, valamint az elektronikus aláírás hitelesítéséhez szükséges adatokat egy adott személyhez kapcsolja, továbbá tanúsítja a kérdéses személy kilétét. További információért lásd a digitális személyi igazolványok és mobil személyazonosító eszközök hivatalos ügyfélkapuját. A digitális személyi igazolványok és mobil személyazonosító eszközök hivatalos ügyfélkapujának „What are certificates” című menüpontja.

elektronikus aláírására is lehet használni; feltéve, hogy mindez olyan szoftver használatával történik, amely kompatibilis az észt személyazonossági kártyákkal.<sup>32</sup> Ennek megfelelően a kártyát úgy lehet elektronikus aláírásra és személyazonosság igazolására használni, hogy előzetesen telepíteni kell a szükséges szoftvert, majd a személyazonosító kártyát egy számítógéphez USB-porton át csatlakoztatott kártyaolvasó használatával kell beolvasni (de vannak olyan számítógépek is, amelyek beépített kártyaleolvasó egységgel rendelkeznek), vagy a felhasználó egy mobil személyazonosító rendszeren keresztül, kártyaolvasó nélkül, mobiltelefonját használva is bejelentkezhet. Egyszerűen megfogalmazva a kártya kettős hitelesítéssel dolgozik – valamely digitális szolgáltatáshoz való hozzáféréshez vagy egy dokumentum elektronikus úton történő aláírásához egy titkos, előzőleg már az e-polgár rendelkezésére bocsátott PIN-kódot is meg kell adni.

Hogy pontosabban is megvilágítsuk a biztonsági vonatkozásokat: a két részből álló kulcs egyik része a mikrocsip nyilvános részében kerül tárolásra, amely azt jelenti, hogy a személyazonossági kártyát leolvasó (akár a számítógépbe beépített, akár ahhoz USB-porton keresztül csatlakoztatott) berendezések, a kártyás beléptető rendszerek, a webes alapú szolgáltatások vagy más, a személyazonossági kártya használatán alapuló applikációk ezt az információt le tudják olvasni. A kártya eme részében található tanúsítvány (a személyes adatokat is beleértve) jelenti a PKI-n keresztül hozzáférhető, személyazonosságra vonatkozó digitális bizonyítékot.<sup>33</sup> A kulcskészlet titkos eleme a mikrocsip védett részében kerül eltárolásra, és ahhoz csakis a tulajdonos rendelkezésére bocsátott PIN-kódok használatával lehet hozzáférni. A fentiek illusztrálására meg kell jegyeznünk azt is, hogy a nyilvános és a magánkulcs között matematikai kapcsolat áll fenn, azonban a nyilvános kulcs alapján a magánkulcsot nem lehet kikövetkeztetni. A nyilvános kulcs használatával titkosított információt csakis a személyre szóló és titkos kulcs használatával lehet visszafejteni, ami azt is jelenti, hogy a bizalmas üzenetet csakis annak címzettje képes elolvasni. Ennek megfelelően ha valaki a személyazonossági kártya használatával azonosítja magát, az internetes szerver a kártyatulajdonosnak küld egy olyan egyedi azonosítót, amelyet a kérdéses személy nyilvános kulcsának használatával titkosítanak, továbbá amelyet csakis a kapcsolódó egyedi hitelesítő kulcs használatával (a PIN-kód megadásával) lehet dekódolni.<sup>34</sup>

Egy további, talán könnyebben megérthető biztonsági aspektust jelent az a tény, hogy egy másik személy PIN-kódjainak pusztán ismerete nem elegendő ahhoz, hogy személyazonossági kártyájával vissza lehessen élni – az e-szolgáltatások igénybe vételéhez megkövetelt személyazonosításhoz szükség van a személyazonossági kártya fizikai birtoklására is. Mindez fordított irányban is működik – ha a kártya fizikailag rossz kézbe kerül, az e-szolgáltatások nem válnak hozzáférhetővé abban az esetben, ha a nyilvános kulcsú infrastruktúra nem képes meggyőződni a tanúsítványok érvényességéről. A fentiekén túl a kártyában található mikrocsip számolja, hogy hány alkalommal került megadásra hibás kód, ami azt jelenti, hogy három sikertelen

<sup>32</sup> IDA, lásd a fenti 19. lábjegyzetet, 9<sup>a</sup> §. A tanúsítvány beiktatása a dokumentumokba.

<sup>33</sup> A digitális aláírásokra vonatkozó törvény 5(1) §-a: „... a tanúsítvány egy olyan dokumentum, amely elektronikus aláírás vagy elektronikus pecsét alkalmazásának és hitelesítésének lehetővé tétele érdekében kerül kibocsátásra, és amelynek keretei között egy nyilvános kulcs egyedi módon kapcsolódik az adott tanúsítvány birtokosához.”

<sup>34</sup> Személyazonossági kártya. Számítógépes védelem. Biztonságos bejelentkezési pont. [ID-kaart. Arvutikaitse. Infoturvalisuse teeviit.]

azonosítási kísérlet után a PIN zárolásra kerül (és azt csakis egy úgynevezett PUK-kód használatával lehet feloldani).<sup>35</sup> A rendszer ellen intézett támadások körében azonban – példának okáért – megtalálhatóak azok a célirányosan megírt kártékony programok is, amelyek a bűngészőprogram felületeit vagy bővítményeit utánozva megkísérelhetik átírányítani a (magukat már sikerrel igazolt) felhasználókat egy másik felületre, vagy megkísérelhetik megváltoztatni egy banki átutalás paramétereit. Mindez azonban azt jelenti, hogy maga a kérdéses számítógép, nem pedig az e-személyazonossági rendszer kompromittálódott.

A jövőbeli fejlesztésekre való tekintettel, továbbá szem előtt tartva mindazt, amit Észtország nemzeti szinten már elért, a közeljövőben lehetővé fog válni a mobil személyazonosító eszközök<sup>36</sup> használata Észtország területén kívül is. Ha az e-polgár már meglévő SIM-kártyáját kicseréli egy olyanra, amely lehetővé teszi a PKI-hez való csatlakozást (ami azt is jelenti, hogy a mobil személyazonosító eszközök használatához szükség van egy észt mobilhálózati szolgáltatóval történő szerződéskötésre is), a digitális személyazonosság mobiltelefon útján történő hitelesítése és ellenőrzése ugyanolyan hatékonyságot és minőséget fog kínálni, mint a számítógépen keresztül történő bejelentkezés (csak ez utóbbinál sokkal kényelmesebb lesz); mindez pedig azt is jelenti, hogy a személyazonosság igazolása és a dokumentumok elektronikus aláírása többé már nem lesz annak a függvénye, hogy valakinek áll-e rendelkezésére számítógép, az ahhoz kapcsolt kártyaleolvasó, valamint a számítógépre telepített speciális program – elég lesz, ha van mobiltelefonja (amelynek nem kell szükségszerűen okostelefonnak lennie) vagy táblagépe. A mobil személyazonosító rendszerek ugyanolyan módon, tehát az 1. és 2. számú PIN-kódok használatával biztosítanak hozzáférést a szolgáltatásokhoz, az adatcsere pedig titkosított csatornán zajlik, amely az előző rendszerhez képest azonos szintű biztonságot garantál (Martens 2013: 217).

### *Politikai célkitűzések*

Az e-polgár személyazonossági kártyát kap, amelyen azonban nincsen fénykép, így – példának okáért – úti okmányként nem használható. Ennek megfelelően az e-polgár személyazonossági kártyája mindenekfelett és elsősorban digitális dokumentum,<sup>37</sup> amely különböző e-szolgáltatásokat testesít meg; ez utóbbiak az új e-polgár előtt egy olyan személyazonossági kártya alakjában nyílnak meg, amely a nemzeti személyazonossági kártyákhoz hasonló biztonsági tanúsítványt hordozó mikrocippel van ellátva.<sup>38</sup> A lényegi vonás az, hogy (tekintet nélkül valódi állampolgárságára, valamint a digitális szolgáltatás jellegére) egy észt digitális polgár mindössze pár kattintással bizonyíthatja a személyazonosságát. Az első e-polgárság 2014 végén történt kibocsátását megelőzően<sup>39</sup> csak néhány

<sup>35</sup> Uo.

<sup>36</sup> A digitális személyi igazolványok és mobil személyazonosító eszközök hivatalos ügyfélkapujától származó, a mobil azonosításra vonatkozó információk.

<sup>37</sup> IDA, lásd a fenti 19. jegyzetet, 20<sup>3</sup>§. A személyazonosító okmányokra vonatkozó törvény különböztet a digitális személyazonossági kártya 2(1)<sup>1</sup>§ és egy személy elektronikus úton történő beazonosítására szolgáló digitális dokumentum között 3(3)§.

<sup>38</sup> Uo., 20<sup>2</sup>§. A digitális személyazonossági kártyára betáplálendő elektronikus adatok.

<sup>39</sup> Az első e-polgár Edward Lucas brit újságíró, az Economist magazin főszerkesztője volt. Lásd többek között az e-Észtország hírlevélhez írott bevezetőjét. Edward Lucas előszava az e-Észtország hírlevélhez: <https://e-estonia.com/foreword-to-the-e-estonia-newsletter-by-edward-lucas/>



olyan további EU-tagállam polgárai azonosíthatták magukat az észt személyazonossági kártya tulajdonosával azonos módon, akiknek országa az észt rendszerhez hasonló digitális személyazonosító rendszert működtetett (és ekkor is kizárólag csak meghatározott szolgáltatásokhoz, például az elektronikus cégnyilvántartáshoz férhettek hozzá). Mindazonáltal, figyelembe véve azt a tényt, hogy az ilyen személyazonosító kártyák és felhasználóik száma a többi EU-tagállamban igen csekély (Martens 2013: 216)<sup>40</sup> (Észtország 2008 óta elfogadja a belga, finn, portugál és litván személyazonosító kártyákat), továbbá tekintettel arra, hogy más országok polgárainak bevonására nem volt más hatékony módszer, kialakult az a vélemény, miszerint az észt gazdaság, kultúra, oktatás és tudomány nem fejlődhet kellő mértékben akkor, ha a külföldi állampolgárok nem használhatják az észt elektronikus szolgáltatásokat – az e-polgárság pedig e probléma kezelésére szolgáló megoldásként jött létre.<sup>41</sup>

Mindez kifejtésre kerül az e-polgárság koncepciójában is, amely a külföldi szaktudás és tőke bevonását és bevonását jelöli meg kizárólagos lehetőségként (sőt előfeltételként) ahhoz, hogy Észtország megfelelő pozíciót biztosíthasson magának a mai globalizált világban, amelyben a gazdasági, politikai és kulturális fejlődés túlnyomórészt a nemzetközi kommunikáción és együttműködésen múlik.<sup>42</sup> Az Alapkoncepció megszövegezői<sup>43</sup> kifejezetten úgy vélekedtek, hogy a külföldi szakemberek fenti közreműködése nem függhet attól, hogy fizikailag a világ mely részén tartózkodnak, emiatt az e-polgárság tökéletes megoldást jelenthet arra, hogy az érdeklődő külföldieknek lehetővé tegyék a hétköznapi ügyekben történő részvételt – olyan digitális alkalmazások segítségével, amelyek egyenértékűek az észt állampolgárok és lakosok részére nyitva álló megoldásokkal, továbbá amelyek a részvételt anélkül biztosítják, hogy az illetőnek fizikai értelemben, ténylegesen is jelen kellene lennie.<sup>44</sup>

Ami pedig a „honfitárs” programot illeti, az e-polgárság támogatói e megoldást megfelelőnek tartják arra a célra is, hogy a kivándorolt észteknek lehetőséget adjanak a szülőföldjükkel történő kapcsolattartásra oly módon, hogy aktuális állampolgárságukra vagy tartózkodási helyükre való tekintet nélkül a digitális szolgáltatásokhoz való hozzáférési lehetőséget kínálják részükre. Lefektetésre kerültek a következő megállapítások: „Bár az észt identitás elsősorban a nyelvhasználaton és az abból eredő kultúrán nyugszik, fontos a más országokban élő emigráns közösségekkel történő, az észt nyelv használatán nyugvó kommunikáció is [...]. Így növekedni fog annak a valószínűsége, hogy a jelenlegi, továbbá a második és harmadik generációs kivándorlók kapcsolatban maradnak Észtországgal, közülük néhányan visszatérnek Észtországba, illetve megőrzik és ápolják a határokon keresztülívelő kapcsolatokat.”<sup>45</sup>

<sup>40</sup> Az észt személyazonossági kártya és digitális személyazonossági kártya lényegesen hasonlít a Belgiumban használatos ilyen kártyára.

<sup>41</sup> Alapkoncepció, lásd a fenti 16. jegyzetet, 4. old.

<sup>42</sup> Uo., 3. old.

<sup>43</sup> Az Alapkoncepcióban található javaslatok az észt Belügyminisztérium, az Észt Köztársaság Miniszterelnöki Hivatala, a Gazdasági és Kommunikációügyi Minisztérium, az Informatikai Hatóság, a Rend- és Határőrség, az észt Belbiztonsági Szolgálat, az észt Adó- és Vámhatóság, továbbá a központi hitelesítő hatóság képviselőinek együttes erőfeszítésével került kidolgozásra, további érdekelt szereplőkkel történt konzultációk alapján.

<sup>44</sup> Alapkoncepció, lásd a fenti 16. jegyzetet.

<sup>45</sup> Uo., 6. old. Ez az érv a kettős/többszörös állampolgárság elemzésén alapul, amelyet a Belügyminisztérium 2013-ban folytatott le. [Mitmikkodakondsus. Analüüs. Siseministeerium 2013].

Ha ellenőrizhető digitális személyazonosságot, valamint digitális személyazonossági kártyát kap, az e-polgár egyetlen okmánnyal igazolhatja kilétét, továbbá az ilyen személy – fizikai megjelenés és arcról történő azonosítás helyett – elektronikus környezetben bizonyíthatja személyazonosságát, illetve írhat alá dokumentumokat. Mindez hozzáférést biztosít továbbá az Észtország által kínált digitális szolgáltatásokhoz, valamint a közeljövőben – az EU egységes digitális piacán belül – a határokon túlnyúló tranzakciók vonatkozásában lehetőséget fog adni az elektronikus személyazonosításra, valamint a bizalmi szolgáltatások igénybe vételére is.<sup>46</sup> Ámbár a magánszektor bizonyos szolgáltatásai, így például az internetes bankolás, a telekommunikációs szolgáltatások stb., valamint az Eesti.ee (Észt Egységes Hozzáférési Pont<sup>47</sup>), az észt Adó- és Vámhatóság, valamint mások is hozzáférhetőek online, mégpedig személyazonossági igazolvány használata nélkül, banki vonalon át, mindez egyáltalán nem olyan biztonságos és kézenfekvő megoldás, mint a digitális személyazonossági kártya használatával történő hozzáférés.

### *A koncepció megkérdőjelezhető vonásai*

Jelen pillanatban a „rendes” személyi igazolvány használatával igénybe vehető szolgáltatások (nem taxatív) listáján magán- és közszolgáltatások egyaránt szerepelnek, így például megvan a hozzáférési lehetőség a kormányzati intézményekhez, az e-szavazáshoz, az e-iskolákhoz és az e-óvodákhoz, a bankokhoz, az egyetemek tanulmányi információs rendszeréhez, a telekommunikációs és internetes szolgáltatókhoz, a biztosítási és e-egészségügyi rendszerhez stb.; mindazonáltal e szolgáltatások közül az e-polgár személyazonossági kártyájának használatával nem mindegyik elérhető.<sup>48</sup> A digitális Észtország e-polgár kártyája mindazonáltal megnyitja a virtuális kapukat ahhoz, hogy online jegyeztessünk be egy gazdasági társaságot (a társasági ügyfélkapun keresztül), elektronikus úton írassunk alá dokumentumokat, titkosított dokumentumokat cseréljünk egymás között, online nyújtsunk be beszámolót a cégnyilvántartáshoz, biztonságos online banki tranzakciókat bonyolíthassunk le,<sup>49</sup> online küldjük el adóbevallásunkat, valamint az éves gazdasági jelentéseket, sőt hogy az észt gyógyszertárakba digitális receptet adhassunk be.<sup>50</sup> Az

<sup>46</sup> Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (eIDAS).

<sup>47</sup> Az Egységes Hozzáférési Pontok (Points of Single Contact, PSC-k) egyablakos e-kormányzati internetes portálok, amelyek a szolgáltatási szektorban tevékenykedő vállalkozók rendelkezésére állnak. 2009 decembere óta az EU szolgáltatásokra vonatkozó irányelvben meghatározottak szerint minden egyes EU-tagállamban jogszabályilag kötelező egy PSC működtetése.

<sup>48</sup> A fentiek a személyazonossági kártya lehetséges felhasználási módjait jelentik. További lehetőségeért lásd a digitális személyi igazolványok és mobil személyazonosító eszközök hivatalos ügyfélkapuját.

<sup>49</sup> Egy e-polgárnak megvan a *lehetősége* arra, hogy Észtországban bankszámlát nyisson, azonban mindehhez szükség van a banknál, Észtországban tett személyes látogatásra, amely azonban nem garantálja a tényleges számlanyitást, hiszen a jóváhagyó döntés a bankon múlik.

<sup>50</sup> Az ügyek úgynevezett zavartalan intézéséhez nyújtott szolgáltatások; további információért lásd az e-Észtország honlapot.

ilyen szolgáltatások potenciális felhasználóit az Alapkoncepció a következő módon határozza meg:

- Külföldi befektetők és az ilyen befektetők által alapított gazdasági társaságok alkalmazottai;
- Az ilyen gazdasági társaságok vezetésében (igazgatótanácsában) részt vevő vagy azokba befektető külföldi állampolgárok;
- Az észt gazdasági társaságok külföldi állampolgárságú szakértői és munkavállalói;
- Az észt vállalkozások külföldi ügyfelei és partnerei;
- Külföldi kutatók, tudósok és diákok;
- Más államok és nemzetközi szervezetek Észt Köztársaságon belül működő képviselői (például a NATO kibevédelmi kiválósági központja, az EU Informatikai Ügynöksége);
- Az előző személyek hozzátartozói.<sup>51</sup>

Az e-polgárság célcsoportjainak, valamint hármás célkitűzési rendszerének (azaz 1) az ország e-szolgáltatásainak vonzóvá tétele az emberek számára, 2) az észt gazdaság, oktatás, valamint tudományos és kulturális élet fejlesztése azáltal, hogy a szolgáltatásokat nemzetközi szintre visszük, valamint 3) a „honfitársakat” támogató program végrehajtása) értékelése során megállapíthatjuk, hogy a koncepció meglehetősen diffúznak tűnik. Szembeötlő, hogy a figyelem középpontjában szinte kizárólag olyan személyek állnak, akiknek gazdasági érdekeltségeik vannak Észországban. Mivel nem történik említés az olyan volt észt állampolgárokról, akik kivándoroltak, a „honfitársakat” támogató program végrehajtásához való hozzájárulás szándéka célként elvész.<sup>52</sup> Ha ragaszkodunk ahhoz az elképzeléshez, hogy a digitális személyazonosító kártyával igénybe vett észt e-szolgáltatások révén egy digitális észt polgár arra is kötelessé válik, hogy hozzájáruljon az észt gazdaság, kultúra, oktatás vagy tudomány fejlődéséhez, ez a konkrét célkitűzés nem tűnik kellőképpen átgondoltnak. A külföldi kutatókon, tudósokon és diákokon túl nehéz olyan célcsoportot találni, amelynek tagjai ténylegesen támogatnák az észt kultúrát, tudományt vagy oktatást. Ezzel párhuzamosan nem kerültek meghatározásra (vagy nyilvánosságra hozatalra) azok az értékelési kritériumok, amelyek alapján el lehetne dönteni az adott területeken végbement fejlődés mértékét – nem derült ki, hogy egy digitális észt polgárnak milyen módon kellene igazolnia azt, hogy az észt e-szolgáltatások általa történt igénybe vételének következményeként a tudomány színvonalában valamely százalékpontos emelkedés következett be; tekintettel továbbá arra, hogy az e-polgárság nem korlátok nélkül érvényesülő kedvezmény, az sem egyértelmű, hogy az e-polgár milyen módon volna köteles bizonyítani az észt fejlődéshez történt hozzájárulását abban az esetben, ha el akarja kerülni az e-személyazonosságtól történő megfosztását.<sup>53</sup> Meglehetősen egyértelmű, hogy a legkívánato-

<sup>51</sup> Alapkoncepció, lásd a fenti 16. jegyzetet, 6. old.

<sup>52</sup> Ha különösen kritikus hangot kívánunk megütni, azt is állíthatjuk, hogy ez a cél mindig is homályos volt. Ha a „honfitárs” program célja az, hogy az észt nyelven történő *kommunikációt* bátorítsuk a kivándorolt (volt) észt állampolgárok között, az e-polgárság egészen biztosan nem alkalmas eszköz mindeerre - különösen, ha figyelembe vesszük az internetes közösségi helyeken használt nyelveket.

<sup>53</sup> Az IDA értelmében, lásd a fenti 19. jegyzetet, 20<sup>6</sup>(4)§, a személyazonossági kártyát vissza lehet vonni abban az esetben, ha az (1) bekezdésben meghatározott jogalap, tehát az észt állammal fennálló kapcsolat, vagy az észt állam által biztosított e-szolgáltatások használatához fűződő jogos érdek megszűnik.

sabb e-polgárnak az üzleti életben érdekelt személy tűnik, aki elsősorban a gazdasági fejlődést pezdíti fel.<sup>54</sup> Mindez természetesen nagyon gyümölcsöző lehet a helyi gazdasági vállalkozások számára – ha digitális és egyben jogilag is kötelezőnek minősülő kommunikáció révén létesítenek üzleti kapcsolatot külföldi kollégáikkal és befektetőikkel, ami természetesen az észti gazdaság számára is komoly löketet jelenthet. Mindazonáltal az e-szolgáltatások igénybe vétele révén a tudósok, művészek vagy az oktatás területén működő személyek által előállított többletérték ezen a ponton legalábbis megkérdőjelezhetőnek tűnik.

## Az ellentmondásos jogszabályi háttér

Észtország tagadatlanul digitális életformát követ, és ezt az életmódot a külföldi állampolgárok részére is hozzáférhetővé teszi. Bár az észti állampolgárok és lakosok személyazonossági kártyájának, valamint az e-polgárok kártyájának használata ugyanazzal a biztonságos számítógépes programmal történik, az e-polgár digitális identitását az előző két csoport identitásától a tanúsítványok alapján meg lehet különböztetni. Ezáltal kerül biztosításra az, hogy az e-szolgáltatásokat igénybe vevő személy jogállása digitális identitás létében is azonosítható maradjon.<sup>55</sup> Ennek alapján a szolgáltatók elkülönítve tudják figyelni az e-polgárok digitális azonosítóinak használatát, illetve szükség esetén korlátozhatják a szolgáltatásokhoz történő hozzáférésüket. Ámbár a kizárólag csak állampolgárok részére fenntartott e-szolgáltatások – mint például az elektronikus úton történő szavazás – nem hozzáférhetőek az e-polgárok számára, amelyre a regisztráció során figyelmeztetik is őket, a digitális személyazonosság megadása ennek ellenére szükségessé teszi az e-polgár applikációinak és online tevékenységének figyelemmel kísérését, annak eldöntése érdekében, hogy a kérdéses személy alkalmas jelölt-e az e-észti státuszra, továbbá annak megállapítása céljából, hogy az e-polgárságot már elnyert személy vajon körültekintően és megfontoltan használja-e azt.<sup>56</sup>

Ahogy ez az e-polgárság bevezető koncepciójában gyakorta hangsúlyozásra kerül, folyamatosan emlékeznünk kell arra, hogy az e-polgár digitális személyazonossága kedvezmény, nem pedig alapjog,<sup>57</sup> amely azt is jelenti, hogy a kibocsátásáról döntő észti hatóságok bizonyos dolgokat kifejezetten megkövetelhetnek az Észtországgal digitális kapcsolatba lépni kívánó személytől, továbbá ezt a kiváltságot visszavonhatják, ha az e-polgár tevékenysége nem felel meg az észti jogszabályi vagy egyéb kötelező magatartási előírásoknak. A személyazonossági okmányokra vonatkozó észti törvény rögzíti az e-polgárság megszerzéséhez szükséges előfeltételeket – az észti digitális identitásért folyamodó személynek vagy „korábbi kapcsolatban kell állnia az észti állammal”, vagy „jogos érdekének kell fenn-

<sup>54</sup> A Gazdasági és Kommunikációügyi Minisztérium e-polgárságot bemutató honlapja a „Why are we doing it?” („Miért csináljuk mindezt?”) cím alatt kijelenti a következőket – „A vállalkozások nyilvántartásba vétele befektetéseket hoz és munkahelyeket teremt Észtországban, amelyek így hozzá fognak járulni a gazdasági fejlődéshez.” Egyetlen szó sem esik a kultúráról, oktatásról vagy tudományról.

<sup>55</sup> Alapkonceptió, lásd a fenti 16. jegyzetet, 4. old.

<sup>56</sup> Uo., 12. old.

<sup>57</sup> Uo., 2.1. Alpont: Alapelvek [Aluspõhimõtted].

állnia az észti állam által biztosított e-szolgáltatások használatára vonatkozóan.”<sup>58</sup> Bár a törvény megköveteli a jogos érdek fennforgását, illetve a korábban keletkezett kapcsolatot, nem határozza meg ezek alapelveit, és mindkét követelményre nézve szabad értelmezést tesz lehetővé. A „korábbi kapcsolat” [észti nyelven: „eelnev seos”] kifejezés tagadhatatlanul széles jelentéstartalommal bír, és egy észtsországi látogatástól kezdve a korábban birtokolt, de később megszűnt észti állampolgárságig bármit jelenthet. Ugyanilyen módon komoly kihívást jelent az e-szolgáltatások használatával kapcsolatos jogos érdek léte, ha megállapítására nincsenek formális szempontok.

### *Az e-polgárság kibocsátása, felfüggesztése és visszahívása*

A digitális személyazonossági kártya kibocsátására vonatkozó eljárási szabályok úgy rendelkeznek, hogy a potenciális e-polgárnak igazolnia kell jogos érdeke tényleges fennállását, akár írásos nyilatkozattal, akár pedig más olyan bizonyíték használatával, amely megnevezi a szándékolt felhasználás tényét és körülményeit<sup>59</sup> (amelyek kiértékelési szempontjai azonban sehol nincsenek meghatározva), vagy az Észtsországgal korábban fennállt kapcsolatát (amelynek mibenléte szintén nincsen meghatározva), továbbá az Észti Rend- és Határőrség számára bizonyos személyes adatokat (ezen belül érzékeny adatokat, például biometrikus adatokat) kell átadnia.<sup>60</sup> Ezt követően a kérelmet elbírálják, amelynek keretében az Észti Rend- és Határőrség munkatársainak átadott információt annak megállapítása érdekében dolgozzák fel, hogy a kérelmezőt valóban alkalmas észti digitális polgárnak lehet-e tekinteni. Ennek megfelelően az Észti Rend- és Határőrség az a hatóság, amelynek hatáskörébe tartozik a kérelemmel kapcsolatos döntéshozatal,<sup>61</sup> a kérelmező kilétének megállapítása és személyazonosságának ellenőrzése,<sup>62</sup> továbbá a kibocsátott e-polgárságok felett az Észti Belbiztonsági Szolgálattal, valamint az Észti Adó- és Vámhatósággal közösen az Észti Rend- és Határőrség jogosult állami felügyeletet gyakorolni.<sup>63</sup> Eredetileg az e-polgár program elindításakor a kérelmező két alkalommal volt köteles Észtsországba utazni (egyszer azért,

<sup>58</sup> IDA, lásd a fenti 19. jegyzetet, 20<sup>6</sup>(1)§. Az e-polgár digitális személyazonossági kártyájának kibocsátására, érvényességének felfüggesztésére és visszavonására vonatkozó feltételek.

<sup>59</sup> A Köztársaság Kormánya által kiadott rendelet 10<sup>2</sup>(1)§-a, amely meghatározza a személyazonossági kártya kibocsátására vonatkozó kérelemmel együtt benyújtandó igazolások és adatok jegyzékét, továbbá a személyazonossági kártya, állandó lakcímet igazoló kártya, digitális személyazonossági kártya, észti állampolgárt megillető útlevél, tengerhajózási szolgálatból történő leszerelési okmány, ideiglenes útlevél, menekültútlevél, továbbá hajón töltött szolgálatot igazoló bizonyítvány kibocsátásának előfeltételeit.

<sup>60</sup> IDA, lásd a fenti 19. jegyzetet, 9 §. A dokumentumok szabványos formátuma és a dokumentumokba bevezetendő adatok köre.

<sup>61</sup> IDA, lásd a fenti 19. jegyzetet, 11<sup>1</sup>§. A személy kilétének megállapítása és személyazonosságának ellenőrzése a dokumentum kibocsátásakor; 12<sup>1</sup> § A dokumentum kibocsátása; 15.§ A dokumentum kibocsátásának és visszavonásának eljárási szabályai, (4). Lásd még az Észti Belügyminisztérium honlapját. Elérhető angolul a következő helyen: <https://www.siseministerium.ee/e-residency/>

<sup>62</sup> Uo., 20<sup>9</sup> §. Az e-polgár személy kilétének megállapítása és személyazonosságának ellenőrzése.

<sup>63</sup> Uo., 20<sup>8</sup> §. Állami felügyelet gyakorlása. Lásd még az Észtsországbán tartózkodó külföldiekre vonatkozó törvény 6. fejezetét.

hogyan benyújtsa a kérelmét és igazolja a személyazonosságát, második alkalommal pedig azért, hogy átvegye a dokumentumot – személyazonossági okmányokat ugyanis nem lehet postai úton kézbesíteni). 2015. április 1-től kezdődően lehetőség nyílt arra, hogy a kérelmet a 38 külképviselet valamelyikén, az észti nagykövetségeken vagy konzulátusokon, avagy az interneten keresztül nyújtsák be,<sup>64</sup> a kérelmeket azonban elbírálásra továbbra is Észtországba továbbítják.<sup>65</sup> A kérelem benyújtását követően a Rend- és Határőrség saját hatáskörében jogosult dönteni arról, hogy a kérelmező részére megadja-e az e-polgárságot vagy sem.<sup>66</sup> A Rend- és Határőrség tisztviselői a jelölt alkalmasságának eldöntésekor, de még a későbbiekben, a folyamatos figyelemmel kísérés alatt is jogosultak arra, hogy minden hozzáférhető forrás felhasználásával ellenőrizzék egy e-polgár megbízhatóságát, amelynek során kapcsolatba léphetnek más illetékes szervekkel, valamint keresést folytathatnak le a releváns adatbázisokban azért, hogy meggyőződjenek a kérdéses személy személyazonosságának hitelességéről, továbbá előzetes értesítés és engedély nélkül folytathatnak adatfeldolgozást.<sup>67</sup>

A kérelmezési folyamat eme szakaszában, amelynek során a Rend- és Határőrség felelős azért, hogy a kérelem benyújtásának indokára vonatkozó információkat begyűjtse, a hatóság számára bonyolult feladatot jelent annak eldöntése, hogy az adott kérelmező az észti e-szolgáltatások (és ezen belül például az e-receptek vagy az internetes bankrendszer) használata révén képes lesz-e hozzájárulni az észti kultúra, oktatás, tudomány vagy gazdaság fejlődéséhez. E legutóbbi tényezővel kezdve, a döntéshozatal talán gazdasági aspektusból a legkönnyebb – ha tehát például a kérelmező kijelenti: jogos érdeke abban áll, hogy egy gazdasági vállalkozást kívánna létrehozni Észtországban –, mivel ez nagy valószínűség szerint fejleszti az üzleti környezetet és egyben az egész gazdaságot is. Ugyanakkor a hatóság számára rendkívül nehéz (sőt lehetetlen) lehet eldönteni azt, hogy valaki, aki már kétszer járt Észtországban (és ennek révén már korábban kapcsolatba lépett Észtországgal?), vajon képes lesz-e előmozdítani az ország kulturális, oktatási vagy tudományos életének fejlődését. Ennek alapján úgy tűnik, hogy az e-szolgáltatások e-polgár általi igénybevételének hatásaira vonatkozó értékelő tevékenység jelentősen eltér az Észt Rend- és Határőrség által végzett tipikus munkától.

A fentiekre való tekintettel, ha a Rend- és Határőrség veszi át és kezeli a kérelmeket, dönt az e-polgárság megadásáról, továbbá általános felügyeletet is gyakorol a kérelmezés kapcsán,<sup>68</sup> a megnövekedett munkateher megfelelő kezelése érdekében a testület munkaerő-kapacitását is meg kell növelni.<sup>69</sup> E vonatkozásban hangsúlyoznunk kell, hogy rend-

<sup>64</sup> 2015. május 13. óta rendelkezésre áll a kérelmek internetes benyújtását lehetővé tevő honlap a <https://apply.e-estonia.com/> címen, amely a dokumentum kiadásához pusztán egyetlen látogatást tesz kötelezővé az észti konzulátuson vagy nagykövetségen, avagy az Észt Rend- és Határőrségnél.

<sup>65</sup> IDA, lásd a fenti 19. jegyzetet, 20<sup>7</sup> (1<sup>1</sup>) §.

<sup>66</sup> Uo., 20<sup>6</sup> § és 20<sup>7</sup> §.

<sup>67</sup> Alapkonceptió, lásd a fenti 16. jegyzetet, 9. old.

<sup>68</sup> Még ha azokat az eljárás megindításakor a külképviseleti szervekhez nyújtják is be, a kérelmeket elbírálásra Észtországba, a Rend- és Határőrség munkatársaihoz továbbítják.

<sup>69</sup> Az online kérelmezési portál megnyitását követően a Rend- és Határőrség munkaterhe tovább növekedett; jelen tanulmány megírásának pillanatában úgy tűnik, hogy a megnövekedett munkateher problémát jelent, legalábbis a hivatalos weboldal közleménye szerint az elbírálási folyamat lelassult: „A kérelmek nagy számára való tekintettel a kérelmek elbírálásának folyamata jelenleg a remélnél hosszabbra nyúlik. Türelmüket köszönjük.”

kívül szembeötlő különbség mutatkozik az e-polgárok létszámára vonatkozó azon elképzelések között, amit az Észtország Digitális Menetrendje 2020 stratégia lefektetett, valamint azon értékek között, amit az ötlet gazdái dolgoztak ki. Az előbbi azt a célt tűzte ki, hogy 2020-ra 5000 e-személyazonossági kártyát bocsássonak ki a nem rezidensek számára, ami hozzávetőlegesen egyezer új e-polgárt jelentene évenként. Mivel már az első 10 hónapban ezt a célt teljesítették, az e-polgárság kifejezetten sikeresnek mondható. Az utóbbi célkitűzés (amely szerint 2025-re legyen 10 millió digitális észt polgár) eléréséhez nem csak az intézményi kapacitás óriási mértékű megnövelésére volna szükség, hanem arra is, hogy magát az alapötletet még kívánatosabbá tegyék.

### *Jogbiztonság teremtése az e-polgárok számára*

Az a tény, hogy az e-polgárrá váláshoz előzetes követelményként Észtországgal fennálló kapcsolatra vagy jogos érdek bizonyítására van szükség, ugyanakkor nem lehet pontosan tudni, hogy ezek mit is jelentenek, arra a körülményre utal, hogy az észt rendszert olyannak kell tekintenünk, amelyből hiányoznak a kidolgozott részletszabályok, viszont amely ugyanakkor kétértelmű rendelkezéseket is tartalmaz. A személyazonossági okmányokra vonatkozó észt törvény jelentős szabadságot hagyott annak értelmezésében, hogy kinek a részére és milyen feltételek mellett lehet e-polgárságot adni, amely viszont az e-polgársággért folyamodó jelöltek és a tényleges e-polgárok körében jogbizonytalanságot eredményezhet. Annak ellenére, hogy az észt e-szolgáltatásokhoz való hozzáférés kulcsaként népszerűsítik, az Alapkoncepció mégis úgy rendelkezik, hogy nem lehet mindenholnans tetszés szerint hozzáférni mindahhoz, amit Észtország az ott élőknek és/vagy az állampolgárainak kínál. Az e-polgárokat korlátozhatják azok a határok, amelyeket a magánszektorban működő szolgáltatók – saját döntésük alapján – a szolgáltatásaikhoz való hozzájutás elé állítanak.<sup>70</sup>

Ennek megfelelően (azon az alapon, hogy egy szolgáltató helyénvalóbbnak vélheti, ha szolgáltatásait csakis a helyben élőknek és/vagy az állampolgároknak kínálja fel) a szolgáltatókat megilleti az a diszkrecionális döntési lehetőség, hogy szolgáltatási körükből kihagyják az e-polgárokat. A fentiekén túl a hivatalos magyarázat leszögezi: megfelelően indokolt esetekben [põhjendatud juhtudel] megtörténhet az, hogy az e-polgárokat korlátozzák a nyilvánosság számára nyitva álló digitális szolgáltatásokhoz történő hozzáférésben, vagy az ilyen hozzáféréshez tőlük további előfeltételek teljesítését követelik meg, mindez pedig segít csökkenteni az e-polgársághoz kapcsolódó kockázatot.<sup>71</sup> A fenti elemek kombinációja egyben azt is jelenti, hogy az e-polgár nem reménykedhet (és talán eleve nem is kellene reménykednie) abban, hogy korlátlan hozzáférése lesz e-Észtország birodalmához.

A személyazonossági okmányokra vonatkozó észt törvény rendelkezései szerint, valamint az Alapkoncepció<sup>72</sup> értelmében egy e-polgár jogállása leginkább egy külföldi állampolgáréhoz hasonlít, a helyzet pedig leginkább a vízumkiadásra emlékeztet – nincsen olyan alanyi jog, amely szavatolná az Észtországban való tartózkodást, továbbá nem létezik olyan

<sup>70</sup> Alapkoncepció, lásd a fenti 16. jegyzetet, 8. old.

<sup>71</sup> Uo., 8. old.

<sup>72</sup> Alapkoncepció, lásd a fenti 16. jegyzetet, 10. old.

alanyi jog sem, amely szavatolná azt, hogy az illető Észtországtól személyazonossági okmányt fog kapni. Ezen túl az e-polgárság megadása, megadásának megtagadása, illetve a felügyeleti jog gyakorlása az állam részéről nem követel meg további indokolást.<sup>73</sup> Ennek megfelelően azt kell hangsúlyoznunk, hogy sem az előbbiekben említett egyetlen intézkedés, sem pedig az állam részéről alkalmazott felfüggesztés, illetve felügyelet sem sérthet „*valamilyen nem létező emberi alapjogot vagy szabadságjogot*”, mivel egy e-polgár helyzete leginkább egy ideiglenes tartózkodási engedéllyel rendelkező külföldi személyéhez hasonlít.<sup>74</sup>

Mindez pedig az e-polgárok jogállását nehezen értelmezhetővé teszi – az ugyan egyértelmű, hogy a kérdéses férfi vagy nő nem észtországi állandó lakos, illetve nem észt állampolgár; mindazonáltal ha a kérdéses személy digitális identitást és azonosítószámot kapott, amelynek alapján ezt a személyt a nemzeti nyilvános kulcsú infrastruktúra használata során egyértelműen be lehet azonosítani, a fentieknek egyben azt is eredményeznie kellene, hogy az ilyen személy Észtországgal fennálló viszonya egy ideiglenes tartózkodási engedéllyel rendelkező külföldi személyéhez képest mélyebb és erősebb bizalmon nyugodjon. A fentiek megkoronázásaként úgy tűnik továbbá, hogy az Alapkonceptió szerzői nem értették meg azt, hogy mit jelentenek az „alapvető emberi jogok” és „szabadságjogok”.

### *Több biztonság – kevesebb magánszférához való jog?*

Ahogy az az előző alponban részletesen bemutatuk, a Rend- és Határőrség, amelyhez az e-polgárságra pályázó jelöltek (a nagykövetségeken keresztül vagy online) benyújtják személyes adataikat, döntési jogkörrel rendelkeznek az e-személyazonosság megadására vagy megtagadására vonatkozóan oly módon, hogy meggyőződik a kérelmező kilétéről, továbbá mérlegeli jogos érdekének indokait. A digitális polgárjelölt szabványos formában megküldi az észt hatóságok részére azokat a dokumentumokat és adatokat (beleértve ebbe a biometrikus adatokat is<sup>75</sup>), amelyek egyébként a szokványos nemzeti személyazonossági okmányok, tehát az olyan észt útlevelek és személyi igazolványok kibocsátásához is szükségesek, amelyeket személyazonosításra lehet használni például utazás esetén. Az észt jogszabályok értelmében a személyazonossági okmányokat és a beküldött adatokat egy különleges állami adatbázisban kell tárolni, amelynek rendeltetése „az állam belső biztonságának szavatolása annak révén, hogy nyilvántartja az egyes személyek személyazonosságát, valamint személyazonossági okmányainak kibocsátását és visszavonását.”<sup>76</sup> Az X-Road rendszeren keresztül, digitális úton történő engedélyezéssel hozzáférhető szolgáltatásokat olyan állami informatikai adatbázisokban tárolják, amelyeknek az állami informatikai rendszer adatcserélő funkciójával közös felülete van.<sup>77</sup>

Az informatikai rendszerekben feldolgozott adatokat olyan három szintű IT biztonsági rendszer (ISKE) védi, amelyet egy német biztonsági szabvány – IT Baseline Protec-

<sup>73</sup> Uo., 10-11. old., valamint az IDA, lásd a fenti 19. jegyzetet, § 20<sup>7</sup> (3).

<sup>74</sup> Alapkonceptió, lásd a fenti 16. jegyzetet, 11-12. old.

<sup>75</sup> IDA, lásd a fenti 19. jegyzetet, § 9.

<sup>76</sup> Uo., §15<sup>2</sup>.

<sup>77</sup> A nyilvánosság számára hozzáférhető adatokra vonatkozó törvény, 43<sup>2</sup> §. Az állami informatikai rendszer.



tion Manual (németül „IT-Grundschutz”) – alapján kifejezetten az észti közszektor igényeihez igazítottak, továbbá amelynek használatára minden olyan állami és önkormányzati szerv köteles, amely adatbázisokat/nyilvántartásokat kezel.<sup>78</sup> Az ISKE szerint a biztonság-nak három szintje van: alacsony (L), közepes (M) és magas (H). A személyazonossági okmányok adatbázisában tárolt információ a legmagasabb (H) védelmi szinttel rendelkezik. Ahogyan ez az e-személyazonossági okmányok technológiai háttérét leíró részben korábban bemutatásra került, egyetlen olyan hitelesítő rendszer létezik, amely mindkét dokumentumtípus, tehát az állampolgárok és az e-polgárok részére kiadott személyazonossági kártyák szempontjából is biztonságosnak bizonyult.<sup>79</sup> Mindazonáltal, a fentiekén túl – a digitális személyazonosságok rendszerének támogatása, továbbá alapvető biztonságának védelme érdekében – minden egyes olyan személy biometrikus adatait, aki valaha is észti személyazonossági kártyát kérelmezett vagy kapott (tekintet nélkül arra, hogy ez az állampolgárokat megillető rendes vagy csak e-személyazonosításra alkalmas digitális személyazonossági dokumentum-e), digitális adatbázis-kártyákon tárolják, amelyeket 50 évre archiválnak és megőriznek<sup>80</sup> (az e-polgárság esetén mindezt annak megelőzése érdekében teszik meg, hogy egyazon személy részére ne kerüljön kibocsátásra több digitális identitás<sup>81</sup>).

A biometrikus adatok útlevélbe és egyéb úti okmányokba történő beépítése a 2252/2004/EK tanácsi rendeletnek<sup>82</sup> megfelelően megy végbe; ugyanakkor megjegyzendő, hogy a biometrikus útlevél bevezetése érdekében az Európai Unióra elsődlegesen az USA kormánya gyakorolt nyomást a „terrorizmus ellen folytatott háború”<sup>83</sup> jegyében, amelynek során többek között azt igényelte, hogy az EU-tagállamok harmonizálják vonatkozó jogszabályaikat az Egyesült Államok jogszabályaival annak érdekében, hogy részt vehessenek az Egyesült Államok Vízummentességi Programjában, amely szerint az EU-tagállamok polgárai vízumigénylés nélkül léphetnek az USA területére.<sup>84</sup> Az e-polgárok szempontjából mindez irreleváns – ahogyan ezt a fentiekben megállapítottuk, a részükre kibocsátott digitális személyazonossági dokumentumok úti okmányként nem használhatóak. Mindazonáltal, annak a ténynek köszönhetően, hogy a személyazonossági okmányokra vonatkozó észti törvény szövegében a „digitális személyazonossági kártya” kifejezés egyaránt jelöli az állampolgárok, valamint az e-polgárok részére kibocsátott digitális személyazonossági okmányt, a biometrikus azonosítókra előírt követelmények szintén mindkét dokumentumtípusra vonatkoznak.

<sup>78</sup> 252. sz. (2007.12.20-án kelt) kormányrendelet az informatikai rendszereket védő biztonsági rendszerekről [Infosüsteemide turvameetmete süsteem]. Csak észti nyelven elérhető. Az angol nyelvű összefoglalóért lásd az informatikai rendszerekért felelős hatóság honlapját. <https://www.ria.ee/en/iske-en.html>

<sup>79</sup> Személyazonossági kártya. Számítógépes védelem. Biztonságos bejelentkezési pont. ID-kaart. Arvutikaitse. Infoturvalisuse teeviit. Csak észti nyelven elérhető a következő helyen: <http://www.arvutikaitse.ee/arvutikaitse-algoed/id-kaart/>

<sup>80</sup> 109 sz. (2008.07.03-án kelt) kormányrendelet, a személyazonossági okmányokra vonatkozó adatbázis működtetéséről [Isikut tõendavate dokumentide andmekogu pidamise põhimäärus] 4. és 18. §. Csak észti nyelven elérhető.

<sup>81</sup> Alapkonceptió, lásd a fenti 16. jegyzetet, 9. old.

<sup>82</sup> A Tanács 2252/2004/EK rendelete (2004. december 13.) a tagállamok által kiállított útlevélbe és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról.

<sup>83</sup> Goncalves és Gameiro (2012: 324)

<sup>84</sup> A 2252/2004/EK rendelet, indokolása, elérhető az EUR-Lex portálon keresztül.

A fentiekre támaszkodva jelen tanulmány szerzői úgy vélekednek, hogy a két dokumentumtípus közötti sikertelen különbségtétel a biometrikus adatok szükségtelen begyűjtését eredményezi, amely viszont ellentétben áll az Adatvédelmi Irányelv 6. cikkében rögzített alapelvekkel, a szükségesség és arányosság követelményével<sup>85</sup> (az Adatvédelmi Irányelv tervezetének 5. cikke<sup>86</sup>). Az Adatvédelmi Irányelv tervezetének 29. cikke alapján létrehozott munkacsoport elismerte, hogy a biometrikus adatok növekvő mértékű használata speciális adatvédelmi kockázatokat eredményez, amely kockázati tényezők tovább növekednek abban az esetben, ha a biometrikus adatokat külső adatbázisokban tárolják; ha pedig alternatívaként a magánszférába kevésbé behatoló megoldások is rendelkezésre állnak, a biometrikus adatok használata ilyen esetben nem célszerű.<sup>87</sup> A munkacsoport hangsúlyozta azt is, hogy már kiinduláskor világosan meg kell határozni, hogy az ilyen adatokat a továbbiakban milyen célra óhajtják használni, majd ezt követően a személyes adatok gyűjtésének terjedelme – azon célokkal összevetve, amelyek érdekében az adatgyűjtés történik – nem lehet túlzott mértékű; „[m]ás szavakkal megfogalmazva, az olyan hitelesítő applikációk, amelyeket biometrikus adatok központi tárolása nélkül is lehet működtetni, nem alkalmazhatnak túlzott mértékű személyazonosító technológiákat.”<sup>88</sup>

Szem előtt tartva azt, hogy az e-polgárok személyazonossági kártyáját csakis digitális azonosításra lehet felhasználni, fizikai értelemben vett személyazonosításra azonban nem, a biometrikus adatok igénylése egyértelműen ésszerűtlennek és aránytalannak tűnik, az e-polgárságra vonatkozó észt jogszabályok pedig a fenti követelményeknek minden vonatkozásban ellentmondanak. A biometrikus adatok fizikai értelemben vett személyazonosításra történő, EU-keretszabályozásban előírt használata nem terjedhet ki a digitális személyazonosításra; számos szerző figyelmeztetett már arra, hogy a biometrikus adatok használatának előnyeit még az úti okmányokban és útlevelekben történő felhasználás során is gyakran elhomályosítja az a körülmény, hogy az ilyen adatokat eltárolják, amely aztán a biometrikus adatok olyan megkérdőjelezhető módon történő felhasználását is eredményezheti, mint a megnövelt felügyelet és kontroll, amely végső soron „ügynevezett Nagy Testvér-effektust” (Schouten és Jacobs 2009: 311) vagy „globális rendőrállamot” (Ashburn 2005: 20) szülhet. Az e-polgárság esetében a biometrikus adatok használatát – a fentiekben említettek szerint – azzal indokolják, hogy ezáltal megelőzhető a többes identitások létrejötte. Jelen pillanatban csak spekulálhatunk arról, hogy mindez arányos és szükséges-e, vagy sem.

A digitális technológiák szabályozásával foglalkozó számos szerző a nemzeti és szupranacionális jogrendszerek szempontjából elemezte a magánszféra és a személyes adatok védelmével kapcsolatos különböző kihívásokat és újonnan felmerülő problémákat, amelyeket az egyre intenzívebbé váló digitalizáció, valamint az e-kormányzati rendszerekbe

<sup>85</sup> 95/46/EK Irányelv.

<sup>86</sup> Javaslat a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet). Végleges COM(2012) 11 javaslat.

<sup>87</sup> A 29. cikk szerint létrehozott munkacsoport. A magánélet-védelem jövője: közös hozzászólás a személyes adatok védelméhez fűződő alapvető jog jogszabályi keretéről szóló európai bizottsági konzultációhoz, 14., 26. és 27. old.

<sup>88</sup> A 29. cikk szerint létrehozott munkacsoport. A biometrikus adatokról szóló munkadokumentum, 6. old.

beépült technológiai újítások generálnak.<sup>89</sup> Dutt és Kerikmäe, akik az e-demokráciával összefüggő kérdésekbe és problémákba nyújtottak betekintést, úgy vélekedtek, hogy „az állampolgárok részére biztosított, védett és biztonságos online identitás” jelenti a kulcs-tényezőt az e-demokrácia sikerre vitelében, amely „a demokrácia sarkalatos vonásai közé tartozik” (Dutt és Kerikmäe 2014: 294). Mindazonáltal ha szembeállítjuk az e-személyazonossági okmányokat körbevevő, biztonságos és többszintű műszaki infrastruktúrát egy másik további biztonságtechnikai megoldással – a biometriával – ez utóbbi potenciálisan káros hatással is bírhat az (e-)demokráciára nézve. Már születtek olyan érvelések, amelyek szerint, ha anélkül engedünk túlzott teret az új technikai fejlesztéseknek, hogy alapjogi szempontból alaposan megvizsgálánánk azok lehetséges hatásait, a biztonsági intézkedések (gyakran szinte észrevehetetlen) megsokszorozódása végső soron a demokrácia létét sodorhatja veszélybe (Goncalves és Gameiro 2013: 322-323). A biztonsági technikaként alkalmazott biometriát nem „dobhatjuk csak úgy be” a gyakorlatba (mint ahogyan azt szemmel láthatólag Észtország tette) anélkül, hogy előzőleg az alapvető emberi jogok és szabadságjogok szempontjából ne folytánánk le megfelelő kockázatelemzést, továbbá annak megfontolása nélkül, hogy az elérendő célt nem tudnánk-e megvalósítani a magánszférába kevésbé behatoló megoldások alkalmazásával.

Tíz évvel ezelőtt Ashbourn elítélte a biometriát támogató kormányokat, és a következő módon emlegette őket: „fejtlenül belerohantak abba, amit csak a biometriával összefüggő kezdeményezések iránti esztelen rajongásként írhatunk le, amelyhez az érzelmileg félrevezető, technikai szempontból pedig pontatlan retorika ködfelhője társult” (Ashbourn 2005: 21). Bár a személyazonosítás innovatív technikai megoldásai érdekes műszaki kihívást jelentenek – írta –, nem viselkedhetünk úgy, mint a technológia játékszereivel játszadozó kisgyerekek.<sup>90</sup> Az e-polgárság bevezetését megelőzően Nyman-Metcalf, az e-kormányzás elismert szakembere, a következőket indítványozta: az e-kormányzás lehetséges jogszabályi kereteinek fontolgatása során (ideértve a digitális személyazonosság jövőjét is), az olyan kérdések, mint az e-aláírás vagy e-személyazonosítás, megfelelő szabályozásuk érdekében vagy speciálisan új jogi normákat igényelnek, vagy a már létező jogszabályokat kell kifejezetten egyedi módon hozzájuk igazítani (Nyman-Metcalf 2014: 41). A szerző azt is hangsúlyozta, hogy a jog jelenti azt a háttérrel, amelyhez viszonyítva eldönthetjük, hogy az új technológiai fejlesztéseket a gyakorlatban mennyire lehet alkalmazni.<sup>91</sup> Az az észti megoldás, amely szerint az e-polgárságnak a személyazonosító okmányokról szóló törvényen belül „szorítottak helyet”, nincsen különösebb tekintettel a biometrikus adatokkal való lehetséges visszaélés által generált kihívásokra, hanem sokkal inkább a technológiai játékszerekkel való játszadozásnak látszik. Ennek alapján jogi szempontból úgy tűnik, hogy a koncepciót túl gyorsan erőltették keresztül, anélkül, hogy átfogóan mérlegelték volna az e-polgárságot körülvevő sokrétű problémák körét.

<sup>89</sup> Lásd például Katrin Nyman-Metcalf, Ülle Madise, Priit Vinkel, Pawan Dutt, Agnes Kasper, Addi Rull, Ermo Täks és Alexander Norta véleményét, in: Kerikmäe, T. (szerk.) *Regulating eTechnologies in the European Union. Normative Realities and Trends*. Springer International Publishing Switzerland. 2014.

<sup>90</sup> Uo.

<sup>91</sup> Uo., 34. old.

## Szülhet-e az e-polgárság digitális világpolgárt?

Az előző részekben bemutatott ellentmondásosságok ellenére az e-polgárság önmagában vett koncepciója innovatív és eddig még nem látott, továbbá megfelel annak az igénynek, hogy a digitális személyazonosság határokon átívelő módon kerüljön elismerésre – észrevételezésre került, hogy a folyamatos műszaki fejlődésnek, továbbá az információáramlás rendkívüli mértékű növekedésének köszönhetően az információk biztonságos és megbízható továbbítása (és ezen belül is az egyén személyazonosságának digitális úton történő ellenőrzése) minden kétséget kizáróan óriási kihívást jelent. Bizonyos elméleti szakemberek (mint például Al-Khouri) úgy érvelnek, hogy a fizikai és digitális személyazonosságot összekapcsoló biztonságos és megbízható eszközök hiánya megakadályozza a fejlődést, továbbá kizárja azt, hogy a globális szintű digitális gazdaság által kínált potenciált teljes mértékben kihasználjuk (Al-Khouri 2014).<sup>92</sup> Érvelése az OECD 2011-es jelentésén nyugszik, amely hangsúlyozza a digitális személyazonosságok globális szintű kezelésének szükségességét, ezen belül a „távrolról történő, biztonságos interakciót” lehetővé tevő eszközök biztosítását, valamint az internetes gazdaság további fejlesztését.<sup>93</sup> A jelentés arra bátorította a kormányokat, hogy a személyazonosságok kezelésére fogadjanak el nemzeti stratégiát, az e-kormányzat által kínált szolgáltatásokat igazítsák ehhez a stratégiához, majd ezt követően nemzetközi szinten kooperáljanak a megoldások kölcsönös elismerése érdekében azért, hogy lehetővé tegyék a határokon átívelő digitális adatkezelést.<sup>94</sup>

Az Európai Unió szintjén a határokon átívelő online szolgáltatások elektronikus személyazonosító és beléptető rendszerek révén történő biztonságos igénybevétele az intelligens, fenntartható és inkluzív fejlődésre vonatkozó „Európa 2020” stratégia részét képezi.<sup>95</sup> A stratégia gyakorlati megvalósítása során az EU-n belül az e-személyazonosítás és a digitális aláírások kölcsönös elismerésére vonatkozóan javasoltak, majd elfogadtak egy külön rendeletet<sup>96</sup> abból a célból, hogy keretet biztosítsanak a biztonságos és megbízható, határokon átívelő digitális kommunikációhoz, valamint az e-kormányzati szolgáltatások olyan rendszeréhez, amely az Európai Unión belül a polgárok, a gazdasági vállalkozások és a hatóságok számára egyaránt átjárható.<sup>97</sup> A rendelet többek között körvonalazza azt is, hogy a digitális tranzakciók biztonságosságának növelése érdekében összeurópai szinten szükség van egy nyilvános kulcsú infrastruktúra megteremtésére, amelynek rendeltetése azonban nem az, hogy akadályozza az elektronikus személyazonosságok kezelésére vonatkozóan már létező nemzeti infrastruktúra (mint például az észt nemzeti e-személyazonosítási rendszer) működését, hanem hogy biztosítsa a rendszerek közötti átjárhatóságot.

<sup>92</sup> Lásd még Graux (2013), De Andrade (2012) valamint De Andrade (2013)

<sup>93</sup> OECD (2011). A digitális személyazonosság innovációt és bizalmat lehetővé tevő kezelése az internetes gazdaságon belül.

<sup>94</sup> Uo.

<sup>95</sup> Az Európa 2020 Bizottság közleménye. Az intelligens, fenntartható és inkluzív fejlődés stratégiája. COM(2010) 2020, végleges változat.

<sup>96</sup> 910/2014/EU rendelet.

<sup>97</sup> Ámbár az Európai Unió szintjén már az Európa 2020 Digitális Menetrend előtt is létezett jogi keretszabályozás a digitális aláírásokra vonatkozóan, ez csak az elektronikus aláírásokra vonatkozott (1999/93/EK irányelv), és nem terjedt ki a digitális személyazonosításra és más olyan bizalmi szolgáltatásokra, mint például az időbélyegzés.

Európa eme kicsiny zugában hatékony megoldásnak az a program tűnik, amely külföldi állampolgároknak digitális bizalmi (e-trust) szolgáltatásokat kínál a már korábban létező nemzeti személyazonosító dokumentumok mintájára, az állami támogatással működő PKI rendszerén belül, amely biztonságos azonosító és beléptető eszközök használatával nyújt hozzáférést a magán- és közszféra szolgáltatásaihoz – mindezt pedig e-polgárságnak nevezzük. Sajátos vonásként az e-polgárság csak azért létezik, hogy hozzájárulást biztosítson az észti gazdasághoz, tudományhoz, oktatáshoz, illetve kultúrához, továbbá hogy felhívja a figyelmet a technológiai szempontból rendkívül fejlett Észtországra (amely ország talán már akkor birtokában volt mindannak, ami a digitális személyazonosságok globális – vagy legalábbis EU-szintű – kezeléséhez szükséges, amikor a világ még nem is gondolt arra, hogy ilyesmire szüksége lesz); továbbá zárt rendszerként működik, amelyet nem arra terveztek, hogy a digitális személyazonosságok kölcsönös elismerését célzó globális *modus operandi* legyen. Az észti személyazonosító kártya továbbá csak egy a számos nemzeti e-személyazonosító megoldás közül, ám bár az is tagadhatatlan, hogy a nemzeti szintű integráció és használhatóság szempontjából valószínűleg a legsikeresebb rendszerek egyike. A személyazonosságok kezelésére szolgáló és a piacon is hozzáférhető rendszerek és technikai megoldások (mint amilyen például az Apple trackpad segítségével történő digitális aláírása) exponenciális ütemű szaporodásának korszakában az észti megoldások kiemeltnek a többi közül (Hoikkanen et al. 2010: 6) – annak eredményeként, hogy a digitális személyazonosítást átfogó módon, a köz- és magánszférában jelen levő digitális szolgáltatások használatára szempontjából egyforma mértékben teszik lehetővé. Ennek ellenére tehát, hogy első pillantásra úgy tűnik, hogy az e-polgárság jelentheti a határokon átvélt digitális személyazonosítás kulcsát, az e-polgár program a kezdet kezdetétől fogva zárt, Észtországot patronáló rendszerként hirdette magát, amely sohasem mutatott fel globális szintű emberbaráti célokat.<sup>98</sup> A fentiekre való tekintettel az e-polgárságra nem szabad úgy tekinteni, hogy ez jelenti a globális digitális állampolgárság megteremtéséhez szükséges csodaszert, hanem – tekintetbe véve mindazt a figyelmet, amelyet Észtország javára generált – inkább egyfajta lelkes nemzeti startup-vállalkozásként kellene értékelni, amely briliáns módon szolgálja eredeti célját; azt, hogy óvja és támogassa egy technológiailag rendkívül fejlett ország imázsát.

## Záró megjegyzések

Jelen tanulmány azt körvonalazta, hogy rendkívül ambíciózusnak tekinthető az a törekvés, amelynek értelmében egy külföldi, mondjuk Sri Lanka-i állampolgárból digitális észtet teremtünk; továbbá annak ellenére, hogy az észti jogi keretszabályozásban mutatkoznak bizonyos hiányosságok, valamint kétség merülhet fel arra vonatkozóan, hogy az illetékes hatóságok vajon képesek-e hatékonyan megvalósítani az e-polgárság programot, maga az alapkoncepció gyorsan átkerült a gyakorlatba, ami világszinten is kiemelkedő figyelmet keltett. Az e-polgárság a világ számos pontján indított arra embereket, hogy digitális észti

<sup>98</sup> Különös módon Graux - miközben az Európai Uniónak a digitális aláírásokra vonatkozó irányelve által felvetett problémákat elemezte - észrevételezte, hogy az átfogó elektronikus hitelesítés EU-ban megszokott kereteit üzleti célokra is fel lehetne használni, mivel hogy az EU szupranacionális szinten ezt a lehetőséget nem tiltotta meg. Lásd Graux (2011).

polgárrá váljanak, akiknek körében példának okáért megtalálhatjuk az ismert brit újságíró, Edward Lucast (aki egyben az első e-polgár is), továbbá olyan magas rangú vezetőket, mint japán miniszterelnöke, Shinzō Abe. Annak a ténynek köszönhetően, hogy az e-polgárság zárt nemzeti rendszerként indult, amely – az észt fejlődéshez való hozzájárulást szem előtt tartva – külföldi állampolgárok számára kínál észtországi e-szolgáltatásokat, továbbá őket az észt e-személyazonossági rendszerben egyesíti, a programot sikeres megoldásnak tekinthetjük. Nem tekinthető viszont sikernek az e-polgárság koncepciójának gyakorlati megvalósítása abból a szempontból, hogy mennyire jól illeszkedik a nemzeti és nemzetközi jogi szabályozás keretei közé.

Bár a kezdet kezdetétől fogva világosan hangsúlyozásra került, hogy az e-polgár program nem törekszik arra, hogy a digitális személyazonosságok kezelésének világszintű vagy EU-s gyakorlati modelljeként szolgáljon, adatvédelmi szempontból a koncepciót újra kell gondolni; mindezt pedig azért, hogy a modell tényleg hasonlítson arra a digitális álmra, amelynek létrehozói szánták. Jelen pillanatban az észt kormányzat az észt polgárok vonatkozásában kettős szerepet tölt be – egyszerre barát és ellenség. A másik oldalról nézve Észtország a személyazonosítás olyan kipróbált, biztonságos és áramlólag támogatott rendszerét kínálja, amely garantálja az észt e-szolgáltatásokhoz történő biztonságos, elektronikus személyazonosítás útján megvalósuló hozzáférést; ugyanakkor adatvédelmi szempontból kihívást jelent az, hogy az e-polgárok személyes adatait hosszú távon észt adatbázisokban tárolják (Hoikkanen et al. 2010: 4). Az IKT e-kormányzati célokra történő felhasználása megfelelő módszertani megközelítést, valamint gondos elemzést igényel egy olyan egységes szabályozórendszer létrehozása érdekében, amely képes együtt létezni az innovációval és a technológiai fejlődéssel<sup>99</sup> – az e-polgárságot azonban úgy illesztették be a már létező szabályok rendszerébe, hogy ezeknek az összefüggéseknek nem szenteltek megfelelő figyelmet.

Végző soron megállapítható, hogy az e-polgárság koncepcióját körbevevő általános keretszabályok szintjén a digitális személyazonosságot óvó biztonsági intézkedések technikai szempontból megbízhatóak, azonban nem állnak teljes összhangban az Európai Unió adatvédelmi irányelveivel. Eme észrevételek célja nem az, hogy Észtországot a titkos és bizalmas adatok biztonságos megőrzése kapcsán potenciális szabálysértéssel vádoljuk meg vagy megkérdőjelezzük kiberbiztonsági stratégiáját, hanem sokkal inkább figyelmeztetést kívánunk megfogalmazni egy olyan ország számára, amely hamarosan külföldi állampolgárok ezreinek adatait fogja digitálisan tárolni egy olyan korszakban, amelyben a kibertámadások egyáltalán nem minősülnek ritkaságnak. Ha továbbá Észtország meg kívánja valósítani a 10 ezer, vagy akár 10 millió e-polgár ötletét, a szerzők ebben a vonatkozásban úgy vélik, hogy elkerülhetetlen az e-polgárságra vonatkozó, jelenleg hatályos jogi szabályozás újragondolása – tehát újra kell gondolni a személyazonossági okmányokra vonatkozó teljes észt törvényt, amelyet korábban csupán módosítottak azért, hogy „helyet csináljanak” az e-polgárságra vonatkozó szabályoknak.

<sup>99</sup> Az innovatív technológiák olyan e-szabályozást igényelnek, amely konzisztens a „hagyományos” szabályozással, valamint azzal együtt alkalmazható. A gyakorlatban megvalósítható e-szabályozás kidolgozása során igény jelentkezik egyfajta progresszív módszertani alap létrehozására is. Az ilyen módszertani megközelítés során alkalmazható 10 elvi irányelvre vonatkozó példát nyújt többek között Kerikmäe és Dutt; lásd Kerikmäe és Dutt (2014: 28-29).

## Irodalom

- A 29. cikk szerint létrehozott munkacsoport. A biometrikus adatokról szóló munkadokumentum. Elfogadva 2003. augusztus 1-jén.  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf)
- A 29. cikk szerint létrehozott munkacsoport. A magánélet-védelem jövője: közös hozzászólás a személyes adatok védelméhez fűződő alapvető jog jogszabályi keretéről szóló európai bizottsági konzultációhoz. Elfogadva 2009. december 1-jén.  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf)
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, OJ L 281, 23.11.1995
- Az Európai Parlament és a Tanács 1999/93/EK irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről, OJ L 13, 19.1.2000
- Az Európai Parlament és a Tanács 2252/2004/EK rendelete a tagállamok által kiállított útlevélek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról, OJ L 385, 29.12.2004
- Az Európai Parlament és a Tanács 2252/2004/EK rendeletének háttéranyaga. Elérhető az <http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R2252>.
- Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről, OJ L 257, 28.8.2014
- Az Észt Köztársaság elektronikus aláírásokra vonatkozó törvénye. [Riigikogu, Digitaalalkirja seadus, 15.12.2000, RT I, 2000, 26, 150 <https://www.riigiteataja.ee/en/eli/ee/530102013080/consolide/current>
- Az Észt Köztársaság személyazonossági okmányokra vonatkozó törvénye. § 205. Az e-polgár digitális személyazonossági kártyája. [Eesti Vabariigi Riigikogu, Isikut tendavte dokumentide seadus, 31.12. 2014, RT I, 29.10. 2014, 5]  
<https://www.riigiteataja.ee/en/eli/512112014001/consolide>
- Az Észt Köztársaság közérdekű információkra vonatkozó törvénye. [Eesti Vabariigi Riigikogu Avaliku Teave seadus, 31.12.2015, RI I, 12.07.2015  
<https://www.riigiteataja.ee/en/eli/522122014002/consolide>
- Az Észt Köztársaság idegenrendészeti törvénye. [Riigikogu Välismaalaste seadus, 01.05.2016, RT I, 06.04.2016 <https://www.riigiteataja.ee/en/eli/513042015008/consolide>
- Az Észt Kormány 109 sz. (2008.07.03-án kelt) rendelete, a személyazonossági okmányokra vonatkozó adatbázis működtetéséről. [Eesti Vabariigi Valitsuse 03.07.2008 nr 109 määrus, Isikut tõendavate dokumentide andmekogu pidamise põhimäärus, RT I 200831, 195].
- Az Észt Kormány 252. sz. (2007.12.20-án kelt) rendelete az informatikai rendszereket védő biztonsági rendszerekről. [Eesti Vabariigi Valitsuse 25.01.2009 nr 252 määrus Infosüsteemide turvameetmete süsteem, RT I 2007, 71, 440].
- Az Észt Kormány 361 sz. (201503.23-án kelt) rendelete, amely meghatározza a személyazonossági kártya kibocsátására vonatkozó kérelemmel együtt benyújtandó igazolások és adatok jegyzékét, továbbá a személyazonossági kártya, állandó lakcímet igazoló kártya, digitális személyazonossági kártya, észt állampolgárt megillető útlevél, tengerhajózási szolgálatból történő leszerelési okmány, ideiglenes útlevél, menekültútlevél, továbbá hajón töltött szolgálatot igazoló bizonyítvány kibocsátásának előfeltételeit. [Vabariigi Valitsuse määrus 26. 11.2002 nr 361, RT I, 23.03.2015, 57, Isikutunnistuse, elamisloakaardi, digitaalse isikutunnistuse, Eesti kodaniku passi, meremehe teenistusraamatu, välismaalase passi, ajutise reisidokumendi, pagulase reisidokumendi või meresõidutunnistuse väljaandmise taotlemisel esitatavate tõendite ja andmete loetelu ning väljaandmise tähtjad]
- A.A.K, „How did Estonia become a leader in technology?” *The Economist*. 2013. július 30.  
<http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21>

- Al-Khouri, Ali. M., „Digital identity: Transforming GCC economies”, *Innovation: Management, policy & practice*, XVI. évf. (2014) 2. szám, pp. 184–194.  
<http://dx.doi.org/10.1080/14479338.2014.11081981>
- Ashbourn, Julian, „The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies”, Background paper for the Institute of Prospective Technological Studies, DG Joint Research Centre, European Commission, 2005.
- Braw, Elisabeth, „‘E-stonia’ Attempts to Become the Uber of Economies by Introducing Virtual Residency.” *Newsweek*. 2014. október 30. <http://www.newsweek.com/2014/11/07/estonia-attempts-boost-economy-introducing-virtual-residency-280571.html>
- De Andrade, Norberto Nuno Gomez, „Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty’s competences and legal basis for eID”, *Computer Law & Security Review*, 28. évf. (2012) 2. szám, pp. 153-162. <http://dx.doi.org/10.1016/j.clsr.2012.01.012>
- De Andrade, Norberto Nuno Gomez, „Electronic Identity for Europe: Moving from Problems to Solutions”, *Journal of International Commercial Law and Technology*, VIII. évf. (2013) 2. szám, pp. 104-109.
- Dutt, Pavan Kumar, Tanel Kerikmäe, „Concepts and Problems Associated with eDemocracy”, in Tanel Kerikmäe (ed.) *Regulating eTechnologies in the European Union: Normative Realities and Trends*, Springer Verlag, 2014, pp. 285-323. [http://dx.doi.org/10.1007/978-3-319-08117-5\\_13](http://dx.doi.org/10.1007/978-3-319-08117-5_13)
- Európai Bizottság, *Európa 2020 Az intelligens, fenntartható és inkluzív fejlődés stratégiája*, 2010. március 3. <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52010DC2020>
- Európai Bizottság, *Európai Digitális menetrend*, 2010. május 19. <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=URISERV%3Aasi0016>
- Európai Bizottság, *Javaslat a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet)*. COM(2012) 11 végleges szöveg.
- Észtország kormánya, *Észtország Digitális Menetrend 2020 stratégia*, 2014. [https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020\\_Estonia\\_ENG.pdf](https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf)
- Észtország kormánya, *Digitális személyazonosság kibocsátása nem rezidens személyek részére: az e-polgárság megteremtése. Alapkonceptió. Az észt személyazonossági dokumentumokra, továbbá állami illetékekre vonatkozó törvénytervezet magyarázó kommentárjának függeléke. 1. sz. Függelék*. [Mitterresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptioon. Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu seletuskirja juurde. Lisa 1.] 2014.
- Freedom House, *Az internet szabadsága 2014. Észt országjelentés*, Freedom House, 2014. <https://freedomhouse.org/report/freedom-net/2014/estonia>
- Goncalves, Maria Eduarda, Maria Gameiro, „Security, privacy and freedom and the EU legal and policy framework for biometrics”, *Computer Law & Security Review*, 28. évfolyam (2012) 3. szám, pp. 320-327. <http://dx.doi.org/10.1016/j.clsr.2012.03.012>
- Graux, Hans, „Rethinking the e-signatures directive: on laws, trust services, and the digital single market”, *Digital Evidence and Electronic Signature Law Review*, VIII. évf. (2011), pp. 9-24. <http://dx.doi.org/10.14296/deeslr.v8i0.1951>
- Graux, Hans, „Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union”, *Journal of International Commercial Law and Technology*, VIII. évf. (2013) 2. szám, pp. 110-117.
- Hoikkanen, Anssi, Maria Bacigalupo, Ramon Compano, Wainer Lusoli, Ioannis Maghiros, „New Challenges and Possible Policy Options for the Regulation of Electronic Identity”, *Journal of International Commercial Law and Technology*, V. évf. (2010) 1. szám, pp. 1-10.
- Kerikmäe, Tanel (ed.), *Regulating eTechnologies in the European Union. Normative Realities and Trends*, Springer International Publishing, 2014. <http://dx.doi.org/10.1007/978-3-319-08117-5>
- Kerikmäe, Tanel, Pavan Kumar Dutt, „Conceptualization of Emerging Legal Framework of E-regulation in the European Union” in Tanel Kerikmäe (ed.), *Regulating eTechnologies in the European Union: Normative Realities and Trends*, Springer Verlag, 2014, pp. 7-32.  
[http://dx.doi.org/10.1007/978-3-319-08117-5\\_2](http://dx.doi.org/10.1007/978-3-319-08117-5_2)



- Madise, Ülle, Priit Vinkel, „Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience Over Six Elections” in Kerikmäe, Tanel (szerk.), *Regulating eTechnologies in the European Union: Normative Realities and Trends*, Springer Verlag, 2014, pp. 53-72.  
[http://dx.doi.org/10.1007/978-3-319-08117-5\\_4](http://dx.doi.org/10.1007/978-3-319-08117-5_4)
- Martens, Tarvi, „Electronic identity management in Estonia between market and state governance”, *Identity in the Information Society*, 3. évf. (2010) 1. szám, pp. 213-233.  
<http://dx.doi.org/10.1007/s12394-010-0044-0>
- n.a. „Digital identity cards. Estonia takes the plunge.” *The Economist*, 2014. június 28. <http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge>.
- Nyman-Metcalf, Katrin, „e-Governance in Law and by Law. The Legal Framework of e-governance” in Kerikmäe, Tanel (ed.) *Regulating eTechnologies in the European Union: Normative Realities and Trends*, Springer Verlag, 2014, pp. 33-52. [http://dx.doi.org/10.1007/978-3-319-08117-5\\_3](http://dx.doi.org/10.1007/978-3-319-08117-5_3)
- OECD, *Digital identity management: Enabling Innovation and Trust in the Internet Economy*, OECD, 2011. <http://www.oecd.org/sti/ieconomy/49338380.pdf>
- Schouten, Ben, Bart Jacobs, „Biometrics and their Use in e-passports”, *Image and Vision Computing*, 27. szám (2009), pp. 305–312. <http://dx.doi.org/10.1016/j.imavis.2008.05.008>

**Sandra Sárav**, MA. A Tallinni Jogi Tanszék kutató munkatársa a Tallinni Műszaki Egyetemen és doktorjelölt a svájci Lausanne-i Egyetemen. Kutatási témája az EU állampolgárok személyes adatainak továbbítása tagállamból harmadik országba. A Tallinni Műszaki Egyetemen Európai Unió jogi és e-kormányzati megoldások jogi kereteivel kapcsolatos témákat oktat, közreműködik kutatási projekteken és több tanulmány társszerzője. Sandra Európai Unió és Nemzetközi Jog szakirányon szerzett BA, valamint jog és technológia MA diplomát. Szakdolgozata a határok nélküli digitális polgárság témáját dolgozza fel az észt e-polgárság mintája alapján. Andrus Ansip alelnök hivatalában, az Európai Bizottság Digitális Egységes Piac munkacsoportban szerzett gyakorlatot, ahol főként e-kormányzattal, kiberbiztonsággal, adatáramlással és a digitális adatvédelemmel foglalkozott.

**Tanel Kerikmäe**, PhD. Európai Jogi Jean Monnet-professzor és a Tallinni Jogi Tanszék Igazgatója a Tallinni Műszaki Egyetemen. Több magas színvonalú jogi folyóiratnál szerkesztőségi tag, több, mint 150 tanulmány és publikáció szerzője, valamint témavezetője volt számos EU integrációval foglalkozó doktori hallgatóknak. Tanel szakértőként részt vesz a magán-, és a közzsféra intézményeinek, valamint nemzetközi szervezetek munkájában, így például kulesfontosságú EU szakértő Közép-Ázsiában. Oktatott és témavezető volt számos egyetemen az Egyesült Királyságban, Lettországban és Svájcban, és kapcsolatban áll nemzetközi kutatási hálózatokkal. Gyakori meghívott előadó magasszintű konferenciákon az Amerikai Egyesült Államokban, Portugáliában, Magyarországon, Új-Zélandon, Németországban, Kambodzsában és más országokban. Kerikmäe professzor jelenleg több olyan projektért felelős, mint a Horizont 2020 vagy az Unió szomszédos országainak versenyképességét növelő fejlesztési segélyezési programok az EU szomszédsgpolitikájának keretén belül.

**Kasper Ágnes**, PhD. 2004-ben, Magyarországon a Szolnoki Főiskolán közgazdász, 2007-ben Észtországban a Nemzetközi Audentes Egyetemen jogi diplomát szerzett, és 2015-ben szintén Észtországban az Európai Üzleti Egyetemen vezetéstudományi szakirányon doktorált. Disszertációja a kiberbiztonság jogi vonatkozásait és a döntéshozatalt támogató háttérelmézés elméleti kereteit taglalja. Szerzett szakmai tapasztalatokat a közzsférában külképviseleten, a versenyszférában szoftverfejlesztő vállalat jogtanácsosaként, valamint emberi jogi szervezet munkatársaként is. A Tallinni Műszaki Egyetemen oktat kiberbiztonsággal, digitális bizonyítékokkal és az infotechnológia jogi aspektusaival kapcsolatos tárgyakat. Kutatási területei: kiberbiztonsági jog, digitális bizonyítékok, technológia-jogi elméletek