Az adatvédelem és adatbiztonság nemzetközi és hazai szabályozása

Vécsi Ádám
Debreceni Egyetem Informatikai Kar
Számítógéptudományi Tanszék

Tartalomjegyzék

1. Bevezetés **2**

2. Az adat és felhasználása **2**

3. A jogi szabályozás koncepciója **3**

3.1. Jogszabályok hierarchiája 3
3.2. Jogalkotás az Európai Közösségben 4
3.3. Európai uniós irányelvek 4
3.4. Jogharmonizáció Magyarországon 5

4. Nemzetközi szabályozás **6**

4.1. A Gazdasági Együttműködési és Fejlesztési Szervezet és irányelvei 6
4.2. Európai Uniós Hálózat- és Információbiztonsági Ügynöksége 7
4.3. Az általános adatvédelmi rendelet 8
4.4. Az elektronikus azonosítási és bizalmi szolgáltatásokról szóló rendelet . . . 9

5. Hazai szabályozások **11**

5.1. Alaptörvény a személyes adatról 11
5.2. Irányelvek az állami és önkormányzati szervek és nemzeti adatvagyon védelméről 12
5.3. Szankcionálás Magyarországon 13

1. Bevezetés

Az információ technológia gyors fejlődése nem csupán mérnöki problémákat hoz előtérbe, hanem jogi szempontból is fontos kérdésekre követel meg válaszokat és szabályozásokat. Dolgozatomban az adatvédelem fontosságát bemutató rövid kitérő után az adatbiztonságra és adatvédelemre vonatkozó irányelveket és szabályozásokat fogom bemutatni, ami az utóbbi évtizedben számos változáson ment keresztül.

Ismertetem a jogszabályok hierarchiájára, valamint az európai közösségben történő jogalkotásra és az EU irányelveire, továbbá a jogharmonizációra. Ezzel egy áttekintést adva a jogi szabályozás koncepciójáról.

Szemléltetem az aktuális nemzetközi szabályozásokat, az Európai Uniós Hálózat- és Információbiztonsági Ügynökségét (ENISA) és ajánlásait, a 2016-ban bevezetett EU Általános Adatvédelmi Rendeletét (GDPR), az elektronikus azonosítási és bizalmi szolgáltatásokról szóló rendeletet és a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) irányelveit.

Ezt követően a hazai szabályozásokat mutatom be, az alaptörvénytől az irányelvekig, illetve szót ejtek a büntető törvénykönyv alapján a szankcionálásról is.

2. Az adat és felhasználása

A fejezet célja, hogy röviden rámutasson a napjaink adatgyűjtési módszereire és a rendelkezésre álló adat felhasználási módjaira, ezzel megindokolva a szükségességét a különböző adatbiztonsági és adatvédelmi szabályozásoknak.

Az adat fogalmával párhuzamosan szokás emlegetni az információt is. Gyakran keverik a kettőt, így első sorban ezeket szeretném tisztázni. Az adat alatt valamilyen tényeket vagy megfigyeléseket értünk, amiket később analizálunk, feldolgozunk. Ilyen például minden amit látunk, érzünk. Az információ pedig olyan adat, amihez valamilyen jelentést társítunk, tehát az adat egy feldolgozás utáni állapotában beszélhetünk információról. Például, ha kinézünk az ablakon és látjuk, hogy esik az eső, de csak tudomásul vesszük és nem foglalkozunk vele, akkor az adat számunkra, de ha épp készülünk valahova, akkor rögtön információvá alakítjuk, hogy vegyünk magunkhoz esernyőt.

Adatvédelem alatt az adatgyűjtés és az adat felhasználásának korlátozásával, ezen folyamatok által érintett személyek védelmével foglalkozó intézkedéseket értjük.

Az adatgyűjtés a mindennapjaink elkerülhetetlen részévé vált, jó néhány formában találkozhatunk vele, például anyakönyvi nyilvántartás, üzletek leltározása, űrlapok kitöltése során, illetve a leggyakoribb előfordulása a digitális lábnyom adatainak gyűjtése.

Digitális lábnyom alatt a felhasználók által internetezés közben létrehozott adatokat értjük. Ilyen a weboldalak látogatása, az ottani tevékenységek, regisztrációk, adatok feltöltése az internetre, e-mailek küldése stb. Manapság egyre inkább körülvesz minket a digitális technológia, így a digitális lábnyomunk is egyre nagyobb és szélesebb körű.

Az adatok közül kiemelkedő figyelmet kapnak a személyes adatok, azaz azon adatok, amelyek alapján beazonosítható a felhasználó, mint természetes személy. Ide tartozik a név, lakcím, e-mail cím, IP-cím stb. Ezen adatok védelme azért kiemelkedően fontos,

mert ezeket felhasználva képet lehet alkotni adott személyről, amivel könnyen vissza lehet élni.

A begyűjtött adatoknak számos felhasználási módja van, rendkívül népszerű a személyreszabott szolgáltatások létrehozása, kimutatások készítése és magától értetődő az személyazonosítás folyamata stb.

A gyűjthető adatok sokszínűsége és a mai világban az adatgyűjtés nagymértékű leegyszerűsödése indokolja az adatgyűjtés korlátozását, azonban a feldolgozás és felhasználás céljának korlátozása is jelentős feladat. Utóbbiak megszorítása nélkül megkötések nélkül folyhatna kereskedelem személyek adataival (anyagi helyzet, betegségek). Egy ide illő visszaélés a politikai eredetű Cambridge Analytica-hoz köthető manipulációs folyamat, amely során Facebook-ról felhasználók millióinak nyerték ki adatait és használták fel a 2016-os amerikai választás során [1].

Ezen felül számtalan ismert eset van hasonló visszaélésekről, azonban nem csupán az adat etikátlan felhasználásának megakadályozása fontos cél, hanem az adat biztonságának garantálása is, hiszen az adatokhoz való illetéktelen hozzáférés, adatszivárgás, adatvesztés mind hatalmas károkat okozhatnak. Az ezzel foglalkozó terület az adatbiztonság, ami egy inkább technikai, műszaki terület.

3. A jogi szabályozás koncepciója

Ebben a fejezetben a jogi szabályozás komponenseit mutatom be, középpontba helyezve hazánk jogszabályainak felépítését. Tárgyalásra kerül Magyarország jogszabályainak hierarchiája, illetve mivel EU-s tagállamban élünk, fontos szerepet játszanak az EK-ban történő jogalkotások is, így arról is szó fog esni. Természetesen ezen két jogrendszer szabályai egymással szoros viszonyt kell ápoljanak, összeegyeztethetővé kell válniuk, ennek folyamatát mutatja be a 3.4 alfejezet.

3.1. Jogszabályok hierarchiája

Magyarországon a jogszabályok hierarchiájának a csúcsán az Alaptörvény áll, amely tartalmazza a magyar állam struktúrájának és működésének alapvető szabályait, továbbá az állampolgárok elemi jogait és kötelezettségeit. Minden jogszabályt úgy kell meghozni, hogy ezzel összhangban legyen. Jelenleg, 2012 január 1-e óta az Országgyűlés által 2011 április 18-án elfogadott Alaptörvény van életben, amely azóta több módosításon is átesett (eddig nyolcon). Az Alkotmány módosításához az országgyűlési képviselők kétharmadának igen szavazata szükséges, amely kétféleképpen is értelmezhető, így megkülönböztetjük az *erős* és *gyenge* kétharmados törvényeket. Az *erős* esetén az összes országgyűlési képviselő kétharmadának érvényes igen szavazata szükséges az elfogadáshoz, míg a *gyenge* esetén a határozatképes Országgyűlés jelen lévő képviselői kétharmadának érvényes igen szavazata is elegendő.

A jogalkotó szerveket és az általuk kibocsátható jogforrásokat az Alaptörvény T) cikke sorolja fel. Eszerint, a hierarchiában a következő szinten a törvények állnak. Egy kiemelkedő típusa a törvényeknek a sarkalatos törvények, amelyek az Alaptörvényben le-

írt tárgykörök kizárólagos szabályozói. Ezeket csak a jelen lévő országgyűlési képviselők kétharmados többségével lehet elfogadni és módosítani.

A törvényeket követően a hierarchiában különböző rendeletek szerepelnek, mint jogszabályok. Ezek csökkenő irányban a következők: kormányrendeletek, miniszteri rendeletek, a Magyar Nemzeti Bank elnökének rendeletei, önálló szabályozó szerv vezetőjének rendeletei, önkormányzati rendeletek és a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kiadott rendeletei. A jogszabályokat az önkormányzati rendelet kivételével a Magyar Közlönyben kell kihirdetni. A jogalkotásról a jelenleg érvényben levő 2010. évi CXXX. törvény és az annak a módosításáról szóló 2019. évi II. törvény szól. [2, 3, 4, 5]

3.2. Jogalkotás az Európai Közösségben

Az Európai Unió joga több forrásból merít, ezeket fogom alább ismertetni. [6]

Elsődlegesen a szerződésekből, mint a Római Szerződések, vagy a Lisszaboni Szerződés. "A szerződés az uniós tagállamok között létrejött, kötelező erejű megállapodás, amely meghatározza az uniós célkitűzéseket, az uniós intézményekre vonatkozó szabályokat, a döntéshozatal módját és az EU és a tagállamai közötti viszonyt. A szerződések módosítására az EU hatékonyságának és átláthatóságának javítása, az új tagállamok csatlakozására való felkészülés, valamint új együttműködési területek (egységes valuta) bevezetése érdekében kerül sor." [7]

A szerződésekkel már egyenrangúvá vált az Európai Unió Alapjogi Chartája, amely "Belefoglalja az EU jogába az uniós polgárok, illetve az EU területén tartózkodó személyek számos személyes, állampolgári, politikai, gazdasági és társadalmi jogát." "Azáltal, hogy világosabbá teszi az alapjogokat és felhívja rájuk a figyelmet, a charta jogbiztonságot teremt az EU-ban." [8]

A szerződéseket követik az Unió által kötött nemzetközi megállapodások. Ezek a nemzetközi közjog szerinti egyezmények, és a szerződő felek számára jogokat és kötelezettségeket hoznak létre, amelyeket az EU egészében alkalmazni kell. [9]

Az egyel lentebbi szinten a másodlagos jog van. Ezen joganyagok akkor tekinthetők érvényesnek, ha összhangban vannak a hierarchiában felette szereplő jogszabályokkal. "Másodlagos vagy származtatott jogforrásnak az Európai Unió intézményei által alkotott joganyagot nevezzük. E jogforrások az alapszerződéseken alapulnak, kizárólag az alapszerződésekben meghatározott szervek által és csak az ott meghatározott eljárás keretei között, megfelelő felhatalmazás alapján kerülhetnek kibocsátásra." "A másodlagos jogforrások közül a rendelet, az irányelv és a határozat kötelező erejű, az ajánlás és vélemény pedig nem bír kötelező erővel." [10]

A jogalkotásban részt vesz az Európai Parlament, az Európai Unió Tanácsa, az Európai Bizottság, az Európai Gazdasági és Szociális Bizottság, és a Régiók Európai Bizottsága.

3.3. Európai uniós irányelvek

Az Európai Unió másodlagos jogforrásainak részét képezik az Európai uniós irányelvek. Az EU működéséről szóló szerződés 288. cikke megállapítja, hogy az irányelv az elérendő

célokat tekintve kötelező a címzett tagállamok számára, a célkitűzések megvalósításának formáját és eszközeit azonban a tagállamok választhatják meg.

Az irányelv eltér a rendelettől és a határozattól. A rendelet a tagországok belső jogrendszerében közvetlenül, a hatálybalépést követően azonnali alkalmazandó, az irányelv pedig nem közvetlenül alkalmazandó. A nemzeti jogalkotó szerv(ek)nek átültető jogszabályt kell elfogadnia, amellyel a nemzeti jogszabályokat az irányelvekben szereplő célkitűzéseknek megfelelően alakítja. Az adott nemzet polgáraira az irányelvben szereplő jogok és kötelezettségek az átültető jogszabály elfogadását követően vonatkoznak. Az irányelv átültetési folyamata megenged bizonyos mérlegelési jogkört, hogy a nemzetek sajátosságait figyelembevéve történjen meg a procedúra. A határozattól az különbözteti meg az irányelvet, hogy míg a határozat egy szűkebb/konkrétabb körre vonatkozik (néhány országra, vállalkozásokra), addig az irányelv egy általános dokumentum, amelyet egy tágabb körnek kell figyelembe venni és alkalmazni (általában minden uniós országnak).

"Az átültetésnek az irányelv elfogadásakor meghatározott határidőig (általában két éven belül) kell megtörténnie. Amennyiben valamely ország elmulasztja egy irányelv átültetését, a Bizottság kötelezettségszegési eljárást kezdeményezhet és eljárást indíthat az adott ország ellen az EU Bírósága előtt." [11] [6]

3.4. Jogharmonizáció Magyarországon

"A jogharmonizáció azt a jogalkotási folyamatot jelenti, amely lehetővé teszi, hogy két jogrendszer szabályai egymással összeegyeztethetővé váljanak." [12] Erre példa az uniós jogharmonizáció, ami az uniós jogszabályok összeegyeztetését jelenti a tagállamok saját jogrendszerével. Tehát a jogharmonizáció feladata a jogi rendszerek közti ellentmondások elkerülése. Tehát, míg az uniós jogot különböző uniós intézmények alkotják, addig a nemzeti jogrendszert a nemzeti szervek formálják. A jogbiztonság érdekében a két rendszer között összhangot kell teremteni, úgy hogy az uniós jog beépüljön az tagállamok jogrendszereibe. Ennek a folyamatnak a neve jogharmonizáció.

A jogharmonizáció vonatkozik az unió elsődleges jogforrásaira és másodlagos jogforrásaira is egyaránt. Azonban elsődleges jogforrások és a rendeletek egységesen alkalmazandók az uniós tagállamokban, így a nemzeti jogba nem kell átültetni, de ha vannak az ezekben szereplőkkel ellentétes nemzeti szabályozások, úgy azokat meg kell szüntetni. A leggyakoribb feladat azonban az uniós irányelvek átültetése a nemzeti jogrendbe. Az előzőekkel ellentétben egy nagyobb szabadságot engedélyező folyamatról beszélünk, mert az irányelvek tartalmazhatnak minimumszabályozást, amely az uniósnál szigorúbb rendelkezéseket engedélyes, illetve maximumszabályozást is, ami viszont tiltja a szigorúbb szabályozást.

A jogharmonizáció egy kötelező folyamat, amelyet a Lisszaboni Szerződés tartalmaz és minden tagállamra vonatkozik. Magyarországon a jogharmonizációért a Kormány a felelős. A jogharmonizációs folyamatban több fontos szereplő és részt vesz. A jogharmonizációs jogszabály-tervezetek elkészítésében az Unió döntéshozatali eljárásban és a Kormány álláspontjának kialakításában részt vevő minisztérium vagy állami szerv a felelős. A feladatok összehangolását és koordinációjáért az igazságügyért felelős miniszter végzi. Ezen felül az ő feladata a jogharmonizációs folyamat teljesítésének figyelemmel kísérése. A teljesítést követően a Külügyminisztérium feladata, hogy jelentse az Európai

Bizottság felé. Az Országgyűlés is szerepet kap a jogharmonizációs folyamatban, ha törvényhozási tárgykörbe esik. "Ezeket az ügyköröket nemzeti jogszabályok tartalmazzák: Magyarország Alaptörvénye és a jogalkotásról szóló 2010. évi CXXX. törvény." [12]

4. Nemzetközi szabályozás

Miután az adatgyűjtés és feldolgozás mérföldköveivel megindokoltuk az adatbiztonsági és adatvédelmi szabályozások fontosságát, majd a jogrendszerek alapvető felépítését és működését is áttekintettük, rátérnék a témánk középpontjában helyezkedő fontos szabályozásokra, irányelvekre. Kezdetnek a Gazdasági Együttműködési és Fejlesztési Szervezetet (OECD) mutatom be és az általuk megfogalmazott irányelveket a magánélet védelméről és a személyes adatok határokon átívelő áramlását. Ezt követően az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA), feladatkörét és ajánlásait tárgyalom. Végül két jelentős EU-s rendeletet fogok részletezni. Egyik az általános adatvédelmi rendelet (GDPR), amely megjelenésekor (2016-ban) és az azt követő pár évben is hatalmas médiafigyelmet kapott. Másik az elektronikus azonosítási és bizalmi szolgáltatásokról szóló rendelet (eIDAS).

4.1. A Gazdasági Együttműködési és Fejlesztési Szervezet és irányelvei

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) egy nemzetközi gazdasági szervezet. A szervezet célja, hogy olyan irányelveket hozzon létre, amelyek jólétet, egyenlőséget és lehetőségeket teremtenek az embereknek és az országok gazdaságának.

A témánkkal kapcsolatos fontos munkája a szervezetnek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szólói irányelvei. Egészen korán, már 1980-ban elhatározta a szervezet, hogy kiadja nemzetközi irányelveit az előbbi témákról. Az irányelvek ajánlásként jelentette meg a szervezet, olyan módon, hogy a megfogalmazása generikus legyen, figyelembe véve a technológiák gyors fejlődését és változását ezáltal az irányelvek hozzáigazíthatók legyenek. Ennek következtében az elvek az egyénekről szóló adatok számítógépes feldolgozásának minden médiumát, a személyes adatfeldolgozás minden típusát, valamint minden adatkategóriát felölelnek.

Az ajánlás öt fő részre van bontva. Az első az általános definíciókat tartalmazza, amelyeket a későbbiekben az alapelvek megfogalmazásakor használnak fel, ezen felül az irányelvek hatályáról ad leírást. Kiemelném a **személyes adatok** definícióját, hiszen ez az adattípus szerepel az irányelvek központjában. "Személyes adatok jelentése bármilyen információ, ami egy azonosított vagy azonosítható személyre (adatalanyra) vonatkozik" [13]. A második és harmadik rész különböző alapelveket fogalmaz meg, a második esetében a nemzeti alkalmazásra koncentrálva, míg a harmadik részben a nemzetközi alkalmazásra. A nemzeti alkalmazás alapelvei közt szerepel két korlátozó elv, név szerint a **korlátozott adatgyűjtés alapelv** és a **felhasználási korlátozás alapelv**, amelyek célja a személyes adatok gyűjtésének és felhasználásának tisztességes módjának garantálása. Az adatgyűjtés, felhasználás és egyéb folyamatok átláthatóságát és egyértelműségét

segítik a **szándékmegjelölés alapelv** és a **nyitottság alapelv**. A személyeknek jogokat is biztosít az **egyéni részvétel alapelvével**, többek között az adott személyre vonatkozó adatok betekintési jogát és ezen adatok szerkesztésének jogát. Fontos, hogy a begyűjtött adatoknak a biztonsága, amit a **biztonsági garancia alapelv** követel meg. Ezen felül a begyűjtött adatok minőségét és aktualitását is szem előtt kell tartani, amelyet az **adatminőség alapelv**-ben fogalmaztak meg. Legvégül pedig az előző alapelvek betartása érdekében a **felelősségre vonhatóság alapelv** mondja ki, hogy "az adatellenőrző legyen felelősségre vonható, hogy azon intézkedések szerint jár-e el, melyek a fenti alapelveknek érvényt szereznek." [13] A harmadik részben az ajánlás alapelveket ad a nemzetközi alkalmazásokra vonatkozóan, kifejtve az adat szabad áramlását és a törvényes megszorításokat. Lényegében a tagországok hatékony és biztonságos együtt és közös működését szorgalmazza, hogy az adat minden kezelési folyamata a lehető legkevesebb problémával menjen végbe. Végül a negyedik és ötödik rész javaslatokat tartalmaz az alapelvek implementálására, hogy miket érdemes szem előtt tartani.

4.2. Európai Uniós Hálózat- és Információbiztonsági Ügynöksége

Az ENISA-t azzal a céllal hozták létre 2004-ben, hogy segítse a magas szintű kiberbiztonság elérését az EU-ban, így feladatuk betölteni a hálózat- és információbiztonság európai szakértői központjának szerepét. "Az ENISA segít az EU-nak és az EU tagországainak abban, hogy jobban fel legyenek készülve az információbiztonsági kihívások felderítésére és kezelésére, illetve megelőzésére." [14]

Ezt több módon is próbálják elérni. Egy gyakorlatiasabb megközelítést jelent a gyakorlati tanácsok és megoldások szolgáltatása az EU-tagállamok köz- és magánszektorbeli szereplőinek és az uniós intézményeknek. Ezek alatt kiberbiztonsági gyakorlatok szervezését, segítség nyújtást a tagállamok nemzeti kiberbiztonsági stratégiájuk kifejlesztésében és a témába vágó csoportok/egységekkel való együttműködést érthetjük. Továbbá elméletibb/tudományosabb irányból is segítséget nyújt azzal, hogy jelentéseket és tanulmányokat, illetve útmutatókat tesz közzé a kiberbiztonság számos területén. Az ENISA ezen felül segít a témába vágó uniós szakpolitikák és jogszabályok szövegezésében, mint szakértői tanácsadó szerv.

Az ENISA-nak központi szerepe volt a NIS direktíva bevezetésében is, amelynek célja a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintre emelése volt. [15]

Tekintve, hogy az információs technológiák egyre jelentősebb és gyorsabb fejlődésen esnek át, az Európai Bizottság javaslatára az Európai Parlament és a Tanács (EU) 2019/881 rendelete [16] hivatott leváltani a korábbi 526/2013/EU rendeletet és megfogalmazni az ENISA felépítését és célját.

Az ENISA struktúrája a következőképpen épül fel: Az ügynökség élén az igazgatóság áll. Feladatuk biztosítani, hogy az ügynökség olyan feltételekkel teljesítse feladatait, amelyek megfelelnek az alapító rendeletnek. Az igazgatóság munkáját a végrehajtó testület segíti az elfogadandó határozatok előkészítésével. A napi szintű igazgatás feladata az ügyvezető igazgató feladata. 2019 óta az ENISA részét képviseli a nemzeti összekötő

tisztviselők hálózata is, ami feladata az információátvitel segítése az ENISA és az EU tagállamok között. Továbbá a struktúra részét képezi egy tanácsadói csoport is, akik feladata a releváns problémákra való figyelemfelhívás és a célok elérésének segítése. Ezen felül ad hoc munkacsoportok tartoznak az ENISA felépítésébe, akik feladata a kitűzött célok elérése.

A 2019/881 rendelet egy fő célja az európai kiberbiztonsági tanúsítási rendszer létrehozása és fenntartása "annak érdekében, hogy átláthatóbb legyen az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kiberbiztonsági megbízhatósága, megerősítve ezzel a digitális belső piacba és annak versenyképességébe vetett bizalmat." [16] Az ENISA-nak többek között ehhez is hozzá kell járulnia és ez is mutatja, hogy mennyire jelentős szerepe van az ügynökségnek az unió működésében.

Összegezve, az ENISA feladata, hogy gyakorlati oktatással, tanácsokkal és irányelvek megfogalmazásával, tanulmányok készítésével segítsék az európai unió tagállamait, állami és magánszektorait és az unió polgárait a megfelelő online biztonság elérésére. Az emberek folyamatosan fokozzák online jelenlétüket, amely a COVID-19 járvány miatt még nagyobb tempóban növekszik, mint valaha, amit a kiberbűnözők is kihasználnak, különös tekintettel az e-kereskedelemre és az e-fizetési vállalkozásokra, valamint az egészségügyi rendszerre. Így az ENISA munkája nélkülözhetetlennek mondható. [17, 14]

4.3. Az általános adatvédelmi rendelet

A röviden GDPR-ként ismert általános adatvédelmi rendeletet az Európia Parlament és a Tanács (EU) 2016/679 rendelete fogalmazza meg. Célja, hogy támogassa az Európai Unió egyik alapelvét, miszerint mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. A 2009-2010-es években akkora változás indult meg az adatok gyűjtésében és azok felhasználásában, amely miatt felismerték, hogy az eddigi témába vágó rendelet már nem váltja be a hozzá fűzött reményeket. Ennek következtében 2012-ben elindult a jogalkotási eljárás, melynek lezárulásával született meg és fogadta el az Európai Parlament és a Tanács a GFPR-t, amit 2018 május 25-ig harmonizálnia kellett az EU tagállamoknak.

A GDPR minden olyan vállalkozásra vonatkozik, ami az EU területén működik, illetve az EU-n kívül működő cégekre is, ha azok árut értékesítenek vagy szolgáltatást nyújtanak az EU-n belül. Mivel a GDPR a személyes adatokra vonatkozik, így ha egy vállalkozás személyes adatot nem kezel, arra nem vonatkozik. Személyes adatnak azon adatok minősülnek, amelyekkel közvetlenül vagy közvetve beazonosítható egy természetes személy. Pár egyértelmű példa a név, lakcím, telefonszám, email cím, de vannak kevésbé nyilvánvaló példák is, mint a marketing célú cookie-k, melyek a számítógépünkre lementésre kerülnek, amelyek szintén a személyes adat kategóriájába tartoznak. A hivatalos megfogalmazás a következő: "azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható." [18] Az adatkezelés alatt pedig minden olyan műveletet értünk amit a személyes adatokon végezni lehet.

A GDPR hét alapelvben foglalja össze, hogy miknek kell teljesülni a személyes adatok

kezelésekor. Ezen alapelvek és az 4.1 fejezetben tárgyalt alapelvek között szép párhuzam látható, természetesen nem teljes az egyezés, de egyértelmű a hasonlóság. A GDPR alapelvei is a tisztességes és átlátható és jogszerű adatgyűjtést és felhasználást szorgalmazzák, amiknek alappillérei a **jogszerűség, tisztességes eljárás és átláthatóság**, **célhoz kötöttség** alapelvei. Két fontos korlátozó alapelv az **adattakarékosság** és a **korlátozott tárolhatóság** alapelvei, amik az adatgyűjtés minimalizálását követelik mind mennyiségben, mind azok tárolásának idejében. Az adatok aktualitása is fontos szerepet kap a GDPR-ban, mint az OECD alapelveinél tárgyalt javaslat is tette. Ezt írja le a **pontosság** alapelve, amely, ha egy adat pontatlan a cél szempontjából, annak törlését vagy helyesbítését igényli. Természetesen elengedhetetlen a személyes adatok tárolásának biztonságossága, mind külső, mind belső veszélyek ellen. Erről szól az **integritás és bizalmas jelleg** alapelve. Legvégül, ezen alapelvek esetén is, hogy a betartásuk garantálva legyen, az **elszámoltathatóság** alapelv kimondja, hogy "az adatkezelő felelős az előbbieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására". [18] Ha ezen alapelvek nem kerülnek betartásra, az komoly szankciókat vonzhat magával.

Az adatkezelők által betartandó eddigi kötelezettségeken felül a GDPR az érintett személyeknek jogokat is biztosít, amelyek teljesítése adatkezelők számára további kötelezettséget jelentenek. Ezek az érintettek teljes körű átlátható tájékoztatását kötelezik. A teljes körűségbe bele tartozik többek között az adatkezelő kiléte, elérhetősége és az adatgyűjtés, tárolás és felhasználás pontos leírása, biztosítva a totális átláthatóságot. Ezen felül az érintett személynek hozzáférést kell biztosítani a róla tárolt személyes adatokhoz és annak szerkesztésére is lehetőséget kell adni. Ezeken felül az érintettnek jogában áll tiltakoznia az adatkezelés ellen vagy korlátozni azt, illetve fontos az **adathordozhatósághoz való jog**, amelynek lehetővé tételéhez az adatkezelőket interoperábilis formátumok kifejlesztésére ösztönzik, ezzel támogatva az adat géppel olvasható formátumát és egyszerű továbbítását/rendelkezésre bocsájtását. A jogokhoz tartozik továbbá az automatizált döntéshozatal elutasítása az érintett részéről.

Az általános adatvédelmi rendelet tehát az érintettek teljeskörű tájékoztatását célozza meg, valamint befolyást próbál adni az érintettek kezébe a személyes adatuk fölött. Megvannak az előnyei és a hátrányai is. 2019-ben lehetőségem volt élőben meghallgatni egy interjút [19] Edward Snowdennel, aki híresen kémkedés ellenes és az emberek személyes adatainak teljeskörű védelméért küzd. Az interjúban többek között a GDPR is szóba került, amit egy jó első erőfeszítésnek nevezett. Rámutatott, hogy az adatvédelem szabályozása azt feltételezheti, hogy az adatgyűjtés helyénvaló és nem jelenthet veszélyt, ami mindenképp egy elgondolkodtató észrevétel, hiszen a GDPR az adatgyűjtés mértékére csupán azt mondja ki, hogy a céloknak megfelelő minimum adat kerüljön begyűjtésre, azonban az adatkezelés célja nem korlátozott.

4.4. Az elektronikus azonosítási és bizalmi szolgáltatásokról szóló rendelet

Mielőtt a rendelet céljára térnénk ki, tekintsük át mi is az elektronikus azonosítás és mik a bizalmi szolgáltatások. Az elektronikus azonosítás hivatalos definíciója a következő: "a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt

egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata". [20] Egy már elterjedt példa erre a folyamatra az Ügyfélkapura való bejelentkezés, amely elektronikusan azonosítja a személyeket, akik ez által elektronikusan képesek ügyintézést végezni. A másik fontos fogalom a bizalmi szolgáltatások, amelyek olyan elektronikus szolgáltatások, amelyek digitális dokumentumok, webhelyek hitelességét garantálják.

A fejezet témáját adó rendelet (910/2014/EU eIDAS rendelet) szükségességét ismét a gyors digitális technológiai fejlődés eredményezte, ugyanis elődje, az 1999/93/EK, amely egy az elektronikus aláírásokra vonatkozó irányelv volt, már nem tudott lépést tartani, mert "nem hozott létre átfogó határokon átnyúló és ágazatközi uniós keretet az elektronikus tranzakciók biztonságának, megbízhatóságának és könnyű használhatóságának érdekében". Így egy aktualizált, megerősített rendelet létrehozásának feltételével született az eIDAS.

Az eIDAS célja, hogy a tagállamok elektronikus azonosítási eszközeinek olyan feltételeket szabjon, amelyet követve minden tagállamban elismert azonosítási eszközzé váljon az, valamint, hogy a bizalmi szolgáltatásokra szükséges szabályokat és jogi keretet nyújtson.

A rendelet az elektronikus azonosítás terén elrendeli a kölcsönös elismerés elvét, miszerint, ha egy közigazgatási szerv elektronikus azonosítást használ és azt megfelelően bejelentette, akkor azt minden tagállamban el kell ismerni. Ez az elv kulcsszerepet játszik abban, hogy külföldi egészségügyi kezelés esetén a szolgáltatások egyszerűen elérhetővé váljanak a betegek számára az elektronikus azonosításnak köszönhetően. Ezen felül az egészségügyi adatoknak is hozzáférhetőnek kell lennie a külföldi kezelő intézet számára, amihez a biztonságos és megbízható keret elengedhetetlen. Természetesen ezen felül egyéb közszolgáltatások igénybevétele esetén is garantálja a hitelesítés lehetőségét.

A rendelet a bizalmi szolgáltatásoknak olyan jogi keretet ad, amely figyelembe veszi a technológia gyors fejlődését, így ezen szempontból semlegesen épül fel. Megköveteli ezen szolgáltatások nemzetközi elismerését is, hogy ez által felhasználhatók legyenek a teljes belső piaci területen. Ezen felül a rendelet számos szabályozást ír elő a bizalmi szolgáltatókra nézve, illetve felügyeleti szervezetek működtetését szabja ki, akiknek erősen együtt kell működni a szolgáltatókkal, illetve felügyelni őket, ezzel garantálva a szolgáltatás minőségét és biztonságosságát. Ha a szolgáltatók nem tartják be az előírt szabályokat, úgy felelősségre vonhatók. A rendelet a bizalmi szolgáltatók egy kiemelt körét is definiálja, amelyeket minősített bizalmi szolgáltatóknak nevez, amelyek magas szintű biztonságot garantálnak. Annak érdekében, hogy egy bizalmi szolgáltató minősítetté válhasson, egy megfelelőségértékelő szervezetet meg kell bíznia, hogy értékelje ki a szolgáltatást, amelyet benyújtva a felügyeleti szerv részére megkaphatja a minősítést. A technikai jellegű szabályozások esetén a rendelet igyekszik a nemzetközileg elismert szabványok követését szorgalmazni, hiszen a szabványok alaposan bevizsgált dokumentumok, amelyeket szakértő szervek hoznak létre.

Összesítve, a rendelet legfőbb célja, hogy felszámolja a tagállamok digitális piacának szétaprózódottságát és egy kurrens, biztonságos egységet hozzon létre. [20]

5. Hazai szabályozások

5.1. Alaptörvény a személyes adatról

Magyarország Alaptörvénye, mint korábban kifejtettem a magyarországi jogszabályok hierarchiájának legtetején áll. A személyes adatok védelmével kapcsolatos szabályok az Alaptörvény hetedik módosítása során 2018-ban kerültek hatály alá. A VI. cikkben szereplők kimondják, hogy mindenkinek joga van személyes adatai védelméhez és ezen jog érvényesülésének garantálása érdekében szó esik arról, hogy sarkalatos törvénnyel alátámasztva szükséges létrehozni egy független ellenőrző hatóságot. [3]

Ezen törvény a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) [21]. A törvény 2012-ben került hatály alá, azonban azóta számos módosításon esett át, többek között azért, hogy a GDPR-ban leírtakkal is teljes harmonizációba kerüljön. Az Infotv. a GDPR-hoz hasonlóan tartalmaz számos alapelvet, követelményt és jogokat ad az érintetteknek a személyes adatuk védelméhez, amik a 2. és 3. fejezet részei.

Ezen felül az Infotv. a közérdekű adatok és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokról is szól. Közérdekű adat: "az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret" [21]. A közérdekből nyilvános adat pedig "a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli" [21]. Az efféle adatokat mindenkinek joga van megismerni, ha arról törvény másképp nem rendelkezik, például minősített adatokról van szó. A közfeladatot ellátó szerv feladatai közé tartozik, hogy elősegítse és biztosítsa a közvélemény pontos és gyors tájékoztatását, valamint a közérdekű adatokat tegye internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozás- és díjmentesen.

Továbbá ezen dokumentum tartalmazza a korábban említett független ellenőrző hatóság, név szerint a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) felépítésének, jogállásának, költségvetésének és eljárásainak leírását.

A veszélyhelyzetben, hogy azonban az Infotv-re módosítások léptek életbe, ezek hatálya átmeneti. [22] A jelenleg hatályban levő 521/2020. (XI. 25.) Korm. rendelet többek között a személyes kontaktus elkerülése, valamint a határidők hosszabbítása érdekében született.

Az általános törvények azonban nem képesek lefedni mindent a megfelelő mértékben, ezért is vannak magyarországon a különböző közigazgatási ágazatok szabályozására vonatkozó törvények, mint ágazati szabályozási vezérvonalak, hiszen több száz ágazat létezik és ezek jelentősen eltérőek egymástól. (Példák ágazatokra: egészségügy, elektronikus média stb.) Ezen ágazati törvények is foglalkoznak (az ágazatra vonatkozó) adatvédelemmel. Ezen törvények GDPR-nak megfelelő módosításait tartalmazza a 2019. évi XXXIV. törvény [23].

5.2. Irányelvek az állami és önkormányzati szervek és nemzeti adatvagyon védelméről

A nemzeti adatvagyon védelme

A nemzeti adatvagyon alatt "a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összességét" [24] értjük. A 2010. évi CLVII. törvény célja, hogy a nemzeti adatvagyon védelme érdekében gondoskodjon annak biztonságáról. Ennek érdekében a törvény kimondja, hogy "a nemzeti adatvagyon részét képező adatállomány tekintetében törvény az adatfeldolgozással megbízható személyek és szervezetek körét korlátozhatja, vagy az adatfeldolgozásnak az adatkezelőtől különböző személy vagy szervezet általi ellátását kizárhatja" [24]. Ezáltal leszűkítve az adathoz hozzáférő elemeket és kizárva potenciális veszélyforrásokat.

A kormány létrehozott egy mellékletet, amely egy táblázatba foglalva meghatározza a nemzeti adatvagyon körébe tartozó állami nyilvántartásokat, azok feldolgozóit, az adatfeldolgozás körét és az adatfeldolgozó igénybevételének jellegét. [25]

A közelmúltban (2020. október) megalakult a Nemzeti Adatvagyon Ügynökség. "Az adatokra azonban nem csak mint védendő információra, hanem mint forgalomképes vagyonelemre is kell tekinteni. Ehhez egy új adatvagyon fogalom megalkotására is szükség van, amelynek rendszerét a Neumann Nonprofit Kft. részeként létrehozott Nemzeti Adatvagyon Ügynökség dolgozza ki."[1] Tehát a közeljövőben ezen a téren további átalakulásokra számíthatunk.

Az állami és önkormányzati szervek információbiztonsága

Napjainkban a digitális technológia gyors ütemű fejlődése és az így keletkező fenyegetések miatt kiemelten fontos törődni az elektronikus adatok és az ezeket kezelő rendszerek biztonságával. Az Országgyűlés az "információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme" [26] érdekében hozta a 2013. évi L. törvényt az állami és önkormányzati szervek elektronikus információbiztonságáról.

A védelemnek a kockázatokkal arányosnak és teljes körűnek kell lennie, ezért a törvény a hatálya alá tartozó elektronikus információs rendszerek 1-től 5-ig számozott biztonsági osztályba való besorolását rendeli el, ahol a számozás emelkedésével párhuzamosan szigorodó védelmi előírásoknak kell eleget tenni. A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és őt terheli a felelősség is. A szervezet vezetője magasabb osztályt is meghatározhat, illetve hatósági engedéllyel és megfelelő indoklással alacsonyabb biztonsági szintet is. A biztonsági osztályba sorolás felülvizsgálatát legalább háromévente vagy szükség esetén soron kívül el kell végezni, arról dokumentációt készíteni. Ha a rendszerben valamilyen változás történik, vagy új elektronikus információs rendszer kerül

[1] Nyilatkozta Gál András Levente, a Nemzeti Adatvagyon Ügynökség vezetője.

bevezetésre, vagy a feldolgozott adatok vonatkozásában történik változás, akkor soron kívüli felülvizsgálatot kell tenni. Az elektronikus információs rendszerek teljes életciklusára kiható követelményeket ír elő a törvény, miszerint "meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét." [26] Ennek érdekében pedig kötelező védelmi intézkedéseket kidolgozni mind logikai, fizikai és adminisztratív szinteken, oly módon, hogy azok támogassák "a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, a biztonsági események kezelését" [26].

A Kormány hatóságot jelöl ki a törvény hatálya alá tartozó elektronikus információs rendszerek biztonsági felügyeletére, aminek feladata többek között biztonsági szint megállapításának ellenőrzése, a követelmények teljesülésének ellenőrzése. Ezen felül a hiányosságok elhárításának elrendelése, javaslattétel és együttműködés és kapcsolattartás az elektronikus ügyintézési felügyelettel és a nemzetbiztonsági szolgálatokkal. "Ha az elektronikus információs rendszert olyan súlyos biztonsági esemény éri vagy annak közvetlen bekövetkezése fenyegeti, amely a rendszert működtető szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár, az eseménykezelő központ a védelmi feladatainak ellátása érdekében kötelezheti a szervezetet, hogy a súlyos biztonsági esemény megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg" [26]. A törvény megengedi bizonyos esetekben információbiztonsági felügyelő kirendelését a hatóságok számára, ha a szervezet nem teljesít szabályokat. Az információbiztonsági felügyelő pedig "a fenyegetés elhárításához szükséges védelmi intézkedések eredményes megtétele érdekében a Kormány által rendeletben meghatározott intézkedéseket, eljárásokat javasolhat, a szervezet intézkedései tekintetében kifogással élhet" [26].

A Kormány számítógépes eseménykezelő központok megalakulását is támogatta. A számítógépes eseménykezelő központ "az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik" [26].

A kormányzati koordináció biztosításáért a Nemzeti Kiberbiztonsági Koordinációs Tanács felelős. "A Kormány javaslattevő, véleményező szerveként gondoskodik a meghatározott szervezetek e törvényben és végrehajtási rendeleteiben meghatározott tevékenységeinek összehangolásáról" [26].

5.3. Szankcionálás Magyarországon

Magyarországon a 2012. évi C. törvény a Büntető Törvénykönyvről (BTK) [27] foglalja össze törvény formájában a büntetendő cselekvések és a büntetések nagy részét, azonban nem feltétlenül terjed ki minden bűncselekményre, például a GDPR visszatartó erejű közigazgatási bírság kiszabását engedélyezi a rendeletet be nem tartóira (Magyarországon a NAIH által kiszabott bírság "százezertől húszmillió forintig terjedhet" [21]). "Bűncselekmény az a szándékosan vagy, (ha e törvény a gondatlan elkövetést is büntetni rendeli) gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre e törvény

büntetés kiszabását rendeli. Társadalomra veszélyes cselekmény az a tevékenység vagy mulasztás, amely mások személyét vagy jogait, illetve Magyarország Alaptörvény szerinti társadalmi, gazdasági, állami rendjét sérti vagy veszélyezteti" [27]. A törvény megkülönböztet két típusát a bűncselekménynek, egyik a bűntett, másik a vétség. "Bűntett az a szándékosan elkövetett bűncselekmény, amelyre e törvény kétévi szabadságvesztésnél súlyosabb büntetés kiszabását rendeli, minden más bűncselekmény vétség" [27].

A témánkkal kapcsolatos részét a BTK-nak XLIII. fejezete tartalmazza, melynek címe tiltott adatszerzés és az információs rendszer elleni bűncselekmények. Ez a fejezet három részre van bontva, első része a tiltott adatszerzésről, második része az információs rendszer vagy adat megsértéséről, harmadik része az információs rendszer védelmét biztosító technikai intézkedés kijátszásáról szól.

Tiltott adatszerzésnek a személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából elkövetett cselekvések minősülnek. Büntetendő a fizikai átkutatással járó és a technikai eszközökkel történő megfigyelés és adatrögzítés egyaránt. A büntetés mértéke függ az elkövetés módjától, de akár öt évnyi szabadságvesztéssel is járhat.

"Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. Aki az információs rendszer működését jogosulatlanul akadályozza vagy az abban levő adatot jogosulatlanul módosítja, három évig terjedő szabadságvesztéssel büntetendő" [27], illetve súlyosbító körülmények is vannak, így akár nyolc évig is terjedhet a szabadságvesztés mértéke.

Aki előbbi "bűncselekmények elkövetése céljából az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő" [27].

Utóbbi esetén nem büntethető az elkövető, "ha (mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó, vagy számítástechnikai program készítése a büntetőügyekben eljáró hatóság tudomására jutott volna) tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását" [27]. Minden más esetben azonban a BTK szabadságvesztéssel bünteti az elkövetőt.

Irodalomjegyzék

[1] Rosalie Chan. The cambridge analytica whistleblower explains how the firm used facebook data to sway elections, Oct 2019. URL: https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10.

[2] A jogszabályok hierarchiája, 2020. URL: https://hu.wikipedia.org/wiki/A_jogszab%C3%A1lyok_hierarchi%C3%A1ja.

[3] Magyarország alaptörvénye, 2011. URL: https://net.jogtar.hu/jogszabaly?docid=A1100425.ATV.

[4] 2010. évi cxxx. törvény, 2010. URL: https://net.jogtar.hu/jogszabaly?docid=a1000130.tv.

[5] 2019. évi ii. törvény, 2019. URL: https://mkogy.jogtar.hu/jogszabaly?docid=A1900002.TV.

[6] Udo Bux. Az európai uniós jog forrásai és hatályai, 2020. URL: https://www.europarl.europa.eu/ftu/pdf/hu/FTU_1.2.1.pdf.

[7] Eu-szerződések. URL: https://europa.eu/european-union/law/treaties_hu.

[8] Alapjogi charta, 2016. URL: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al33501.

[9] Nemzetközi megállapodások és az eu külügyi hatáskörei, 2020. URL: http://publications.europa.eu/resource/cellar/0bb808cd-f2cd-4df4-91cb-20419602eac3.0009.03/DOC_1.

[10] István Dr. Gárdos and Andrea Dr. Tömösvári. Az európai unió jogforrásai iii. a másodlagos jogforrások, 2004. URL: https://gmtlegal.hu/cikkek/az-europai-unio-jogforrasai-iii-a-masodlagos-jogforrasok.php.

[11] Európai uniós irányelvek, 2018. URL: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l14527.

[12] Jogharmonizáció magyarországon. URL: https://www.parlament.hu/biz39/eib/link1/jogharm.htm.

[13] Áttekintés: Oecd irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, 2003. URL: http://www.oecd.org/sti/ieconomy/15590228.pdf.

[14] Európai uniós kiberbiztonsági Ügynökség (enisa). URL: https://europa.eu/european-union/about-eu/agencies/enisa_hu.

[15] Az európai parlament és a tanács (eu) 2016/1148 irányelve, 2016. URL: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016L1148.

[16] Az európai parlament és a tanács (eu) 2019/881 rendelete, 2019. URL: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A32019R0881.

[17] Az enisa hivatalos honlapja. URL: https://www.enisa.europa.eu/.

[18] Az európai parlament és a tanács (eu) 2016/679 rendelete, 2016. URL: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679.

[19] Morality in the age of tech surveillance - edward snowden, 2019. URL: https://www.youtube.com/watch?v=X4_7A-SGLo8.

[20] Az európai parlament és a tanács 910/2014/eu rendelete, 2014. URL: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32014R0910#d1e752-73-1.

[21] 2011. évi cxii. törvény, 2020. URL: https://net.jogtar.hu/getpdf?docid=a1100112.tv.

[22] 521/2020. (xi. 25.) korm. rendelet, 2020. URL: https://net.jogtar.hu/jogszabaly?docid=A2000521.KOR&dbnum=1.

[23] 2019. évi xxxiv. törvény, 2019. URL: https://mkogy.jogtar.hu/jogszabaly?docid=A1900034.TV.

[24] 2010. évi clvii. törvény, 2010. URL: https://net.jogtar.hu/jogszabaly?docid=a1000157.tv#lbj6id3b95.

[25] 38/2011. (iii. 22.) korm. rendelet, 2011. URL: https://net.jogtar.hu/jogszabaly?docid=a1100038.kor.

[26] 2013. évi l. törvény, 2013. URL: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv.

[27] 2012. évi c. törvény, 2012. URL: https://net.jogtar.hu/jogszabaly?docid=a1200100.tv.