Az adatvédelem és adatbiztonság nemzetközi és hazai szabályozása

Vécsi Ádám
Debreceni Egyetem Informatikai Kar
Számítógéptudományi Tanszék

Tartalomjegyzék

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 adatgyűjtés és elemzés átalakulását bemutató rövid kitérő után az adatbiztonságra és adatvédelemre vonatkozó irányelveket és szabályozásokat fogom bemutatni, ami az utóbbi évtizedben számos változáson ment keresztül.

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

Szemléltetem az aktuális nemzetközi szabályozásokat, az Európai Uniós Hálózat- és Információbiztonsági Ügynöksége (ENISA) 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 büntetőtörvékönyv alapján a szankciónálásról is.

2. Az adatgyűjtés és feldolgozás evolúciója

Az adat számos szemszögből is változott az idő során, a legszembetűnőbb módosulás az adat mennyiségén, gyűjtésének módszerén, típusán és az elemzésén ment végbe. Napjainkban az adat minden emberre és minden iparágara jelentős hatással van. Ebben a fejezetben ezt az átalakulást fogjuk végigtekinteni, ezzel megindokolva a szükségességét a különböző adatbiztonsági és adatvédelmi szabályozásoknak [1, 2].

2.1. Az adat korai időszaka

Adatgyűjtésről már a történelem korai időszakában is beszélhetünk, amikor még csak rovásokkal ábrázoltak mennyiségeket. Ekkoriban csupán arra alkalmazták, hogy leltárat készíthessenek, kis mennyiségű adattal dolgoztak, kevés típussal. Később ez folyamatosan bővült és fejlődött, azonban az első érdekesnek tekinthető időszak az 1950-es évektől naggyából 2009 közé tehető.

Az '50-es években jöttek létre olyan eszközök, amelyek rendkívül leegyszerűsítették az adatgyűjtést és a különböző minták/trendek gyors felismerését. Ezt az időszakot *Analytics 1.0*-nak is szokták nevezni. Erre az időszakra az a jellemző, hogy kevés, struktúrált adatal dolgoztak. Az adat leginkább valamilyen belső forrásból származott (vásárlói adatok, eladási adatok, pénzügyi rekordok) és általában az adatgyűjtés több időt vett igénybe, mint az elemzői folyamatok. Erre az időszakra jellemző az adat tárház fogalma, a központi adattárak, amelyek végezték az adatgyűjtést és ezekhez társultak különböző "business intelligence" szoftverek, amelyek a jelentéseket készítették az adatról.

Ennek az időszaknak a vége 2009-re tehető, amikoris többek között a Facebook és a Google óriási népszerűség növekedésnek indult az internet és az internetképes eszközök

gyors terjedésének köszönhetően. Ekkortól kezdett megjelenni a "Big Data" fogalma és az adat hatalmas fordulatot vett.

2.2. A Big Data

Az internet és szociális média nagyvállalatok a 2000-es években egy teljesen új adattípust kezdtek gyűjteni és elemezni. Ezt az adattípust "big data-nak" nevezték el, találóan, hiszen valóban hatalmas adatmennyiségről van szó.

Az előző időszakban kevés, belső adatról volt szó, ebben az időszakban azonban egy teljes fordulatról beszélhetünk, hiszen az adat kívülről érkezik, az internetről, publikus adatforrásokból és sokkal nagyobb mennyiségben, struktúrált és struktúrálatlan formában. A szociális média, a mobil eszközök és lényegében az internet minden felhasználójáról begyűjtik a vállalatok az elérhető adatokat, amely lehet bármi (GPS adatok, böngészési adatok, a mobilkészülék közelében történő társalgás). Mindezt olyan szinten, hogy mármár az emberek teljes személyisége felépíthető lenne a róluk gyűjtött adatból. "It is not data that is being exploited, it is people that are being exploited" - Edward Snowden

Ahhoz, hogy ez a rengeteg adat elemezhető formába kerüljön, számos technológia is előtérbe került, mint például a NoSQL adatbázisok. A fókuszba már nem az adatgyűjtés fejlesztése van, hanem az elemzési módszerek gyorsítása, hiszen adat gyakorlatilag "végtelen" mennyiségben áll rendelkezésre. Megjelent a Hadoop framework, amely elosztott adatfeldolgozást tesz lehetővé, ezen felül elterjedt az adat memóriában való tartása és feldolgozása is, ezzel is növelve a sebességet a lassú adattárolókkal szemben. Ezt az időszakot *Analytics 2.0*-nak nevezik.

2.3. Az adat jövője

Az adatelemzés sokak szerint már most elérte az *Analytics 3.0*-t, az IoT eszközök gyors terjedésével és a peremszámítás (edge computing) bevezetésével, amivel az adat elemzése jelentősen gyorsult, csökkentve a nyers adat továbbításának mértékét. Ezen felül a gépi tanulási módszerek is elérték azt a szintet, amivel már a gyakorlatban is bevethetők és nagy hatékonysággal végezhető velük adatelemzés és akár valós idejű eredményekkel is szolgálhatnak.

A feldolgozott adattal már prediktív adatelemzésről is beszélhetünk. Az elemző szoftverek ekkor események bekövetkezésének valószínűségét becslik, kockázatot számolnak és ezzel támogatják a különböző döntéshozatali lépéseket.

A közeljövőben valószínűl ezen technológiák és elemzési módszerek továbbfejlesztése lesz a cél. Ami a következő nagy változást okozhatja az a kvantumelemzés megjelenése, amely a kvantumszámításra alapozna. Ennek a várható bekövetkezése csupán találgatásokon alapszik, már évtizedek óta ígérik. A nagyvállalatok (IBM, Google, Microsoft) folyamatos kutatásokat végeznek a kvantumszámítógépek területén. Hogy ez fogja-e szolgáltatni az *Analytics 4.0* alapjait vagy sem, még a jövő kérdése.

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. 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. Ez azonban nem minden szempontból jelenti ugyanazt. Beszélhetünk *erős* és *gyenge* kétharmados törvényekről. 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 csökkenő irányban a következőket értjük jogszabályoknak: törvények, 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 kihírdetni. A jogalkotásról a jelenleg érvényben levő 2010. évi CXXX. törvény és az annak a módosításáról szóló 2019. évi II. törvény szól. [3, 4, 5, 6]

3.2. Jogalkotás az Európai Közösségben

Az Európai Unió joga több forrásból merít, ezeket fogom alább ismertetni. [7]

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. [8]

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. [9]

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. [10]

Az ez alatti szinten a másodlagos jog található, amely csak akkor érvényes, ha összhangban van a hierarchiában felette álló 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. [11]

A jogalkotásban részt vesz az Európai Parlament, az Európai Tanács, az Európai Bizottság, a Gazdasági és Szociális Bizottság, és az Állandó Képviselők 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 rendelettől eltérően, amely az uniós országok belső jogrendszerében közvetlenül és a hatálybalépést követően azonnali hatállyal alkalmazandó, az irányelv nem közvetlenül alkalmazandó az uniós országokban. A nemzeti jogalkotónak átültető jogszabályt kell elfogadnia, amellyel a nemzeti jogszabályokat az irányelvekben megállapított célkitűzésekhez igazítja. Az egyes polgárokat alapvetően csak akkortól illetik meg a jogok, illetve terhelik a kötelezettségek, miután az átültető jogszabályt elfogadták. A tagállamok a nemzeti jogba való átültetés tekintetében bizonyos mérlegelési jogkörrel rendelkeznek, amely lehetővé teszi a nemzeti sajátosságok figyelembevételét. A határozattól eltérően az irányelv olyan dokumentum, amely általánosan alkalmazandó valamennyi uniós országra nézve.

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. [7, 12]

3.4. Jogharmonizáció Magyarországon

A jogharmonizáció azt a jogalkotási folyamatot jelenti, amely lehetővé teszi, hogy két jogrendszer szabályai egymással összeegyeztethetővé váljanak. Erre példa az unóis jogharmonizáció, ami az uniós jogszabályok összeegyeztetését jelenti a tagállamok saját jogrendszerével. Az uniós jog ugyanis önálló jogrendszert alkot. Autonómnak nevezhető ez a rendszer, hiszen az uniós jogszabályokat az uniós intézmények (Európai Bizottság, Tanács, Európai Parlament) alkotják meg, az uniós jog által szabályozott döntéshozatali

eljárások során. Emellett azonban fennmaradnak a nemzeti jogrendszerek is. Nyilvánvaló, hogy a jogbiztonság megteremtése érdekében alapvető szükséglet a két jogrendszer összhangjának megteremtése. Az uniós jognak be kell épülnie az Európai Unió tagállamainak jogrendszereibe. Ez a folyamat a jogharmonizáció.

A jogharmonizációs feladat elsősorban az Európai Unió intézményei által hozott irányelvek átültetését jelenti (de bármely uniós jogi rendelkezésből fakadhat). Az Európai Unióról működéséről szóló szerződés 288. cikke értelmében az irányelv "az elérendő célokat illetően minden címzett tagállamra kötelező, azonban a forma és az eszközök megválasztását a nemzeti hatóságokra hagyja". A tartalmi kérdések tekintetében ugyanakkor eltérő lehet a harmonizáció mértéke, hiszen nem ritkán ún. minimumszabályozást tartalmaznak az irányelvek, amely esetben az uniós jogszabálynál szigorúbb tagállami rendelkezések hozhatók (pl. a környezetvédelem vagy a fogyasztóvédelem területén). Ugyanakkor maximumszabályozás is előfordul, ekkor nem enged szigorúbb tagállami rendelkezéshozatalt. Amennyiben az uniós jogrendszerrel való összhang megteremtése érdekében új jogszabályok meghozására, meglévő jogszabályok módosítására van szükség, "pozitív jogharmonizációról" beszélünk; amennyiben meglévő rendelkezések hatályon kívül helyezése válik szükségessé, a "negatív jogharmonizáció" fogalmát használjuk.

A Lisszaboni Szerződés és korábban az EK-Szerződés is, a tagállamok feladatává teszi a jogharmonizációs kötelezettségek teljesítését. (Ezek elmulasztása esetén is a tagállammal, nem például annak valamely szervével szemben indul eljárás.) Az uniós jog viszont nem határozza meg a teljesítés módját, vagyis azt hogy milyen jogi formában, milyen eljárások során, mely szervek közreműködésével történjék meg a jogharmonizáció. Magyarország alkotmányos rendjében a jogharmonizáció felelőse a Kormány. Egyik fontos feladat a jogharmonizációs jogszabály-tervezetek elkészítése, amelyért az a minisztérium, vagy más állami szerv a felelős, amely az adott kérdésben részt vett az Unió döntéshozatali eljárásában, illetve a Kormány álláspontjának kialakításában. Kiemelt szerep jut az igazságügyért felelős miniszternek, aki a jogharmonizációs feladatok összehangolásáért, koordinációjáért felelős. Ennek keretében a jogharmonizációs javaslatokat meg kell jeleníteni a Kormány féléves munkatervében, illetve. törvényalkotási programjában. A miniszter felelős továbbá a jogharmonizációs kötelezettségek teljesítésének figyelemmel kíséréséért; egyetértési joggal rendelkezik a jogharmonizációs tervezetekkel kapcsolatban; jogharmonizációs adatbázist tart fenn. A teljesítést a Külügyminisztérium jelenti az Európai Bizottság felé. Az ellenőrzést és a visszakereshetőséget segítése érdekében minden jogharmonizációs céllal készült jogszabály záró rendelkezései között fel kell tüntetni, hogy az mely uniós jogszabály szabályainak átvételét szolgálja (jogharmonizációs záradék). Az Országgyűlés abban az esetben felelős a jogharmonizációs kötelezettség ellátásáért, ha az adott ügy törvényhozási tárgykörbe tartozik. Ezeket az ügyköröket nemzeti jogszabályok tartalmazzák: Magyarország Alaptörvénye és a jogalkotásról szóló 2010. évi CXXX. törvény. Amennyiben valamely átültetésre szoruló uniós jogszabály ilyen törvényhozási tárgykört érint, az Országgyűlés köteles új törvényt hozni, illetőleg hatályos törvényt módosítani. Ellenkező esetben törvényi, kormányrendeleti, vagy miniszteri rendeleti formában történhet a jogharmonizációs tervezetek elfogadása. [13]

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 Ügynöksége-et (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. Jogelődje az Európai Gazdasági Együttműködési Szervezet (OEEC), melyn 1948-ban alapult a Marshall-terv megvalósításának céljával. A Marshall-terv célja az volt, hogy a második világháború hatására elszenvedett gazdasági veszteségeket követően helyreálljon az európai országok gazdasága. Ezt a célt az 1950-es évek végére sikerült is teljesíteni, amivel az OEEC feladatát elvégezte, azonban a rengeteg felhalmozott tudást nem hagyták kárbaveszni, ezért alapulhatott meg utódja, az OECD 1961-ben. Fontos megemlíteni, hogy eddig hazánkról és az EU-ról volt szó, azonban az OECD egy világszervezet, számos európán kívüli tagállammal.

A témánkkal kapcsolatos fontos munkája a szervezetnek a magánélet védelméről és aszemélyes adatok határokon átívelő áramlásáról szólói irányelvei. Egészen korán, már 1980-ban elhatározta a szevezet, hogy kiadja nemzetközi irányelveit az előbbi témákról. Az irányelvet, mint ajánlást fogadta el a szervezet, amely szánékosan általánosan van megfogalmazva, hogy a technológiai változások könnyen hozzáidomíthatók legyenek. Az elvek az egyénekről szóló adatok számítógépes feldolgozásának minden médiumát, a személyes adatfeldolgozásminden típusát, valamint minden adatkategóriát felölel.

Az ajánlás nyolc alapelvet tartalmaz. Az **adatgyűjtés korlátozásának elve**, miszerint korlátozni kell a személyes adatok gyűjtését, valamint bármilyen ilyen jellegű adatot törvényes és tisztességes eszközökkel kell beszerezni, esetenként, az alany tudtával és beleegyezésével. Az **adatminőség elve** alapján a személyes adatok legyenek relevánsak azokra a célokra nézve, amelyekre azokat felhasználják, és amennyire ezen célokhoz szükséges, legyenek pontosak, teljesek és állandóan aktualizáltak. Az előző alapelvben is említett célra is van megkötés, amelyet a **célhoz kötöttség elve** határoz meg. A személyes adatok gyűjtésének célját legkésőbb az adatgyűjtéskor meg kell jelölni és azok későbbi felhasználását csak ezen célokra, vagy azokkal nem összeegyeztethetetlen célokra kell korlátozni. A **korlátozott felhasználás elve** kimondja, hogy a személyes adatokat

nem szabad nyilvánosságra hozni, rendelkezésre bocsátani vagy bármilyen más módon felhasználni a meghatározott célokon kívül, kivéve az adatalany beleegyezésével, vagy a törvény hatalmánál fogva. Ennél fogva mégjobban nyomatékosítja a célhoz kötöttség elvét. Az adatokat nem csupán az adatkezelőtől, hanem külső részvevőktől és védei az ajánlás. Az adatkezelési célnak és a technika mindenkori állásának megfelelő ésszerű biztonsági intézkedések megtételét követeli a **biztonság elve**. A **nyiltság elve** szerint az adatkezelésnek és az adatkezelési politikának nyilvánosan elérhetőnek kell lennie, az adatok körének, kezelésük céljának, jogalapjának, az adatkezelő kilétének megismerhetőségét biztosítani kell. Az **egyén részvételének elve** kimondja, hogy az adatalanynak joga van tudni a róla tárolt adatról, azokat megkapni, kifogásolni, módosítani vagy törölni. Legvégül a **felelősség elve** szerint a fenti alapelvek betartásáért az adatkezelő a felelős.

Az ajánlás leírást azt a nemzetközi és nemzeti alkalmazásokra vonatkozóan is, 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. [14]

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.

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 stragiájuk 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 hálózat- és információbiztonságra vonatkozó uniós szakpolitikák és jogszabályok megszövegezésében is, és ezzel közvetve hozzájárul a gazdasági növekedéshez az EU belső piacán.

Az ENISA-nak központi szerepe volt a NIS dírektíva 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 tes-

tület 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. Az ENISA-nak többek között ehhez is hozzá kell járulnia.

Tehát az ENISA feladata, hogy gyakorlati oktatással, tanácsokkal és irányelvek megfogalmazásávl, tanulmányok készítésével segítsék az európai unió tagállamait, állami és magánszktorait és az unió polgárait a megfelelő online biztonság elérésére. Az emberek folyamatosan fokozzák online jelenlétüket, amely a COVID-19 járvány miatt mégnagyobb 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, 18]

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 Alapjogi Chartája (Charta) 8. cikkének (1) bekezdését és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdését, miszerint mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Ahogyan azt a 2 fejezetben bemutattam a 2009-2010-es években akkora változás indult meg az adatok gyűjtésében és azok felhasználásában, amely miatt felismerték, hogy a 95/46/EK irányelv [19] nem váltja be a hozzá fűzött reményeket. Ennek eredményeként 2012-ben megindult a jogalkotási eljárás, melynek lezárulásával 2016 április 27-én elfogadta 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 működnek, 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 kevésbényilvánvaló 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;

A GDPR hét alapelvet fogalmaz meg, amelyet az érintett vállalkozásoknak be kell tartaniuk. **Jogszerűség, tisztességes eljárás és átláthatóság**, miszerint a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. A **célhoz kötöttség** elve szerint a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. **Adattakarékosságra** kötelez, tehát a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. A negyedik elv a **pontosság**, hogy a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék. A személyes adatok tárolásának hosszát a **korlátozott tárolhatóság** elve mondja ki. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Az **integritás és bizalmas jelleg** elve alapján a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. Végül az **elszámoltathatóság** elve kimondja, hogy az adatkezelő felelős az előbbieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

Az adatkezelők által betartandó kötelezettségeken felül a GDPR az érintetteknek különböző jogokat is megfogalmaz. Első az **átlátható tájékoztatáshoz való jog**, miszerint az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az érintettet tájékoztatni kell többek között az adatkezelő és annak képviselőjének kilétéről, elérhetőségeiről, az adatkezelés céljáról, a személyes adatok címzettjeiről, annak tárolásának időtartamáról, stb. Lényegében minden paraméterről, ezzel totális átláthatóságot biztosítva. Az érintett **hozzáférés joga** kimondja, hogy az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és számos a kezelés célját és módját leíró információkhoz hozzáférést kapjon. Az érintettnek joga van a személyes adatok manipulálására, ide értve a **helyesbítést** és a **törlést**. Az érintett jogosult arra, hogy kérésére az adatkezelő **korlátozza** az adatkezelést, ha azok pontatlanok, az adatkezelés jogellenes, az adatkezelőnek már nincs szüksége a személyes adatokra, vagy ha az érintett tiltakozott az adatkezelés ellen. Ha az adatkezelés automatizált módon történik és az adatkezelés az érintett hozzájárulásán vagy szerződésen alapszik, akkor vonatkozik rá az **adathordozhatósághoz való jog**, tehát jogosult arra, hogy a rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta. Az érintett számos esetben jogosult, hogy **tiltakozzon** az adatkezelés ellen, valamint joga van az **automatikus döntéshozatal elutasításához**. Utóbbi szerint az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá

nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. [20]

Az általános adatvédelmi rendelet tehát az érintettek teljeskörű tájékoztatását célozza meg, valamint befolyást próbál adni az éreintettek kezébe a személyes adatuk fölött. Megvannak az előnyei és a hátrányai is. 2019-ben lehetőségem volt élőben meghallgatni egy interjút [21] 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

Az elektronikus azonosításról és bizalmi szolgáltatásokról szóló egységes, szabványosított rendelet (910/2014/EU eIDAS rendelet) hatályon kívül helyezte, hogy megerősíthesse és bővíthesse vívmányai az 1999/93/EK európai parlamenti és tanácsi irányelvet, amely az elektronikus aláírásra vonatkozott. Utóbbi hibája, hogy nem hozott létre átfogó határokon átnyúló és ágazatközi uniós keretet az elektronikus tranzakciók biztonságának, megbízhatóságának és könnyű használhatóságának érdekében.

A rendelet célja a belső piac megfelelő működésének biztosítása, ugyanakkor az elektronikus azonosító eszközök és a bizalmi szolgáltatások megfelelő szintű biztonságának garantálása. Ennek érdekében megállapítja azokat a feltételeket, amelyek mellett a tagállamok elismerik a természetes és jogi személyek más tagállamok bejelentett elektronikus azonosítási rendszerének keretébe tartozó elektronikus azonosító eszközeit. Továbbá megállapítja különösen az elektronikus tranzakciókhoz kapcsolódó bizalmi szolgáltatásokra vonatkozó szabályokat. Végül pedig létrehozza az elektronikus aláírások, az elektronikus bélyegzők, az elektronikus időbélyegzők, az elektronikus dokumentumok, az ajánlott elektronikus kézbesítési szolgáltatások és a weboldal-hitelesítési szolgáltatások jogi keretét. Ezen feltételek a mai körülmények között teljesen elengedhetetlenek és nélkülözhetetlenek, tekintve a társadalmi, gazdasági és technológiai fejlődésre, hiszen az online környezet egyre nagyobb bizalmat igényel. Továbbá számos hozama/előnye is van, többek között a külföldi kezelések során a betegek egészségügyi adatainak hozzáférhetőeknek kell lenniük a kezelés helye szerinti országban, ehhez az elektronikus azonosítást szolgáló szilárd, biztonságos és megbízható keretrendszer biztosít.

A rendelet az elektronikus azonosítás terén elrendeli a kölcsönös elismerés elvét, miszerint ha egy köztigazgatási szerv elektornikus azonosítást használ és azt megfelelően bejelentette, akkor azt minden tagállamban el kell ismerni.

A rendelet követelményeket és előírásokat vezet be a bizalmi szolgáltatások területén is és azon bizalmi szolgáltatásokat, amelyek megfelelnek a követelményeknek, minősített bizalmi szolgáltatásokká lépteti elő. A bizalmi szolgáltatások, amelyekről szó esik az elektronikus aláírás, elektronikus bélyegzés, elektronikus időbélyegzés, elektronikus kézbesítési szolgáltatás és weboldal-hitelesítés.

A rendelet legfőbb célja, hogy felszámolja a tagállamok digitális piacának szétaprózódottságát és egy egységet hozzon létre. [22]

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 szereplő törvények kimondják, hogy mindenkinek joga van személyes adatai védelméhez és ezen jog érvényesülését törvénnyel létrehozott független hatóság kell ellenőrizze. [4]

Ezen törvény a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) [23]. A törvény 2011-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 a bármilyen közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat. A közérdekből nyilvános adat pedig olyan adat, amelynek nyilvánosságát a törvény közérdekből elrendeli. 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 közzétegye internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozás- és díjmentesen.

A veszélyhelyzetben, hogy azonban az Infotv-re módosítások léptek életbe, ezek hatálya átmeneti. [24] A jelenleg hatályban levő 521/2020. (XI. 25.) Korm. rendelet többek között a személyes kontaktuk elkerülése, valamint a határidők hosszabbítása érdekében született.

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 értjük. Az állami szervek által kezelt, a nemzeti adatvagyon körébe tartozó nyilvántartások fokozott biztonságáról való gondoskodás elengedhetetlen az állampolgárok államba vetett bizalmának

visszaállítása, valamint a közigazgatás folyamatos és zavartalan működésének biztosítása érdekében. Ezért törvény az adatfeldolgozással megbízható személyek és szervezetek körét korlátozhatja, vagy az adatfeldolgozásnak az adatkezelőtől különböző személy vagy szervezet általi ellátását kizárhatja. Ezen felül az adatfeldolgozást korlátozhatja csupán államigazgatási vagy kizárólag állami tulajdonú gazdálkodó szevezetekre. [25]

A kormány létrehozott egy mellékletet, amely meghatározza a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóinak körét, az adatfeldolgozó igénybevételének kötelező vagy az adatkezelő döntésétől függő jellegét. [26]

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 kiemelten fontos az információs társadalmat érő fenyegetések miatt az elektornikus adatok és az ezeket kezelő információs rendszerek biztonsága. A társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus 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 érdekében hozta az Országgyűlés a 2013. évi L. törvényt az állami és önkormányzati szervek elektronikus információbiztonságáról [27].

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 emelekdésével párhuzamosan szigorodó védelmi előírásoknak kell eleget tenni. A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A szervezet vezetője magasabb osztályt is meghatározhat, illetve hatósági engedéllyel és megfelelő indoklással alacsonyabb biztonsági szintet is. A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. Ha a rendszerben valamilyen változás történik, vagy új elektornikus információs rendszer kerül bevezetésre, vagy a feldolgozott adatok vonatkozásában történik változás, akkor soron kívüli felülvizsgálatot kell tenni. Az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell a 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. Külön logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatározni amelyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást és a biztonsági események kezelését.

A Kormány hatóságot jelöl ki a törvény hatálya alá tartozó elektronikus informá-

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

ciós rendszerek biztonsági felügyeletére, aminek feladata többek között biztonsági szint megállapításának ellenőrzése, a követelmények teljesülésének ellnőrzése. 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. A hatóság, ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, információbiztonsági felügyelő kirendelését kezdeményezheti. Az információbiztonsági felügyelő a fenyegetés elhárításához szükséges védelmi intézkedések eredményes megtétele érdekében a Kormány által rendeletben meghatározott intézkedéseket, eljárásokat javasolhat, a szervezet intézkedései tekintetében kifogással élhet.

A Kormány számítógépes eseménykezelő központok megalakulását is támogatta, amelyek az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egységek, amelyek a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkeznek.

A kormányzati koordináció biztosításáért a Nemzeti Kiberbiztonsági Koordinációs Tanács felelős, ami javaslattevő, véleményező szerveként gondoskodik a szervezetek e törvényben és végrehajtási rendeleteiben meghatározott tevékenységeinek összehangolásáról. A Tanács tevékenységét az e-közigazgatásért felelős miniszter által delegált kiberkoordinátor, valamint a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító kiberbiztonsági munkacsoportok és a Nemzeti Kiberbiztonsági Fórum támogatja.

5.3. Szankcionálás Magyarországon

Magyarországon a 2012. évi C. törvény a Büntető Törvénykönyvről (BTK) [28] foglalja össze törvény formájában a büntetendő cselekvéseket. Bűncselekmény minősül 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. A törvény megkülönböztet két tipusát 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.

A témánkkal kapcsolatos része 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.

Témánkbavágóan tiltott adatszerzésnek minősül, ha személyes adat, magántitok, gaz-

dasági titok vagy üzleti titok jogosulatlan megismerése céljából valaki elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti, vagy információs rendszerben kezelt adatokat titokban kifürkész, és az észlelteket technikai eszközzel rögzíti. Ennek büntetése három évig terjedő szabadságvesztés.

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, 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.

Utóbbi esetén nem büntethető az elkövető, ha tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását. Minden más esetben azonban a BTK szabadságvesztéssel bünteti az elkövetőt.

Irodalomjegyzék

[1] The evolution of data collection and analytics, Mar 2020. URL: https://taxandbusinessonline.villanova.edu/blog/the-evolution-of-data-collection-and-analytics/.

[2] A history of data collection, storage, and analysis, May 2018. URL: https://www.gutcheckit.com/blog/a-history-of-data/.

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

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

[5] 2010. évi cxxx. törvény, 2010. URL: https://net.jogtar.hu/jogszabaly?docid=a1000130.tv.

[6] 2019. évi ii. törvény, 2019. URL: https://mkogy.jogtar.hu/jogszabaly?docid=A1900002.TV.

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

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

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

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

[11] 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.

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

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

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

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

[19] Az európai parlament és a tanács 95/46/ek irányelve, 1995. URL: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A31995L0046.

[20] 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.

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

[22] 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.

[23] 2011. évi cxii. törvény, 2020. URL: https://net.jogtar.hu/getpdf?docid=a1100112.tv.

[24] 521/2020. (xi. 25.) korm. rendelet, 2020. URL: https://net.jogtar.hu/jogszabaly?docid=A2000521.KOR&dbnum=1.

[25] 2010. évi clvii. törvény, 2010. URL: https://net.jogtar.hu/jogszabaly?docid=a1000157.tv#lbj6id3b95.

[26] 38/2011. (iii. 22.) korm. rendelet, 2011. URL: https://net.jogtar.hu/jogszabaly?docid=a1100038.kor.

[27] 2013. évi l. törvény, 2013. URL: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv.

[28] 2012. évi c. törvény, 2012. URL: https://net.jogtar.hu/jogszabaly?docid=a1200100.tv.