HORVÁTH REGINA*

Az okoseszközök világának kockázatai a GDPR tükrében, avagy mennyire vagyunk biztonságban?

I. Bevezetés

Napjainkban egyre többet hallani arról, hogy egy eszköz „okos". Ezen eszközök lassan az életünk minden területét áthatják és jelentőségük a következő években csak még tovább fog növekedni. Ugyanakkor tagadhatatlan, hogy az okoseszközök alkalmazása jelentős adatvédelmi kockázatokkal is jár. A felgyorsult technológiai fejlődés megkönnyíti és lehetővé teszi egyrészről a személyes adatokhoz való hozzáférést, és azok nagy számban való gyűjtését. Másrészről a személyes adatok áramlása is egyre nagyobb méreteket ölt, immáron nem csak az egyes államokon belül, de az egyes államok között is. Az Európai Unió felismerte ezen terület védelmének a fontosságát, hiszen a személyes adatok áramlásának a gazdasági fejlődés szempontból nem célszerű határt szabni, azonban ezek az adatok olykor ellenőrizhetetlenül vándorolnak tagállamok és harmadik államok között.

A személyes adatok megfelelő szintű védelme érdekében az Európai Unió egy mindenre kiterjedő, átfogó szabályozást alkotott meg. Ez az ún. Általános Adatvédelmi Rendelet (General Data Protection Regulation, röviden: GDPR), amely mondhatni forradalmi változást hozott. Kutatásomban erre az új szabályozásra koncentrálok az okoseszközök világának tükrében.

Dolgozatomban elsőként bemutatásra kerülnek az egyes intelligens megoldások, azok térnyerésének előnyei és-árnyoldalai is. Az újabb és újabb eszközök megjelenésével egyre több szolgáltatás is napvilágot lát. A technológiának köszönhetően már szinte minden vállalat átalakulásra kényszerült a 90'-es évekhez képest, akik pedig nem képesek a modernizációra, azok többnyire arra kényszerülnek, hogy befejezzék tevékenységüket. Ezt követően az Európai Unión belül az Európai Bizottság tevékenységére fókuszálok, amelynek többrétű tevékenysége mutatható ki mind az infokommunikációs technológiák, mind a személyes adatok védelme kapcsán. Végezetül a GDPR rendelkezéseit elemzem, majd kifejezetten az okoseszközökre való alkalmazásukat vizsgálom

* SZTE Állam- és Jogtudományi Kar

meg. Az így leszűrt következtetések alapján fogalmazom meg arra vonatkozó javaslataimat, hogyan lehetne még hatékonyabbá tenni a jelenlegi szabályozást.

II. Az okoseszközök világa

A digitalizálódás útján haladva emelkedik az integráció szintje, ami révén megváltozik a felhasználók szerepe, és fogyasztókból bizonyos szinten ők maguk is szolgáltatókká válhatnak. Ez a változás lehetővé teszi az erőforrások hatékonyabb megosztását és kiaknázását. Mindezek mellett számos problémával is szembesülhetünk, hiszen az elmúlt években igen rohamos fejlődésnek indult a digitális világ és épp a sokszínűsége miatt nehezen átlátható és még nehezebben kézben tartható. Manapság az élet minden területét áthatja. Minden tevékenységhez tartozik olyan szolgáltatás vagy alkalmazás, amely a technológia gyümölcse. 2025-re több mint 31 milliárd okos eszköz lesz jelen az Internet of Things-en (IoT, dolgok internete).[1] A felhasználók nemcsak, hogy nem látják át ezek működését, hanem a technikai bonyolultságuk miatt ezen eszközök kapcsán a fogyasztók, a felhasználók is egyre laikusabbakká válnak, nehezebben látják át a felmerülő biztonsági kockázatokat is.

Nem kétséges, hogy a technológia ilyen felgyorsult fejlődése mellett egyre nagyobb hangsúlyt kell helyezni a biztonságra. Számos esetben maga a jogalkotó is falnak ütközik ezekben a kérdésekben, hiszen rendkívül nehéz mind az uniós, mind a hazai jogot adaptálni a rendkívül gyorsan fejlődő technológiára. Dolgozatom témájaként éppen ezért választottam az adatvédelem problematikáját az okoseszközök világában, mivel rendkívül aktuális, folyamatosan fejlődő területről van szó, amellyel az adatvédelem uniós jogi szabályozása próbál lépést tartani. Az Európai Unió alapvető jogként ismeri el a személyes adatok védelméhez való jogot.[2] Az 5G közeledte és az IoT megjelentése pedig már szinte a „nyakunkon" van. A jövő új technológiája már az ajtónkon kopogtat.[3] Mielőtt áttérek az okoseszközök bemutatására még érdemes pár szót ejteni a IoT-ről[4], azaz az Internet of Things-ről,[5] amelynek elterjedése és jelentősebb térnyerése már

---

[1] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), Forrás: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, Utolsó letöltés ideje: 2018.12.06.

[2] Európai adatvédelmi jogi kézikönyv (Az Európai Unió Alapjogi Ügynöksége és az Európa Tanács, 2014) Forrás: https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf, Utolsó letöltés ideje: 2018.12.06.

[3] ESKENS, SARAH: *Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?* (February 29, 2016). Available at SSRN: https://ssrn.com/abstract=2752010, 12. p.

[4] Noto LA DIEGA GUIDO – WALDEN, IAN: *Contracting for the 'Internet of Things': Looking into the Nest*. (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016. Available at SSRN: https://ssrn.com/abstract=2725913, 4. p.

[5] The Guardian- What is the internet of things?, Forrás: https://www.theguardian.com/technology/2015/may/06/ what-is-the-internet-of-things-google, Utolsó letöltés ideje: 2018.12.06.; Rise of the machines: who is the 'internet of things' good for? Forrás: www.theguardian.com/technology/2017/jun/06/internet-of-things-smart-home-smart-city, Utolsó letöltés ideje: 2018.12.06.

2-3 éven belül megvalósulhat, tehát ez nem más, mint a Mi jövőnk.[6] A pontos fogalma akként határozható meg, hogy ebbe a csoportba tartozik minden olyan eszköz, amely képes más eszközökkel kommunikálni valamilyen formában. Működés közben képes az információkat más berendezésekhez eljuttatni és a technológiának köszönhetően felhő formájába feltölteni és a világ bármely pontjára eljuttatni másodpercek alatt. Tehát röviden megfogalmazva minden olyan eszköz, amely képes csatlakozni az internethez és az általa begyűjtött információt megosztani felhő formájában a világgal.[7]

A IoT eszközöket gyakran szokták egyébként Smart-nak is nevezni, ami persze nem fedi le egy az egyben ezt a meghatározást. IoT és Smart is lehet például egy monitor, egy fülhallgató, egy mobiltelefon, azonban egy okos konyhai robotgép már inkább csak Smart és nem IoT, hiszen míg a mobiltelefon képes felhő formájában megosztani tapasztalatait, addig egyelőre egy robotgép nem. A módszer sikerének titka, hogy rengeteg pénz és energia takarítható meg, és gyorsasága nem hasonlító más technológiához. 2018-ban a IoT belátható közelségbe került számunkra, pár év és ki fognak teljesedni az erre alapuló biztonságtechnikai rendszerek, riasztórendszerek, csak a megrendelő fantáziája szabhat határt annak, hogy hogyan szeretné a háztartását irányítani és annak is, hogy honnan. Egyik fő mozgatórugója a versenyképessége, gyorsasága, energiatakarékossága és környezetkímélete. Kialakulása számos vezeték nélküli hálózat kidolgozásához vezetett.[8]

Napjainkban a vállalkozások az adatok tárolásához szolgáló hibrid megoldásokat kezdik el preferálni, egyre több cég választja magának a felhő[9] alapú rendszereket az infrastruktúrája kialakításakor. Számos nagy cég kiáll az ügy érdekében és igyekszik olyan eszközöket fejleszteni, amelyek teljes mértékben biztonságos eszközül szolgálnak a IoT rendszerekben. Az *Internet of Things Security Foundation* (IOTSF) egy olyan közel 30 vállalatból álló kezdeményezés, melynek fő célja, hogy biztonságosabbá tegyék a „Dolgok Internetét". A kezdeményezéshez csatlakozott az Intel, a Siemens, a British Telecom is. *John Moor* a szervezet egyik kiberbiztonságtechnikai szakembere akként fogalmazta meg az IoT-t, mint amely „olyan mint a repülés, addig félnek tőle az emberek, amíg be nem bizonyítjuk, hogy biztonságos".[10]

Fontos figyelembe venni azt is, hogy az eszközök egymáshoz való csatlakoztatásának képessége nem csak pozitív célokra használható. Melegágyként szolgálhat a vírus- és hacker támadásoknak.[11] A különböző alkalmazások segítségével például a Google és a Facebook tudja a tartózkodási helyünket, azonban az IoT rendszerek létrehozásával már

---

[6] THIERER, ADAM D.: *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation.* (February 18, 2015). 21 RICH. J.L. & TECH. 6 (2015). Available at SSRN: https://ssrn.com/abstract=2494382, 2-3. pp.

[7] THIERER, ADAM D.: i. m. 1. p.

[8] ESKENS, SARAH: *Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?* (February 29, 2016). Available at SSRN: https://ssrn.com/abstract=2752010, 13. p.

[9] HON, W. KUAN – MILLARD, CHRISTOPHER – SINGH, JATINDER*: Twenty Legal Considerations for Clouds of Things*. (January 4, 2016). Queen Mary School of Law Legal Studies Research Paper No. 216/2016. Available at SSRN: https://ssrn.com/abstract=2716966, 4. és 14. p.

[10] The home of IoT security, IoT Security Foundation, Forrás: https://www.iotsecurityfoundation.org, Utolsó letöltés ideje: 2018.10.24.

[11] PEPPET, SCOTT R.: *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent.* (March 1, 2014). Texas Law Review. Forthcoming. Available at SSRN: https://ssrn.com/ abstract=2409074, 27. p.

minden adatunkat ismerik majd.[12] A megszerzett információk birtokába jutott cégek könnyen kideríthetik, hogy mik a vásárlási szokásaink, milyen termékeket használunk, és ez alapján befolyásolni tudják a piaci kínálatot[13]. Mint minden technikai termék esetében, itt is fennáll az elavulás veszélye, ezért gyorsabban cserélni kell az elektronikai cikkeket.[14]

További kockázatkat rejtő probléma az internet-függés, és ez csak még kritikusabbá válik, ha már teljes mértékben ez vesz körül minket. A 4G hálózat, azaz a 4.generációs vezeték nélküli hálózat napjaink fő meghatározója, amely elődjeihez képest nagyobb adatátviteli sebességgel és kapacitással bír.[15] A VoLTE (Voice-over-LTE) technológiának köszönhetően a mobilinternetezésen túl a hangszolgáltatások is a 4G minőségében bonyolíthatók le, ami elsősorban gyorsabb hívásfelépülést, HD hangminőséget és hívás közben is 4G sebességű adatkapcsolatot tesz lehetővé. Jelenleg a 4G-s adathasználatra képes mobiltelefonok egy hívás indításakor a közelben elérhető 2G vagy 3G hálózatra váltanak, ami növeli a hívás felépülésének idejét. A 4G hanghívások megmaradnak majd a 4G hálózaton, így érezhető mértékben lecsökken majd a kapcsolás időtartama. Azonban nem ez lesz az egyetlen, érezhető előnye a teljesen IP-alapúvá váló telefonhívásoknak, hanem többek között az is, hogy a 4G-n indított hívások a telefonok akkumulátorát is jóval kisebb mértékben terhelik meg, mint a hagyományos technológia. Ezek mellett már belátható közelségbe került az 5G kialakítása is. Globális szinten az 5G-s kereskedelem beindítását 2020-ra tervezik. Az 5G-t támogató okostelefonok várhatóan 2019 elején jelennek meg majd, amely egy új és idáig még nem tapasztalt gyorsasággal repíti el az információkat a világ egyik pontjáról a másik pontjára, amely gyorsabb lesz az emberi érzékelésnél is.[16] Az EU célja, hogy 2020 végére minden háztartás számára 30mbs sebességű internet legyen elérhető, viszont az 5G minimum 1, maximum 10 gigabites sebessége ezt a célértéket többszörösen túlszárnyalná. E hálózat célja az 1 milliszekundumos késleltetés. Ez akár olyan gyors is lehet, mintha egy vonat 500km/h sebességgel lenne képes közlekedni.[17] Alappal feltételezhetjük, hogy ez már teljesen felesleges. Feltöltünk egy videót a Youtubera és akár pár másodperc alatt már elérhető akár Izlandon is. Ijesztő lehet ez a gyorsaság, de attól függ, mely oldalról közelítjük meg ezt a kérdéskört. Például az önvezető autók tekintetében milyen jelentőséggel bírna, ha hogy az tízszer gyorsabban reagálna, mint a szemünk? Mennyi balesetet lehetne ezzel elkerülni? Az pedig, hogy ez személyes adataink biztonságára nézve és magánszféránk védelme tekintetében mennyire jó, vagy mennyire hasznos, azt dolgozatom

[12] WACHTER, SANDRA: *The GDPR and the Internet of Things: A Three-Step Transparency Model*. (February 5, 2018). Law, Innovation and Technology. Available at SSRN: https://ssrn.com/abstract=3130392, 26. p.

[13] EDWARDS, LILIAN: *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective.* (January 5, 2016). *European Data Protection Law Review* (Lexxion), 2016, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2711290, 3-6. pp.

[14] HOFFMAN, DONNA L. - NOVAK, THOMAS: *Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things* (August 20, 2015). Available at SSRN: https://ssrn.com/abstract=2648786, 41. p.

[15] How fast is EE's 4G, Forrás: https://www.theguardian.com/technology/blog/2012/oct/03/4g-ee-mobile-broadband, Utolsó letöltés ideje: 2018.12.06.

[16] The 5G network: when will it launch and what will it mean for consumers? Forrás: https://www.theguardian.com/media-network/media-network-blog/2014/aug/26/5g-network-launch-mobile-consumers-connectivity-download, Utolsó letöltés ideje: 2018.12.06.

[17] South Korean 5G internet move to further increase download speeds, Forrás: https://www.theguardian.com/technology/2014/jan/23/south-korea-intenet-download-speeds-5g, Utolsó letöltés ideje: 2018. 12. 11.

további részében kívánom elemezni. Az okoseszközök tulajdonságainak és lehetséges veszélyeinek bemutatását aszerint kategorizáltam, hogy az életünk mely területén van jelen velünk, kifejezetten a biztonság kérdéskörére összpontosítva.

1. Okoseszközök rajtunk/nálunk

a) Okostelefon: Nehéz manapság az okostelefon pontos definícióját megadni. Úgy lehetne körülírni, miszerint egy olyan „high-end" eszköz, amelyben ötvöződik a mobiltelefon képessége PDA[18] (Personal Digital Assistant) funkcióval, tehát elvárás az, hogy telefonként és egy személyi asszisztensként (P.I.M.= Personal Information Manager) is működjön. Számos további funkciót várunk el manapság az okostelefonokkal szemben, amelyek egyben biztonsági kockázatot is jelentenek. Például a kamera, a böngészés, HD videó felvétel készítése, zene lejátszás, multimédia (sms, mms) stb. Először 2007-ben használták ezt a kifejezést, amikor bemutatták az első Iphone-t[19], amely forradalmian újnak számított e területen a „multy-touch" képernyőjével és az új designnal megalapozva az okostelefonok piacát. A legújabb Iphone okostelefonok manapság már rendelkeznek beépített Face ID-vel, amely az arcfelismerés révén végez hitelesítést, tehát csak a beállított tulajdonos arcára nyílik fel. Jelszó helyett használhatunk Touch ID-t, ahol az ujjlenyomatunk segítségével oldjuk fel a készülékünket. Az okostelefonokban elérhető a helymeghatározás funkció is, ami által könnyedén bemérhetik tartózkodási helyünket. A Geotagging funkció képes az elkészített fényképhez, médiafájlokhoz, honlapokhoz földrajzi koordinátákat (GPS adatok) hozzárendelni. A Geotagging pozitívummal és negatívummal is rendelkezik. A pozitívumra példa az Apple által kifejlesztett a Find My Iphone funkció, amellyel bejelentkezve az Icloud webhelyre megkereshetjük saját készülékünket vagy akár elveszett módba tehetjük, illetve távolról is törölhetjük a készülékünk tartalmát lopás esetén, ezzel védve magánszférákat azzal, hogy mások ne tudjanak hozzáférni a személyes adatainkhoz. Szintén Apple találmány a „Barátok keresése" alkalmazás, amellyel az előzetesen felvett személyek helyzetét nyomon követhetjük a telefonunkkal, amennyiben a másik fél engedélyezte láthatóságát, ezáltal láthatjuk ismerőseink helyzetét. Az Apple biztonsági lépéseket is bevezetett ezen alkalmazás használata során. A felhasználóknak kell a követési kéréseket jóváhagyni és elutasítani. Törölhetünk a követőink közül, vagy választhatjuk az elrejtőzés funkciót, amikor más felhasználók nem láthatják a tartózkodási helyünket.[20] Van egy rendkívül előremutató lehetősége is, be lehet állítani egy szülő-gyermek követést, amelyen a szülő egy jelkódot tud beállítani a korlátozásokhoz, így a gyermek ezt nem fogja tudni kikapcsolni. Ezekkel a funkciókkal azonban vissza is lehet élni, hiszen informatikához jól értő személy könnyedén rá tud kapcsolódni más felhasználó készülékére, annak hozzájárulása nélkül, így hozzájutva információkhoz, személyes adatokhoz.

---

[18] Magyarul személyes digitális asszisztens, amely egyben a hívásfogadási funkciókon felül egy hordozható számítógépnek is megfelel, tehát képes például: adatgyűjtésre, naplózásra, fotózásra, adattárolásra.

[19] HOFFMAN, DONNA L. – NOVAK, THOMAS: *Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things*. (August 20, 2015). Available at SSRN: https://ssrn. com/ abstract=2648786, 86. p.

[20] HON, W. KUAN-MILLARD – CHRISTOPHER SINGH: *Jatinder* i.m. 14. p.

b) Okosóra: Az okosóra a hagyományos időmutatási funkciókon kívül számos más ún. PDA funkcióval rendelkezik, amely alapján hasonló mind tulajdonságai, mind működése alapján az okostelefonokhoz. Az Apple Watch Series 3-mal párosított Iphone akkor is megosztja a GPS helyzetet, ha az Iphone hatókörén kívül helyezkedünk el. A szülő-gyermek követési funkció itt is érvényesülhet, ahogyan az okostelefonoknál. Belső memóriával rendelkezik az óra, tehát már nincsen szükség mp3 lejátszóra sem. Rögzíti az aktivitás adatait, pulzust mér és figyelemmel kísérhetjük eközben az időjárás alakulását, szükség esetén telefonálást is lebonyolíthatunk, elolvashatjuk üzeneteinket. Számolhatjuk az óránkkal adott esetben, hogy mennyit futottunk, hány kmnél járunk. Futás közben rögzített GPS adatokból létrehoz egy útvonalat a futásunk végén a térképen, és ha ezt megosztjuk az interneten, akkor bárki láthatja hol futni, hány óra körül és kivel. Kitérnék arra, hogy vannak kifejezetten olyan okosórák, amelyek a gyermekünk követésére szolgálnak. Ezek az órák le vannak korlátozva egy kétirányú telefonálásra, tehát a szülő és gyermek oda-vissza hívhatja egymást ezen keresztül. Szintén GPS helymeghatározással bír, tehát a gyermek helyzetét folyamatosan jelzi a szülőknek az okostelefonukra töltött alkalmazáson, applikáción keresztül. Létrehozható egy elektronikus kerítés az órával. Ezalatt értendő, hogy kijelölhető egy terület a gyermek számára, pl. a lakóhely, hogy ha ezt a területet elhagyja a gyermek, akkor a szülő erről értesítést kap. Rögzíti az útvonalat, amerre a gyermek jár. Olyan négysávos GSM rendszer alapján van létrehozva, amely alapján bármilyen sim kártyát le tud olvasni. Beépített távfigyelési rendszere van, amely képes a környezetből kiszűrődő hangokat más felhasználóknak elküldeni vagy akár hívást is indítani az előre beprogramozott hívószámukra. Beépített nyomkövetővel is rendelkezik, amely alapján megfigyelhető, hogy a gyermek merre közlekedik. A biztonság oldaláról megközelítve számos kockázatot hordoz magában, hiszen épp úgy ahogyan az okostelefonokra rá lehet idegen felhasználóknak kapcsolódni, így az okosórára is lehetséges.

c) Okos fülhallgató: A viselhető audio eszközök térnyerése is megindult, hiszen jóval kisebb rádiófrekvencia kibocsátással működnek a telefonokhoz képest, így az egyészségünk megóvása szempontjából kedvezőbbek. A nemrégiben piacra dobott LG modell megkapta a Google Hangalapú asszisztensét, tehát képes arra, hogy a Google fordító használatával valós időben lefordítson hallás után bármilyen szöveget. Egyes fülhallgatók képesek gombnyomásra élő hangot rögzíteni, amely adott esetben súlyosan sértheti a személyiségi jogokat, a másik fél hozzájárulása nélkül. Bizonyos esetekben hasznos lehet, hogyha a hangfelvételünk esetleg bizonyítékul szolgál egy hatósági ügygyel kapcsolatban, azonban fontos tudni, hogy tilos a másik fél beleegyezése nélkül hangfelvételt rögzíteni.

d) Okos szemüvegen keresztül képes a technológia már egy virtuális valóság kiépítésére is, amely sikeresen elmossa a valóság és a virtuális világ közötti határokat. A beépített fényérzékelőkkel, mikrofonnal és kamerával felszerelt szemüvegeket,[21] egyes cégek kifejezetten tudományos orvosi célokra képzelik el a gyártását, a hétköznapi embereket célzó cégek inkább a játékok által nyújtott élmények kibővítését célozzák meg. Egyesek szerint 2022-re az okostelefonokat fel fogják már váltani az okos szem-

[21] Sony aims to outdo Google Glass with SmartEyeglass smart glasses, Forrás: https://www.theguardian.com/technology/2015/feb/18/sony-smarteyeglass-smart-glasses-google-glass, Utolsó letöltés ideje: 2018. 12. 12.

üvegek, amelyekkel már nem csak hallhatjuk egymást hívás közben, hanem látjuk magunk előtt a másik felet a szemüvegeken keresztül.

2. Okos eszközök a háztartásunkban, otthonunkban

Az okos háztartás, okos otthon fogalma szintén nehezen definiálható, de általánosan elfogadott jelentése az, hogy okos az a háztarás, amelyben a takarékosság-környezetvédelem-jövőtervezés szorosan egybe kapcsolódik. Más megközelítésből nézve, olyan otthon, amelyben a háztartási berendezéseinket mobiltelefonunkról vagy egyéb eszközről vezérelhetjük a világ bármely pontjáról[22]. Az intelligens otthon az interneten keresztül összekapcsolt eszközökkel rendelkezik és ezeken a felhasználók olyanokat állíthatnak be, mint például a hősmérséklet, világítás vagy a házimozihoz való hozzáférés.[23] Háztartási berendezéseinknél, gépinknél is manapság a fő szempont az energiatakarékosság, hatékonyság. Mivel ez a modern korban alapelvárássá válik, így a többi plusz funkció adja el a terméket. Nagyot fordult a kocka ezek körében is, hiszen már nem a gyártó határozza meg az igényeket, hanem maga a vásárló. A kényelmi funkciók beépítése határozza meg az adott termék népszerűségét.[24] Az okos háztartás csak akkor alakítható ki teljes egészében, ha már építéskor ez áll a középpontban.

Az intelligens háztartás kialakítása számos kihívás elé állítja a gyártókat. Alapvető feltétel a kialakításukban a kommunikáció, tehát a gépek közötti információcsere az ún. M2M (Machine to machine) adatáramlás. Az automatizálás feltétele, hogy a magukra hagyott eszközök megfelelő megoldással egymáshoz legyenek kapcsolva, tehát megvalósuljon az emberi közreműködés nélküli kommunikáció. Az M2M adatáramlás[25] javítja a működés hatékonyságát és a felhasznált energia mennyiségét, ezáltal környezetbarátabbá válik otthonunk. Hasznosíthatóvá válik a technológia a biztonság területén, riasztórendszerekben, a központi fűtés beállításánál, automata garázsajtónál, okos zárnál. Akár már a munkahelyünkön az utolsó munkaórában beállíthatjuk a mobilunkon keresztül, hogy mire hazaérünk milyen zene szóljon a tv-ben, hány fok legyen a lakásban vagy éppen hánykor nyíljon ki a garázsajtónk[26]. Ennek kapcsán rendkívül érdekes az a felvetés, hogy a családban ki is kezelje az automatizált berendezéseket? Rendkívül sokat elárul ez a család hierarchiai felépítéséről, hiszen az fogja kezelni a rendszereket, aki otthon is lényegében irányító szerepben van.[27] Az otthoni okos háztartási gépek rendkívül széles skálán mozognak, de egy okos robotgép nem veszélyezteti életünket, így megkíséreltem azokat kiválogatni, amelyek a biztonsághoz szorosabban kötődnek:

---

[22] HOFFMAN, DONNA L. – NOVAK, THOMAS: *Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things*. (August 20, 2015). Available at SSRN: https://ssrn.com/abstract=2648786, 18. p.

[23] Uo. 16. p.

[24] Uo. 18. p.

[25] NOTO LA DIEGA, GUIDO – WALDEN, Ian: i. m. 6. p.

[26] HOFFMAN, DONNA L. – NOVAK, THOMAS: *Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things.* (August 20, 2015). Available at SSRN: https://ssrn.com/abstract=2648786, 92. p.

[27] RICHARD HARPER (ed.): *Inside the smart home*. Springer Science and Business Media. London, 2003. 4. p.

a) Okos zár: A standard lakácskulcsok ideje meg van számlálva, legalábbis a Xiaomi cég szerint. A biometrikus ujjlenyomatok már a záraknál is megjelennek és az otthon biztonságát fogják újjá alakítani. A biztonsági zár feloldható egyébként bluetooth-on keresztül az okosmobilunkkal is, amely élő ujjlenyomat chip-et használ, itt egy belső helyen minden biztonsági adat tárolva van. 0,0005%-os hibaaránnyal működik a gyártó szerint. A DEFCON konferencián[28] viszont ezt hackerek cáfolták meg, mivel zárból 12-őt minden gond nélkül sikerült feltörniük. A konferencián előadást tartottak az ilyen zárak előnyeiről és hátrányairól is. Az okos zár működése hétköznapi emberek számára biztonságosabb, mint a normál kulcsos megoldás, viszont a hozzáértő hackerek számára ún. szabad prédák az ilyen lakások. A Google készített egy arcfelismerővel rendelkező csengőt a zárrendszerhez, amely felismeri a családot és barátokat, de ez számos privátszférához és adatvédelemhez kapcsolódó jogot sért.[29] Hozzá lehet adni a belépő közé vendégeket, akik betudnak jönni, illetve el is lehet a vendégeket távolítani a „vendéglistáról". A zár tárol vendéglistát, üzenetlistát visszamenőleg is, tehát megtekinthető hónapokra visszamenőleg kik jártak a lakásunkban, milyen eszközökkel csatlakozva. Veszélye abban rejlik, hogy a felhőből jön az információ az okostelefonokra, amellyel nyílik a zár, és a hackerek a felhő és a mobil közötti kapcsolatot könnyedén meg tudják támadni és feltörni az érkező jeleket.

b) Okos riasztórendszer: Az okos riasztórendszer képes a védelem mellett a fűtés és világítás beállítására, kapu kinyitására, redőny lehúzására mindezt egy okos telefonról vezérelve.[30] Helységenként riasztási zónákat állíthatunk be, amely alkalmas arra, hogy ha csak bizonyos helységet biztosítsunk. Kezelése működhet okostelefonon keresztül, de integrálható az okos otthonunk falra szerelhető kezelőfelületébe. Képes az üvegtörés érzékelésére ablakbetörés esetén. Gyakran felszerelnek egy pánik gombot, amellyel lehúzhatjuk a távolból a redőnyt, felkapcsolhatjuk a villanyt, vagy elviselhetetlen szirénázó hangot is képes kibocsátani. Képes jelenlét szimulációra, amellyel a ház úgy „viselkedik" mintha a lakója otthon tartózkodna, annak valódi jelenléte nélkül okos riasztórendszer felhasználó jogosultságokkal bír.[31] Megadhatjuk kik léphetnek a lakásba, ezzel egy-egy jogosultságot osztva nekik, de bizonyos személyeket ki is zárhatunk a ház egyes részeiből. Az intelligens riasztó és zár együtt képesek akár rabul is ejteni és bezárni a betörőt, ráhúzni a redőnyt és zárolni mindent, amíg értesítik ezalatt a hatóságokat a távfelügyeleti összekapcsoláson keresztül.

3. Okoseszközök a követlen környezetünkben

c) Okos autó: Térhódításuk szintén az Egyesült Államokból indul. A Google hatalmas projectet végez a vezető nélküli autók technológiájának megalkotására. A projektet

[28] Backdooring the Frontdoor, Forrás: https://www.youtube.com/watch?reload=9&v=MMB1CkZi6t4, Feltöltés ideje: 2016. 11. 23., Utolsó letöltés ideje: 2018. 09. 28.

[29] Google launches video doorbell with facial recognition in UK, Forrás: https://www.theguardian.com/technology/2018/may/31/nest-hello-google-launches-facial-recognition-data-doorbell-uk-privacy-concerns-amazon-ring, Utolsó letöltés ideje: 2018. 12. 06.

[30] HOFFMAN, DONNA L. – NOVAK, THOMAS i.m. 75. p.

[31] Intelligens riasztórendszer és okos riasztó távoli eléréssel, Forrás: https://incelor.com/intelligens-otthon-riasztorendszer-biztonsagtechnika-tavfelugyelet/, Utolsó letöltés: 2018. 09. 26.

jelenleg *Sebastian Thurn*[32] vezeti, aki a Google Street View társalapítója is egyben és az életét ennek kialakítására szentelte. Az ő személyének köszönhető, hogy Nevada államban 2012-óta törvény szabályozza a vezető nélküli autók jelenlétét a közúti közlekedésben.

d) Drón: napjaink egyik szinte teljesen új találmánya és egyben kérdéses jogi megítélés alá eső eszköze a pilóta nélküli légi jármű, azaz a drón. Ma már ezek jelentőségét és elterjedését nem lehet figyelmen kívül hagyni, így lehetetlen elkerülni, hogy szabályozás szülessen a használatukra, a biztonságunk és személyiségi jogaink megóvása érdekében.[33] Az Egyesült Királyságban egyszerűbb szabályokat követnek a hobbi drónreptetéssel kapcsolatosan, miszerint távolságokhoz van kötve a szabályozás például személyekhez 50 méternél közelebb nem lehet velük közelebb repülni, sűrűn beépített területeknél 150 méter az alsó korlát. A nem hobbi célra megalkotott drónoknál speciális engedélyek szükségesek. Németországban 2017-ben léptek életbe az új jogszabályok a drónokra vonatkozóan. Itt szintúgy súly és távolság kategorizálást használnak alapelgondolásként.[34]

4. Közösségi oldalak

Személyes adataink biztonsága és a magánszféránk vizsgálatakor kihagyhatatlan téma a közösségi oldalak működésének, használatának megértése. Nem véletlenül tekintenek a vállalatok, médiatartalom-szolgáltatók aranybányaként a közösségi oldalakra.

a) Facebook: Dolgozatomban főként a Facebook munkásságát emelném ki, nem véletlenül, hiszen az elmúlt évek egyik legnagyobb vívmánya és immáron a legnagyobb közösségi platformmá alakult át. Közel 2,27 milliárd felhasználója van[35] és ha ez így halad, akkor 2030-ra, amikor a Föld várhatóan eléri a 8,5 milliárdos lakosságszámot, a Facebooknak várhatóan 5 milliárd felhasználója lesz,[36] amely azt jelentené, hogy 10 emberből 6 rendszeresen használja. Azonban emellé számos veszély társul. Érdemes megvizsgálni a Facebook Adatkezelési Szabályzatát, ugyanis ebben tételesen fel is sorolják, melyek azok az adatok, amelyeket gyűjtenek a felhasználókról. Például, mely személyekkel vagyunk kapcsolatban, milyen csoportokhoz csatlakozunk, milyen tartalmakat kedvelünk, mikhez kommentelünk, vagy milyen tartalmakat osztunk meg. Ezeket az információkat arra használják fel, hogy személyre szabják az oldalt, és azok a hirdetések, tartalmak, képek, személyek jelenjenek meg, amelyek érdekelhetnek minket,

---

[32] THURN, SEBASTION: *The google driverless car* Forrás: https://www.ted.com/talks/sebastian_thrun_google_s_driverless_car/ transcript?source=googleplus&language=hu#t-88146, Utolsó letöltés ideje: 2018. 12. 06.

[33] CALO, RYAN: *The Drone as Privacy Catalyst* (December 12, 2011). Stanford Law Review Online. Vol. 64. 29–33. pp.

[34] SONNEWEND GYULA: *A drónok repülésének szabályozása hazai és nemzetközi viszonylatban*. Repüléstudományi Közlemények Folyóirat, Szakdolgozat és OTDK dolgozat, Szolnok 2018. Forrás: http://www.repulestudomany.hu/tdk/2018_Sonnewend_Gyula_TDK.pdf, Utolsó letöltés ideje: 2018. 09. 07.

[35] „Number of monthly active Facebook users wordwide as of 3rd quarter 2018" Forrás: The Statistics Portal, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/,Utolsó letöltés ideje: 2018. 11. 01.

[36] MARCO DELLA CAVA: *„Facebook in 2030? 5 billion users, says Zuck" USA today.* Feb 4, 2016. Forrás: https://eu.usatoday.com/story/tech/news/2016/02/04/facebook-2030-5-billion-users-says-zuck/79786688/, Utolsó letöltés: 2018. 12. 06.

vagy akit ismerhetünk. A Facebookba való belépéskor lehet az engedélyt megadni a Facebook számára a GPS adatokhoz, a kamerához, a hangfelvételhez és a fényképekhez való hozzáféréshez; gyűjti a mobil hálózatok adatait, amelyekre felcsatlakozunk, az eszközök típusát, az IP címet.[37] A hirdetők, alkalmazások fejlesztői a Facebook-on keresztül üzeneteket küldhetnek a felhasználóknak az okos hirdetéseken keresztül, amellyel „rááll" az oldal a felhasználó szokásaira és érdeklődési körére és ezáltal számára kedvező hirdetéseket ajánl fel. Számos fényképen bejelölhetjük a készítés földrajzi helyét, de ennél veszélyesebb az élő követés funkció használata, hiszen itt be kell kapcsolnunk a GPS-t és már meg is jelenik a Google térképen a tartózkodási helyünk, ahol a kikapcsolásig van lehetőség követni minket, de akár arra is, hogy csak pillanatnyi helyzetünket osszuk meg a világgal. Ezek alapján, ha bárki megszeretne bennünket találni, igazából nincsen nehéz dolga, jelentsen ez akár pozitív, akár negatív szándékot. Nagyon egyszerű, de annál inkább releváns példa, ha egy felhasználó a családi nyaralás képével jelentkezik be a Facebookon, akkor a betörő tudni fogja, hogy valószínűleg üres a lakás. Számos hiteltelen nyereményjátékkal is kecsegtetnek az oldalakon, amelyek még inkább csak a személyes adatok begyűjtésére szolgálnak, mint sem arra, hogy nyereményt szolgáltassanak. Ezekben begyűjtik az e-mail címeket, amelyekre később további hiteltelen információkat, vírusokat küldhetnek. Sajnos a fiatalok még nagyobb veszélyben vannak ezeken a platformokon, hiszen a sokszor helytelen és tudattalan használat következtében nyitott könyvek a kiberbűnözők számára.

b) Instagram: mára már az Instagram is világméretűvé fejlődött a közel 800 millió[38] felhasználójával. Számos hasonló biztonsági kockázatot hordoz magában, mint ahogyan a Facebook. Mivel az Instagram okos keresővel rendelkezik, így a felhasználók szokásaira, érdeklődési körére koncentrál és egy idő után már csak olyan képeket ad ki a keresője, amely a felhasználó igényeit teljes mértékben kiszolgálja. Az Instagram-on kialakult virtuális világ eredményeképpen a fiatalok elveszíthetik a racionális képet a világgal szemben támasztott képzeteik miatt.

Az okoseszközök tulajdonságainak, a lehetséges adatvédelmi kockázatok bemutatását követően áttérek az Európai Uniós szabályozásra. Ezt követően részletesen elemzem, hogy a szabályozás az okoseszközökre lebontva hogyan alkalmazható, vagy hogyan nem, továbbá, hogy milyen eszközök állnak rendelkezésre a szabályozás betartása és betartatása érdekében.

III. A Bizottság Munkája az Okoseszközök világában

Ebben az „okos" világban, amelyben élünk, szükség van arra, hogy a technológia gyümölcsei megfelelő jogi keretet kapjanak. Az Európai Unió intézményei igyekeznek egységben tartani a fejlődési szintet a szabályozási keretekkel, hiszen az információs és

[37] *A Facebook adatkezelési szabályzata.* Forrás: https://www.facebook.com/privacy/explanation/, Utolsó letöltés ideje: 2018. 10. 25.

[38] „Number of monthly active Intagramm users from January 2013 to June 2018". Forrás: https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/, Utolsó letöltés ideje: 2018. 11. 02.

kommunikációs technológiák (továbbiakban IKT) a termelékenység fokozódásához és növekedéséhez vezettek.

A fentiek érdekében az Európai Bizottság 2010 májusában bemutatta az *Európa 2020*[39] tervezetet. Ez nem más, mint egy akcióterv annak kapcsán, hogy hogyan zárkózzunk fel a korszak vívmányaihoz, illetve ezek népszerűsítését fogalmazza meg célkitűzésként 2010-2020 közötti időszakra vonatkozóan. A Bizottság hét kiemelt kezdeményezésének egyike a *Digitális Menetrend* nevet viseli.[40] „Célja általánosságban, hogy a nagy sebességű és szupergyors internetre és interoperábilis alkalmazásokra épülő egységes digitális piac révén fenntartható gazdasági és szociális előnyöket teremtsen." [41] A menetrend bemutatja azokat a területeket, ahol fejlődésre van szükség a válságból kilábalás kapcsán. Ezek a területek például az IKT, a termelékenység, a szén-dioxid kibocsátás, a foglalkoztatási arány, illetve ezek kapcsán olyan átalakulásokat kívánnak véghez vinni, amely a lakosság minél nagyobb digitalizálódásához vezet vagy vezethet.[42] A menetrend feladata legfőképp felvázolni azokat a gazdasági potenciálokat, amelyekhez az IKT hozzásegíthet. A Menetrend elsősorban a gazdaságra fókuszál, de olyan megoldásokkal szolgál, amelyek a hétköznapi emberek számára is kedvezőek lehetnek. Fontosnak tartja a hálózatok korszerű kiépítését[43], illetve említést tesz az 5G hálózat közeledtére[44]. 2020-ra digitális tartalmak és alkalmazások kizárólag a világhálón lesznek elérhetőek, hiszen már 250 millió európai használ internetet és minden európai polgár rendelkezik mobiltelefonnal. [45]

A Bizottság kiváló elméletet dolgozott ki arról, hogy egy digitális gazdaságot kellene létrehozni, amely önmagát működteti, erősíti. Ennek hasznosítása érdekében Európának komoly kihívásokkal kell szembe néznie, hiszen a felhasználók nem bíznak egy alig működő, bizonytalan világban, ahol azt látják, hogy egy távközlési szolgáltató is rendszeresen akadályokkal néz szembe, és nem képes folyamatosan ugyanazt a szintet bárhol biztosítani. Ezért érhető, hogy aggodalmat éreznek, hogy egy ilyen rendszer befolyásolja a munkahelyeket, a gazdasági érvényesülésben folytatott állandó versenyt. A Bizottság rávilágított arra, hogy Európa még nem rendelkezik 2010-ben azokkal az alapokkal, hogy képes legyen befogadni az IKT-t, és ennek elérését tűzte ki céljául 2020-ra.[46] A Menetrend vázolja és felismeri azokat a problémákat, amelyek miatt nem voltunk képesek idáig lépést tartani más kontinensekkel.[47] Rendkívül szétaprózódott a digitális piac[48] az EU-n belül, amelynek nincsenek megfelelő közösségi platformjai és

[39] A Bizottság közleménye. Európa 2020. Az intelligens, fenntartható és inkluzív növekedés stratégiája. COM (2010) 2020 végleges, Brüsszel, 2010. 3. 3. Forrás: http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf, Utolsó letöltés ideje: 2018. 12. 06.

[40] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, Az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az európai digitális menetrend. COM(2010)245 végleges, Brüsszel, 2010. 5. 19., Forrás: http://infoter.eu/attachment/0003/2807_com2010_0245hu01.pdf, Utolsó letöltés ideje: 2018. 12. 06.

[41] Az európai digitális menetrend, i.m. 3. p.

[42] Uo. 6. p.

[43] Uo. 7. p.

[44] Uo. 22. p.

[45] Uo. 4. p.

[46] Uo. 3. p.

[47] Uo. 5. p.

[48] Uo. 6. p.

garanciái. Az egyre elterjedtebb kiberbűnözéssel kapcsolatban az európai emberek bizalmukat vesztették a technológiákban.[49] A Bizottság ezért tűzte ki egyik fő céljául, hogy a társadalom bizalmát visszaszerezze olyan adatvédelmi rendelkezésekkel, amelyek lényegesen képesek visszaszorítani a bűnözést ezen a téren. A Bizottság vizsgálatai azt mutatják, hogy rendkívül kevés beruházás törekszik a megfelelő hálózat és infrastruktúra kialakítására,[50] és a fejlődésre vonatkozó kutatások sem feltétlen zárulnak sikerrel. Kifejezetten az előbb említett problémák megoldására hozták lére a Menetrendet.

A Menetrend területeket vázol, amelyek között első az egységes digitális piac.[51] Sajnos a sikeres internetes piacok nagy része nem európai találmány (Pl.: eBay, Amazon, Aliexpress). Ahhoz, hogy Európa is hasonló sikereket érjen el lényegi változtatásokra van szükség, főként arra, hogy ugyanolyan könnyű legyen az internetről is beszerezni bármit, mint azon kívül. Ennek megvalósulása érdekében a közös jogkezelő társaságok irányíthatóságát és átláthatóságát is hozzá kell igazítani a technológia fejlődéséhez. A könnyebb beszerezhetőség természetesen nem csorbíthatja a jogtulajdonosok érdekét, hiszen ők fejlesztették ki az adott terméket és az ő munkájuk eredménye, viszont ezáltal a termékeik még nagyobb célközönséghez el tudnak jutni, mint valaha. Ez a széles kínálat alapul szolgálhat az ún. kalózkodásra, amelynek megoldása és visszaszorítása az EU és a tagállamok közös feladata. A kalózkodás, mint kifejezés mára már egy újabb többletjelentéssel bővült a korábbihoz képest, ami olyan személy vagy egyéb szellemi tevékenységet jelent, aki vagy ami más szellemi tulajdonát teszi elérhetővé, a szerzői jogok megkerülésével.

A határokon átnyúló fizetési tranzakciók egyszerűsítése is a célkitűzések között szerepel. Az emberek 92%-a inkább a hazai kínálatból választ, mintsem más országokéból, így számos országon kívülre nyúló fizetési tranzakció hiúsul meg. Ez is jól mutatja mekkora fejlődésre van szükség jelen területen is. Véleményem szerint a világ nagyobb platformjai, mint például az Aliexpress is azért tudott sikeres lenni, mert a termékeket annyival olcsóbban adja, hogy az emberek úgy vannak vele, hogy inkább kockáztatnak, ilyen alacsony összegért nem akkora tétel, ha elbukják, megpróbálták, de ez nem azért van mert bíznának ebben a szolgáltatóban. A Bizottság *az Egységes Eurofizetési Térség (SEPA)*[52] mielőbbi megvalósítását is javasolja, amelyhez elengedhetetlen az emberek bizalmának megerősítése a digitális világban. Vizsgálata alapján az internetes vásárlások elkerülésének fő okai között magasan vezet a bizalomhiány és a személyes adatokkal való visszaéléstől való félelem, illetve a visszaküldés feltételeinek bizonytalansága.

A Menetrend további célkitűzése a nagy sebességű és bárhol elérhető internethálózat[53] mindenki számára elérhetővé tétele, amelyre a gazdaság növekedése érdekében van szükség. A Menetrend biztosítani kívánja, hogy 2020-ra mindenkinek legalább 30 mbps sebességű internethozzáférése legyen. A Bizottság álláspontja szerint nem szabad, hogy a digitális eszközök megértését befolyásolják a készségek (azok hiánya) és a szociális/anyagi háttér.[54] A „digitális kompetenciának" már az alapműveltség részévé kell

[49] Uo.
[50] Uo.
[51] Uo. 8. p.
[52] Uo. 12. p. 2.1.2. pont.
[53] Uo. 21. p. 2.4. pont.
[54] Uo. 28. p. 2.6. pont.

válnia. A 0-25 éves korosztály már ebben a világban született és nőtt fel, és számukra ez már nem tanulás kérdése, hiszen folyamatosan az életük részévé vált. Az idősebb korosztálynak azonban ebbe bele kell tanulnia ahhoz, hogy a digitális egységes piac meg tudjon valósulni.[55]

A fent említett területeken számos eredményt értek már el, és rengeteg kapcsolódó irányelvet bocsátottak ki a Menetrend végrehajtása érdekében. Így a *szerzői jogok védelme* még inkább előtérbe került a szerzői jogokról szóló „Javaslat Az Európai Tanács és Parlament rendelete a digitális egységes piacon a szerzői jogról"[56] kibocsátásának kapcsán. A gyakorlatban a közösségi platformok, mint például a Youtube, Facebook vizsgálják a feltöltött tartalmakat, és amennyiben észlelik, hogy a feltöltött videóban aláfestésként más zenéjét használják, abban a pillanatban törlik a videót, vagy teljesen elveszik a zenei aláfestést alóla. Csak olyan videót tölthetünk fel, amely a saját zenénk, vagy a zene használatához engedélyünk van.[57] A Youtube felületén van egy űrlap, amely kitöltésével jelezhetjük az adminnak/adminoknak, hogy megsértették a szerzői jogunkat.

Az *Egységes Euró Fizetési Övezetről szóló rendelete*[58] (Single Euro Payments Area-SEPA), amely támogatja az egységes fizetési övezet létrehozását.[59] A SEPA fizetési mód az Európai Unión belül „belföldi fizetésnek" tekintendő. Az euro-övezeti tagállamoknak 2014. február 1-jétől kötelező volt áttérni az ún. SEPA fizetési módra. Ennek célja a hatékony, gyors és biztonságos fizetés. Ahhoz, hogy lehetséges legyen ilyen módon pénzforgalmat bonyolítani, mint az átutaló félnek, mind a kedvezményezettnek szükséges, hogy a saját bankja állítson ki, egy ún. IBAN kódot[60]. A pénzforgalom kapcsán fontos még megemlíteni az ún. HÉA irányelvet[61], amely egyenértékűvé teszi az elektronikus számlát a papír formátumúval.

A Bizottság kiadott egy számítógépes bűnözés elleni küzdelemre vonatkozó általános politika meghatározását szolgáló közleményt,[62] amelynek célja, hogy egy egységes politikát mutasson fel a számítógépes bűnözés elleni összehangoltsághoz. Az ehhez szükséges célkitűzések között szerepel az Europol és egyéb szervek erre szolgáló osztályainak kibővítésére, egy Uniós számítógépes bűnüldözési platform létrehozása, mérőszámok kidolgozása a bűncselekmények mérése kapcsán, illetve uniós figyelemfelhívás a veszélyekre.

A „digitális tudás" fejlesztése a hétköznapi emberek között és a kohéziók csökkentése érdekében létrehozták az *Európai strukturális és beruházási alapok*[63] 2014-2020-ig

---

[55] DEMIRIS, G. – RANTZ, M. – AUD, M. – MAREK, K. – TYRER, H. – SKUBIC, M. – HUSSAM, A.: *Older adults' attitudes towards and perceptions of 'smart home'technologies: a pilot study*. Med Inform Internet Med. 2004 June 29(2): 87–94. pp.

[56] COM/2016/0593 final - 2016/0280 (COD).

[57] Youtube: Közösségi irányelvek, Biztonsági eszközök és erőforrások, Bejelentés és jogérvényesítés. Forrás: https://www.youtube.com/intl/hu/yt/about/policies/#community-guidelines, Utolsó letöltés: 2018.10.26.

[58] Az Európai Parlament és a Tanács 260/2012/EU rendelete (2012. március 14.) az euroátutalások és -beszedések technikai és üzleti követelményeinek megállapításáról és a 924/2009/EK rendelet módosításáról.

[59] SEPA: Európai Gazdasági Térség területén az euróban történő fizetések küldését és fogadását szolgáló, a fizetéseket egységes szabványok és szabályok alkalmazásával lebonyolító, közös európai fizetési eszköztár.

[60] IBAN kód: Nemzetközi bankszámlaszám.

[61] *Uo.* 13. p. 2.1.2.pont.

[62] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának: A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé. COM(2007) 267 végleges, 2007.5.22.

[63] Európai strukturális és beruházási alapok (Az Európai Parlament és a Tanács 1303/2013/EU rendelete (2013. december 17.) az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alapra, a Kohéziós

tartó irányelvet, amelyben kifejezetten kiemelik, hogy az Európai Unió feladata törekedni arra, hogy a gazdasági és szociális egyenlőtlenségeket csökkentse. Az öt fő gazdasági alap közösen támogatja az összes tagállam gazdasági fejlődését az Európai Unió céljaival összhangban. Az öt fő alap a következő: Európai Regionális Fejlesztési Alap, Európai Szociális Alap, Kohéziós Alap, Európai Mezőgazdasági Vidékfejlesztési Alap, és az Európai Halászati Alap.

Szintén a Menetrend eredményeként jöhetett létre 2015-ben a Bizottság által a *„Digitális Egységes Piac"*[64] gondolata, miszerint elő kell segíteni az internetben rejlő lehetőségek kiaknázását nehezítő körülmények felszámolását. Az ehhez szükséges tisztességes, nyílt és biztonságos digitális környezet biztosítása érdekében a Bizottság az alábbi három pillérre építette a digitális egységes piaci stratégiát: a) a fogyasztók és vállalatok könnyebb hozzáférése a digitális termékekhez és szolgáltatásokhoz Európa-szerte; b) megfelelő körülmények teremtése a digitális hálózatok és szolgáltatások számára, hogy felvirágozzanak, és c) maximalizálják a digitális gazdaság növekedési potenciálját. Európa digitális, hiszen közel 360 millió európairól beszélhetünk, akik internetet használnak nap mint nap a tanuláshoz, a munkájukhoz, vásárláshoz és eladáshoz. A digitalizáció számos új lehetőséget kínál a technológia területén, az orvostudományban, összekapcsolt közlekedésben, amelyek megvalósításául szolgál a Digitális Egységes Piac (Digital Single Market). Ennek keretében számos, számunkra is nagyon hasznos fejlődés valósult meg, többek között, hogy 2017-ben eltörölték a roaming többletdíjakat.

A digitális fejlődés nem fog megállni, ezért egyre több és több intézkedésre van szükség a biztonságunk megóvása érdekében és a fejlődés biztosításaképpen, amely ahhoz szükséges, hogy a digitális jövő élhető legyen és megakadályozzák a kiber incidenseket. Ahogy mondani szokták, az „adat a 21. század olaja" [65] a gazdaságban, éppen ezért van arra szükség, hogy kiemelt védelemben részesüljenek. Erre szolgál az Európai Unió Általános Adatvédelmi Rendelete (a továbbiakban: GDPR), amelyet a következő részben kívánok elemezni. Elsőként magát a rendeletet, annak tartalmát, így rávilágítva a gyakorlati jelentőségére, amely szorosan kapcsolódik a biztonság kérdéséhez.

IV. A GDPR

A GDPR[66] 2018. május 25-től hatályos az Európai Unió tagállamaiban, egyben hatályon kívül helyezi a korábbi 95/46/EK adatvédelmi irányelvet. 2009-ben indult az Európai Unió, illetve az Európai Bizottság kezdeményezésére az adatvédelem reformja. A ren-

Alapra, az Európai Mezőgazdasági Vidékfejlesztési Alapra és az Európai Tengerügyi és Halászati Alapra vonatkozó közös rendelkezések megállapításáról, az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alapra és a Kohéziós Alapra és az Európai Tengerügyi és Halászati Alapra vonatkozó általános rendelkezések megállapításáról és az 1083/2006/EK tanácsi rendelet hatályon kívül helyezéséről.

[64] A digitális egységes piaci stratégia megvalósítása terén elért elért eredmények áttekintése (videó) Forrás: https://ec.europa.eu/commission/priorities/digital-single-market_hu, Utolsó letöltés: 2018. 09. 01.

[65] *Idézet Peter Sondergaard-tól.* In: Hansen, Marit - Kosta, Eleni – Nai-Fovino, Igor – Fischer-Hübner, Simone (eds.): Privacy and Identity Management. The Smart Revolution. Springer, 2018. 78. p.

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

delet végső szövegét 2016-ban fogadta el az Európai Parlament és a Tanács.[67] Nem szeretném dolgozatomban megismételni a rendelet tartalmát, hanem röviden be kívánom mutatni a témám szempontjából releváns rendelkezéseit és ezeket elemzem, majd áttérek a gyakorlati megvalósulásra példákkal szemléltetve.

A GDPR nem más, mint az Európai Parlament és Tanács együttes 2016/679 számú rendelete. A rendelet Preambuluma kimondja, hogy a személyes adatok védelme egy alapjog, tehát emiatt kiemelten fontos ezt védeni.[68] Ezzel az alapjogok is fejlődést mutatnak, hiszen manapság már nem csak a nagy klasszikus alapjogokat tekinthetjük kiemelt védelem alatt állónak. Ebben a digitális világban szerintem kiemelten fontos a privát adataink biztonsága, mivel, ha ezek az adatok kikerülnek a személyes kezelésünk alól, akkor nagyon súlyos károkat okozhatnak ezáltal, amely kihatással lehet az egész életünkre, emberi méltóságunkra. Viszont az adatok védelme nem abszolút jog, hiszen a szükséges mértékben ez korlátozható.

E rendelet előtt nem volt egységes a személyes adatok kezelésének szabályozása, éppen ezért az Európai Unió a teljes jogegységesítést tűzte ki célul ezen a téren a tagállamok között. A gyors technológiai változások új kihívásokat hoztak létre a jogalkotóval szemben, hiszen valamiféle jogi keretet kell, egy olyan jelenségnek szabni, amely egyik napról a másikra is rengeteget képes változni. A „természetes személyek következetes és magas szintű védelmének biztosítása és a személyes adatok Unión belüli áramlása előtti akadályok elhárítása érdekében, a természetes személyeknek az ilyen adatok kezelésével összefüggésben fennálló jogait és szabadságait, minden tagállamban azonos szintű védelemben kell részesíteni.”[69] A GDPR meghatározza az alkalmazó személyek és hatóságok körét és a kivételeket is, amelyekre e rendelet nem alkalmazható, így az otthoni felhasználás körében végzett tevékenységre, nemzetbiztonsági kérdéskörben, vagy bűncselekmények felderítése körében, nyomozásnál, büntetési szankciók végrehajtásánál. Lefektet számos alapfogalmat ezzel kapcsolatosan és kifejti az adatkezelés célját és az adatkezelés fontos alapelveit:[70]

- az adatkezelés legyen jogszerű, tisztességes, átlátható
- egyértelmű és jogszerű célból történjen
- adattakarékos és pontos gyűjtés
- „korlátozott tárolhatóság” megvalósuljon
- integritás és bizalmas jelleg fennálljon
- és elszámoltatható legyen.

A fentieken túl meghatározza az adatalanyjogait is:[71]
- Hozzáférés joga
- Helyesbítéshez való jog
- Törléshez való jog („Elfeledtetéshez való jog”)

[67] VOIGT, PAUL – VON DEM BUSSCHE, AXEL: *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer, 2017. 2. p.
[68] GDPR 1. p. 1. pont.
[69] GDPR 2. p. 10. pont.
[70] GDPR II. fejezet 5. cikk.
[71] GDPR III. fejezet 11. cikk.

- Adatkezelés korlátozásához való jog
- Adathordozhatósághoz való jog
- Tiltakozáshoz való jog (+ Automatizált döntés elleni tiltakozáshoz való jog)
- Tiltakozás közvetlen üzletszerzés ellen

Az adatkezelő számára is számos kötelezettséget fogalmaz meg a rendelet. Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket kell, hogy végrehajtson annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.[72]

V. GDPR elemzése

Dolgozatom ezen fejezetében a GDPR mindennapi életben való jelentőségére térek ki, azaz arra, hogyan alkalmazzák a felek a gyakorlatban a rendelkezéseit.

A GDPR hatálya nem csak azokra a vállalatokra terjed ki, akik az EU-ban rendelkeznek székhellyel, telephellyel, hanem azokra is, akik az EU-n kívül vannak, tevékenységüket azonban az Európai Unió területén végzik, európai ügyfeleknek nyújtanak szolgáltatásokat. A rendelet kiterjed az IoT-re, azaz az Internet of Things-re, vagyis a Dolgok Internetére is. Itt már sokkal inkább az a kérdés, hogyan képesek az üzemeltetők megfelelni a rendelet követelményeinek és milyen eszközökkel fogják megvalósítani. Az IoT rohamos közeledte miatt éppen időben keletkezett a GDPR, mivel segít felhívni az internetes közönség figyelmét a tudatos és kellőképpen biztonságos adatmegosztás és adatkezelés fontosságára. Az IoT rendszerek önállóan kommunikáló eszközökből (things) állnak, amelyek képesek adatokat szolgáltatni környezetükről és azt továbbítani egy felhőbe, vagyis egy távoli szerverre.[73] A felhő formájú adattárolásban azonban nehézkes az adattárolás megfelelő biztonságának igazolása. A készülék és az adatok közötti kölcsönhatás nem egyszerű, számos szereplő között bonyolódik le és a GDPR-nak való megfelelés biztosítása az egész láncolatra kiterjed.[74] Ezekben az esetekben az a fő kérdés, hogy még is hogyan tudna valaki a felhő alapú rendszerekhez hozzájárulni? Az adatkezeléshez való hozzájárulás annyira széles skálán mozoghat, hogy teljes mértékben attól függ, hogyan használjuk és mire, ezért rendkívül nehéz rá egy általános megoldást kitalálni.

---

[72] GDPR IV. fejezet 24. cikk.

[73] ATTILA KERTESZ – SZILVIA VARADI: *Legal Aspects of Data Protection in Cloud Federations.* In book: "Security, Privacy and Trust in Cloud Systems", S. Nepal and M. Pathan (Eds.), Springer, Signals & Communication. 2013, 2013. 433–455. pp.

[74] SZ. VARADI – G G, VARKONYI – A, KERTESZ: *Law and IoT: How to see things clearly in the Fog.* In: Institute, of Electrical and Electronics Engineers (szerk.): Third International Conference on Fog and Mobile Edge Computing (FMEC), 2018. 233–238. pp.

1. Hozzájárulás az IoT rendszerek működéséhez

Nem egyszerű egy olyan összekapcsolt hálózat egyes elemeiben megvalósuló adatkezeléshez hozzájárulni, amelyeket lényegében még csak nem is látunk. Értendő ezalatt például az, hogy az okos riasztórendszer valamilyen incidens észlelése esetén azonnali értesítést küld az azzal összekapcsolt mobilra.

Először is ebben az esetben fontos pontosan meghatározni azt, hogy mi is minősül *személyes adatnak*. Ez alatt értendő: az azonosított vagy azonosítható természetes személyre vonatkozó bármely információ. Azonosítottnak minősül az a természetes személy, aki közvetett vagy közvetlen módon, különösen valamely azonosító, például név,[75] szám, helymeghatározó adat, online azonosító vagy természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságra vonatkozó egy vagy több tényező alapján beazonosítható.[76] Másrészről az *adatkezelő* definíciója is elengedhetetlen, hiszen mindenki adatkezelőnek minősül, aki bármilyen személyes adattal kapcsolatos adatkezelést végez.

A fentieken túlmenően tisztázni kell a *hozzájárulás*t. Az érintett hozzájárulása az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatásán alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őr érintő adatok kezeléséhez.[77] A korábbi irányelvhez képest ez nagy változás, hiszen korábban elegendő volt a hallgatás is, azonban most már az adatalanynak tevőleges beleegyezését kell adnia. Ahhoz, hogy ezek megfelelően megvalósuljanak, az adatkezelőknek is be kell bizonyos szabályokat tartaniuk. Összehangoltan kell működniük az EU-n belül és egy tisztességes, átlátható, jogszerű tájékoztatást kell adniuk az érintetteknek arról, hogy pontosan milyen adatokat gyűjtenek róluk, mi az adatkezelés jogcíme és jogi alapja, milyen célból használják fel az adatokat, illetve kiknek adhatják ezeket pontosan ki és milyen célra.[78]

Az IoT rendszereknél véleményem szerint maga az IoT eszközök és rendszerek megvásárlása, regisztrációja, majd használata egyfajta beleegyezés ezekbe a folyamatokba, hiszen lehetetlen minden egyes apró lépéshez a hozzájárulásunkat adni ezeken felül. Aki vásárol egy Iphone-t például, annak létre kell hoznia kötelezően egy Icloud fiókot, hogy az egész eszközt működtetni tudja, tehát hozzájárulását kell adnia az összes funkció alkalmazásához. Amennyiben ezt nem teszi meg, akkor így nem is tudja használni. Ilyen alapon működik például a Find my Iphone funkció is, ennek a segítségével találhatjuk meg, vagy mérhetjük be a mobiltelefonunkat. Már a regisztrációval beleegyezünk abba, hogy ezt használni fogjuk, szerintem nem szükséges még ezt követően minden egyes folyamatnál külön hozzájárulásunkat adni akkor, ha az adatkezelő megfelelő tájékoztatást adott nekünk, hogy mire használja majd az adatainkat, illetve ennek során betartja a személyes adatok védelmére vonatkozó előírásokat. Az első használat előtt az okostelefon is például a galéria megnyitásakor rákérdez, hogy beleegyezünk-e

[75] A korábbi irányelvben nem szerepelt nevesítve az, hogy a név személyes adatok köréhez tartozna.
[76] GDPR 4. cikk. Fogalommeghatározások 1. pont.
[77] GDPR 4. cikk. Fogalommeghatározások 11. pont.
[78] GDPR 7. p. Preambulum 39. pont.

abba, hogy az Iphone hozzáférjen a képeinkhez, médiatartalmainkhoz, hangfájlokhoz, de ezt követően már nem szükséges megkérdeznie minden egyes file esetében.

Ugyanakkor a fenti technológiák átláthatatlan mivolta miatt, annak megoldásaként született meg az ún. Privacy by design, más néven a data protection by design[79] (magyarul: beépített adatvédelem) irányvonal és módszer, amely konkrétan alapelvként tekint az adatvédelemre.[80] Dolgozatomban korábban is utaltam ennek fontosságára, hiszen ezek megsértése vagy a személyes adatok kikerülése a világba éppen akkora sérelmet tud okozni, mint bármilyen más generációs alapjog megsértése. Az irányvonal célja, hogy olyan rendszereket alkossanak, hozzanak létre, amelyek már kezdetüktől fogva képesek legyenek megvédeni minket. Úgy vannak kialakítva, hogy „beléjük van építve" az adatvédelem, és nem csak utólag formálisan korrekciózzák őket, mint például egy böngészőbe épített süti tájékoztató. Ezen megoldás alkalmazása az IoT rendszerek kialakításánál is rendkívüli szerepet játszhatna, hiszen olyan megoldást nyújtana a problémára, amely magából a rendszerből származik és nem is lenne szükség ahhoz, hogy külön hozzájáruljunk ennek a bizonyos elemeihez.

Másik különleges rokon ágazata az ún. Privacy by default, vagy data protection by default (magyarul: alapértelmezett adatvédelem).[81] Lényege az, hogy a személyes adatok feldolgozására, kezelésére csak kifejezetten, az adatalany kérésére kerülhet sor. Az adatkezelők megfelelő hozzáállása kell ahhoz, hogy minden körülmények között – üzleti érdekeiket is olyakor félre téve – figyelembe vegyék az adatvédelmi szempontokat és ennek megfelelően járnak el.[82]

A GDPR foglalkozik az online azonosítókkal, amelyek szintén köthetőek az IoT rendszeréhez is, hiszen a Dolgok Internetének működésének alapjául szolgálnak a természetes személyekhez köthető eszközök igénybevétele, mivel ezek nélkül a Dolgok Internete sem állna össze. A természetes személyekkel összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és a protokollok online azonosítói, mint például az IP-cím, a cookie azonosítók, vagy a rádiófrekvenciás azonosítók.[83] Az IP-cím egy olyan számsorozat, mellyel az internetre fellépő felhasználók számítógépei egyértelműen azonosíthatóak. Az IP címek segítségével akár földrajzilag is lokalizálható az adott IP-címet használó látogató. Megmutatja mindezek mellett az operációs rendszer pontos típusát és a böngésző típusát is. Ezek által olyan nyomok keletkezhetnek, amelyeket más adatokkal összekapcsolva akár a természetes személy profiljának létrehozására vagy akár beazonosítására is képessé válik az eszköz. Egyértelműen ezek az eljárások sértik a személyes adatok kezelését. Az IoT-vel kapcsolatosan felmerül az eszközök valós idejű tárgyi megfigyelése is, amely ritkán ugyan, de megvalósulhat. Ezekre hozták létre az ún. *Managed Security Services*, azaz Irányított Biztonsági Szolgáltatásokat, amelyek egyelőre még csak a nagyobb vállalatok IoT rendszereit követik

[79] GDPR Preambulum 78. pont. 25. cikk.
[80] European Union Agency for Network and Information Security (ENISA): Privacy by design. Forrás: https://www.enisa.europa.eu/topics/data-protection/privacy-by-design, Utolsó letöltés ideje: 2018. 08. 27.
[81] GDPR Preambulum 78. pont. 25. cikk.
[82] Lambert, Paul: Understanding the New European Data Protection Rules. CRC Press, Taylor and Francis Group 2018. e-book; Nemzeti Adatvédelmi és Információszabadság Hatóság adatvédelmi értelmező szótár, Forrás: https://www.naih.hu/adatvedelmi-szotar.html, Utolsó letöltés ideje: 2018. 10. 24.
[83] GDPR Preambulum 30. pont.

nyomon és tartják biztonságban, de hamarosan el fog terjedni a természetes személyek körében is.[84]

2. A weboldalak helyzete a GDPR hatályba lépését követően

A weboldalak szerkesztőinek is követnie kell a GDPR rendelkezéseit az alábbi szempontok szerint: amennyiben a honlapon csak Google Analytics kerül alkalmazásra és más módon nem gyűjt személyes adatokat, abban az esetben nem szükséges a honlappal semmit tenni a GDPR-nak megfelelés tükrében. Azonban, ha az oldal ezen kívül használ Google Adwords, Facebook vagy más külső oldalról beépülő megoldást,[85] amely során külső cégek gyűjtenek adatokat az adott weblapon böngésző felhasználókról, akkor a weboldalaknak eleget kell tenni a GDPR által előírt kötelező lépéseknek, amelyeket az alábbi megoldásokkal oldottak meg:

a) A sütik

A HTTP-süti (továbbiakban: süti, angolul: cookie) is hasonló működési elven alapul. A süti nem más, mint egy információcsomag, amelyet a szerver küld a webböngészőnek, majd a böngésző visszaküldi a szervernek, minden egyes böngészés alkalmával. A sütiket maga a webszerver hozza létre elkülönítve a gépen egy erre a célra szolgáló mappába. A sütik célja, hogy összekapcsolja a felhasználó aktuális látogatását a korábbiakkal kizárólag a saját tartalma tekintetében. Ezáltal lehetőség nyílik arra, hogy a látogató keresések pontosítása, kiegészítése, így személyre szabott kiszolgálás megvalósuljon. Európai adatvédelmi szakértők egy csoportja szerint már nem elegendő a sütik letiltása, hanem külön ehhez való hozzájárulást tesznek szükségessé, amelyet előzetesen kell megtenni, még a honlap megtekintését megelőzően.[86] A weboldalakon kétféle változatban van jelen többnyire. Az első, ahol nem ajánl fel választási lehetőséget a süti fajták között, hanem egyféle lehetőséget kínál fel, amelyet vagy elfogadunk, vagy nem. Ez általában arról szól tájékoztató jelleggel, hogy a weboldal sütiket használ az optimális működése érdekében. Általában úgy vannak kialakítva, hogy amíg nem fogadjuk el, addig a szöveg láthatósága valamelyest korlátozva van. Második fajta kialakítás számomra sokkal jövőbe mutató kialakítással bír, hiszen felajánlja a sütik között a választási lehetőséget. Háromfelé bontja a sütiket: 1. szükséges süti, amely az oldal megfelelő működéséhez elengedhetetlen; 2. a funkcionális süti, amely az érdeklődési körünknek megfelelő tartalmat biztosít; 3. a leginkább személyre szabott kategória: a kényelmi süti, amely az oldal használatát elemezve személyre szóló tartalmakat és hirdetéseket jelenít

[84] ABOLHASSAN, FERRI (ed.): *Cyber Security. Simply. Make it Happen: Leveraging Digitization Through IT security.* Springer 2017, 65. p.

[85] Voigt, Paul – von dem Bussche, Axel: i. m. 55. p.; A GDPR megfelelésről-amit mindenképpen meg kell tenni egy weblap tulajdonosnak. Forrás: http://devsolution.hu/a-gdpr-megfelelesrol-amit-mindenkeppen-meg-kell-tenni-egy-weblap-tulajdonosnak/, Utolsó letöltés ideje: 2018.02.09.

[86] GUTWIRTH, SERGE – LEENES, RONALD – DE HERT, PAUL (eds.): *Reforming European Data Protection Law.* Springer. New York – London, 2015. 40. p.

meg vagy küld a felhasználónak.[87] Ezeket az elemzéseket felhasználva fejlesztik tovább az oldalt a felhasználók igényeire törekedve, azt kihasználva.

b) Az adatkezelési tájékoztató

A weboldalak másik megoldása a GDPR-nak való megfelelés megoldásával kapcsolatosan, hogy felkerültek az adatkezelési tájékoztatók a weboldalakra. Ezekben kötelezettséget vállalnak a fejlesztők arra nézve, hogy a tevékenységükkel kapcsolatos minden adatkezelés megfelel az ezen szabályzatban és hatályos jogszabályokban meghatározott elvárásoknak. Fel kell tüntetniük a kezelt és gyűjtött személyes adatok körét, célját, jogcímét és az időtartamát. Amennyiben a weboldal rendelkezik mobilalkalmazással, akkor erre kiterjedő pontot is meg kell fogalmazni a tájékoztatóban. Meg kell jelölni az összes adatfeldolgozót, beleértve azokat, akik az oldalakról gyűjtenek információkat és azokat is akik a hírleveleket küldik. Szót kell ejteni arról, hogy a szerver mely tevékenységeket naplózza, milyen időközként és ezt mennyi ideig tárolja. Tartalmaznia kell a honlap süti kezelését és annak szabályait, működését. Meg kell jeleníteni benne a telefonos/email/személyes elérhetőségeket, illetve, ha van ügyfélszolgálat, akkor annak az elérhetőség. Ki kell emelni minden ügyfélszolgálatnál, hogy ha a hívások rögzítve vannak. Személyes adatok tárolásának a módja, adatok biztonságának kifejtése is fontos elem. Végezetül tartalmaznia kell az adatkezelő adatait, elérhetőségét, illetve a személyes adatok megsértése esetén a felhasználókra vonatkozó jogorvoslati lehetőségek köré, mindezt érthető és tömör módon.

Az email-marketing is elérhető számos weboldalon keresztül. Ahhoz, hogy személyre szóló email-t kapjunk, először fel kell iratkozni a hírlevél feliratkozó űrlapra, amelynél hozzá kell járulni előzetesen a személyes adatkezeléshez, illetve, hogy szabad akaratából történt. A felhasználóknak be kell jelölni, hogy tudomásul vette és elfogadta az adatvédelmi feltételeket. Biztosítaniuk kell az utólagos leiratkozás lehetőségét is a weboldal fejlesztőinek, abban az esetben, ha a felhasználó már nem szeretné igénybe venni a szolgáltatást.[88] Megvalósul az adattakarékosság elve, hiszen ezeken az űrlapokon csak olyan adatokat szükséges bekérni, amelyek feltétlenül szükségesek ahhoz, hogy az email-marketing működni tudjon, ezért például nem kérdhetnek be telefonszámot, lakcímet. A hozzájárulások nem csak konkrétan a honlapon történhetnek meg, hanem az egyes közösségi portálokra beágyazott ún. „lead ad" hirdetésekkel. Amennyiben valaki online vásárol, abban az esetben a személyes adatok kezeléséhez hozzá kell járulnia, de felajánlja szintén az email-marketing lehetőséget is, amelyet nem kötelező elfogadni.

Véleményem szerint a GDPR rendelkezései a weboldalak tekintetében megvalósulnak, hiszen minden oldalnak rendelkeznie kell adatvédelmi tájékoztatóval és sütivel, hiszen amennyiben nem valósul meg, abban az esetben komoly bírsággal kell számolniuk, így szabálykerülő megoldásra nincs lehetőség. Probléma adódhat abban az esetben, amikor a felhasználók ezeket nem olvassák el. Ennek kiküszöbölésére a weboldalak fejlesztői olyan megoldásokat alkalmaznak, mint például a felhasználóknak kifejezetten le kell görgetni az adott oldal aljára, kipipálni az egyetértésre vonatkozó rubrikát, majd

[87] Uo.
[88] GUTWIRTH, SERGE – LEENES, RONALD – DE HERT, PAUL (eds.): i. m. 40. p.

bezárni. Amennyiben valaki ezek után sem olvassa el, önhibának tekintendő számomra, hiszen ennél egyértelműbb módon nem tudják a felhasználó szeme elé tárni az adatvédelmi tájékoztatót. Számos jogorvoslati fórum áll a felhasználók rendelkezésére, hogy adataikat megvédjék, és az adatkezelőkkel szemben kiszabható bírság is rendkívül magas. A bírság összege ugyanis az éves bevétel meghatározott százalékában is meghatározható, így kellő motiváció arra, hogy betartsák a rájuk vonatkozó rendelkezéseket. Például nemrégiben a brit adatvédelmi hatóság, a kiszabható legmagasabb büntetést szabta ki a Facebookra, 500 ezer fontra (182,5 millió forint) bírságolta meg a személyes adatok kezelésére vonatkozó szabályok be nem tartása végett. A dolgozat írásának idején aktuális továbbá Ausztria esete, ahol szintúgy jelentős összegű, mintegy 3800 eurós bírságot szabtak ki.[89]

3. A GDPR megjelenése az okoseszközeink vonatkozásában

Az okoseszközökre áttérve számos alkalmazást használunk feltelepítve a mobiltelefonunkra, okosóránkra. Ezek vonatkozásában a GDPR a rátelepített alkalmazások tekintetében jöhet szóba. Nagy részük a közösségi portálok mobil applikációi (pl.: Facebook, Instagram, Messenger), de van rátelepített böngésző, térkép, hangfelvevő, felhő, számos webhely mobilra tölthető applikációja, amelyekre szintúgy vonatkozik a GDPR rendelkezése, hiszen a rendelet vonatkozik minden olyan nem EU-s székhelyű vállalkozásra is,[90] amelyek az uniós tagállamok állampolgárainak adatait kezelik. Számos problémát vethet fel az, hogy ha csak akkor használhatjuk az alkalmazásokat, ha mindenhez hozzájárulásunkat adjuk. Az lenne a helyes megoldás álláspontom szerint, ha attól függetlenül, hogy hozzájárul-e az érintett az adatai kezeléséhez, tudná használni az adott alkalmazást, hiszen e célból lett létrehozva. Ezeken kívül szabadon dönthessen arról, hogy szeretné-e, hogy bizonyos funkciók leginkább az ő kényelmét szolgálják, és ezáltal adatokat gyűjtsenek róla, vagy sem. Amennyiben ezt nem szeretné a felhasználó, akkor meglátásom szerint a megoldás az lehetne, ha egy „alap" módban használhatná az adott felületet.

Véleményem szerint a közösségi oldalak kezelőinek volt az egyik legnagyobb feladat felkészülni a rendelet hatályba lépésére, hiszen több millió ember adatát kezelik a világon. Számos újítást vezetett be ennek kapcsán a Facebook a GDPR hatályba lépése óta. Többek között kialakított a Facebook felületen megnyitható új fület, amelyek az adatvédelmi beállításokra vonatkoznak. Itt beállíthatjuk, ki láthatja a saját tevékenységünket vagy konkrét személyeket is kizárhatunk, illetve másrészről azt is be tudjuk itt állítani, hogy velünk miként vehetik fel a kapcsolatot, miként kereshetnek meg. Megtekinthető külön a Facebook Cookie szabályzata is, amely mindenki számára elérhető. Garanciát vállal arra, hogy csak olyan hirdetéseket jelentet meg, amelyekhez a felhasználók előzetesen itt, vagy esetlegesen más honlapokon hozzájárultak, hiszen a Facebook adatkezelőnek és adatfeldolgozónak is tekinti saját magát. Ezt azonban a Facebook, Instagram, Whatsapp összekapcsolása időként ki akarja kerülni. Hiába külön alkalmazá-

[89] Austria announces first GDPR fine. Iapp, The world's largest global information privacy community, Forrás: https://iapp.org/news/a/austria-announces-first-gdpr-fine/ ,Utolsó letöltés ideje: 2018. 11. 01.
[90] GDPR Preambulum (23) bekezdés.

sok, és külön-külön kellene minden egyes felületen hozzájárulni az adatkezeléshez, mégis sokszor keveredik a három alkalmazás. Ebben az esetben vonatkozik rá a GDPR (32) Preambulum bekezdése és a 7. cikk, amelyek értelmében adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli- ideértve elektronikus úton tett-, vagy a szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez.[91]

A Facebookra is vonatkozik az adattakarékosság elve, tehát csak azokat a személyes adatokat gyűjtheti, amelyek feltétlenül szükségesek ahhoz, az oldal működni tudjon, de meglátásom szerint ahhoz, hogy valóban biztonságosan és hitelesen tudjon működni, ahhoz hiteles felhasználók is szükségesek. Ez utóbbira kell megoldást találni a Facebook és más közösségi portálok szerkesztőinek, hiszen rengeteg valótlan névvel és adatokkal szereplő profil és a mögötti felhasználó van. A Facebook inkább utólagosan próbál orvosolni mindent, mintsem inkább a megelőzésre törekedne.

A megelőzés keretében egy olyan megoldást javasolnék, amely szerint a tagállamokban létre lehetne hozni egy olyan központi ellenőrző rendszert, amely előre vizsgálná meg az állami adatbázisok alapján azt, hogy a beírt adatok megfelelnek-e a valóságnak, ezáltal egy ún. késleltetett regisztráció valósulhatna meg. Kiskorúak esetében össze lehetne csatolni a szülőével a fiókokat, ezáltal a szülő betekintést nyerhetne abba, hogy kikkel tart kapcsolatot a gyermek és miket oszt meg. Ellenőrzés után email-ben vagy sms-ben, attól függően, hogy mit adott meg a felhasználó a regisztrációnál, értesíthetnék, hogy a sikeres volt-e a fiók létrehozása, vagy valamely adat változtatásra szorul, ebben az esetben lenne lehetőség egy utólagos pótlásra. Amennyiben valaki megpróbálja kijátszani a regisztrációt, abban az esetben büntetésként el lehetne tiltani a regisztrációtól bizonyos ideig. Ez mindenképpen arra sarkallná a felhasználókat, hogy ne kísérletezzenek a felülettel. Személyes adatok védelme olyan tekintetben valósulna meg ezáltal, hogy így jobban ki lehetne szűrni a nem valós személyeket, akik például szélsőséges esetben bűncselekményt terveznek megvalósítani jelen mesterséges környezetet segítségül hívva az elkövetéshez.

Az utólagos kiszűrés azonban véleményem szerint jobban működik, mint az előzetes. Utólagos alatt értendő például az, amikor egy valótlan profil létrehozásának észlelésekor azt „jelenteni" lehet a portál üzemeltetőjének vagy az adatkezelőnek. Ebben az esetben szinte 1-2 órán belül megvizsgálják és törlik azt. Vizsgálatot folytattam ennek kapcsán, és valóban működik, mintegy 2 óra leforgása alatt törölték a valótlan profilt és ez idő alatt számos email-t küldtek a vizsgálat folyamatosságáról és eredményéről.

Az okos fülhallgató, szemüveg és a drónok tekintetében nem igen beszélhetünk számunkra lényeges rátelepített alkalmazásokról. Ezek tekintetében a GDPR szempontjából két releváns szempont azonosítható: élő hang és videó felvétele. A rendelet ezt is épp úgy védi, mint bármely személyes adatot, így nem lehet a másik fél előzetes tájékoztatása és beleegyezése nélkül rögzíteni a hangját vagy róla kép/videó felvételt, hiszen ezek olyan biometrikus adatok, amelyek alkalmasak a személy beazonosítására. Míg az első kettő tekintetében úgy oldható meg, hogy a felvételt készítő személy közli az érintettel, hogy rögzítésre kerülnek jelen információk, addig a drónoknál ezt távol-

[91] GDPR Preambulum (32) bekezdés.

sággal is megpróbálják megakadályozni. Számos európai országban meg van határozva, hogy hány méternél közelebb nem lehet személyekhez repülni. Ez nem véletlen, hiszen 150-200 méteren belül már az emberi alak sem vehető ki a felvételből, illetve akkor már feltételezhetjük, hogy nem megfigyelésre irányul a folyamat, viszont sok esetben elkerülhetetlen, hogy teljesen lakatlan terület felett reptessük. A GDPR meghatározza az így nyert személyes adat fogalmát: „Egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítóját, ilyen például az arckép vagy a daktiloszkópiai adat”.[92] Kivételek vannak ez alól, amelyekre nem vonatkozik a GDPR hatálya, ilyen például a bűncselekmény felderítése, nyomozás, vádeljárás lefolytatása céljából rögzített bizonyítékok.

Az okos otthon (értendő ezalatt: zár és riasztórendszer) kapcsán a megfigyelésre, mások életébe való jogtalan belátás ellen értelmezhető a GDPR. Nyilvánvalóan mindenkinek az otthona a saját személyes szférája, amelyben nem szereti, ha idegenek belelátnak. Sajnos az okos otthonok megtervezésénél nagyon körültekintően kell cselekednünk a megfelelő eszközök kiválasztásánál. Számos eszköz ugyanis így nyílt hozzáférhetőségű webes felületet használ, amelyen jelszó nélkül hozzá lehet férni az eszközökhöz, ezáltal bárkihez eljuthatnak nem kívánatos információk, arról például, hogy általában mikor nem tartózkodunk otthon, mikor megyünk nyaralni vagy éppen mikor alszunk. Megoldásképp mindenképp egy saját hálózatot kell létrehozni az otthoni eszközeinknek, illetve ezen belül jól elkülönített alhálózatokat, amelyek jelszóval védve vannak. Nem javasolt véleményem szerint az okos riasztórendszerhez vagy zárhoz más IoT eszközt kapcsolni, hiszen minél több eszköz van hozzá kapcsolva, annál nagyobb esély van arra, hogy valamin keresztül esetleg a másik eszközt irányítsák külső személyek. Mindig érdemes frissíteni az okos otthon szoftvereit, hiszen nem véletlenül tökéletesítik őket, így próbálják a biztonsági réseket minimalizálni. Mielőtt beszerzünk valamilyen otthoni okos eszközt mindenképp érdemes alaposan utána nézni annak, hogy milyen hibái, hiányosságai vannak más használók szerint, és ez alapján meghatározni a számunkra legtökéletesebbet. GDPR vonatkozásában itt is a biometrikus adatokra vonatkozó szabályok hozhatóak fel, hiszen az okos zár tekintetében nem szabad senki ujjlenyomatát rögzíteni vagy a riasztórendszer nem rögzítheti senki képmását az érintettek hozzájárulása nélkül. Mivel ezek a berendezések kifejezetten ilyen célokra lettek létrehozva, így nem lehet ezt kiküszöbölni, de mindenképp még az eszköz láthatósági körén kívülre el kell helyezni egy erre vonatkozó figyelmeztetést (Pl.: kamerával őrzött terület), így a személy, aki ebbe a helyiségbe belép, elfogadja azt, hogy a biztonság megóvása érdekében egy videófelvételen szerepel.

Az önvezető autók és a rendelet összekapcsolásaként arról kell szót ejteni mindenképpen, hogy az autók nagy része rögzíti a gépjárműre és vezetőre (amennyiben van), illetve az utasra vonatkozó adatokat. Önmagában ez még nem sérti az adatvédelmi rendeletet, hiszen ezek inkább műszaki jellegű adatok, viszont amint ezek összekapcsolódnak, például a rendszámmal, akkor már következtetéseket vonhatunk le az autó üzembentartójának személyére nézve. Először ezek az adatok kizárólag autón belül kerülnek rögzítésre, de amennyiben továbbításra kerülnek kívülálló eszközökre vagy akár más autókhoz

[92] GDPR 4. cikk. 14. pont.

(C2C=Car to Car),[93] akkor már ezekre is vonatkoztatni kell az adatvédelmi rendeletet. Itt sem tökéletes a szabályozás és mindent megoldó, hiszen egyértelmű, hogy kell a továbbításhoz a hozzájárulás, viszont abban az esetben, amikor például balesetet okoz az önvezető autó, akkor az adatokat kiadják a hatóságoknak, és pontosan lekövethető az, hogy hogyan történt, pontos földrajzi koordináták állnak rendelkezésre a kivizsgáláshoz.[94]

4. Az életkor problémája

A GDPR értelmében a gyermekek fokozott figyelmet érdemelnek a személyes adatok védelmének körében, hiszen ők nincsenek tisztában az ebben rejlő veszélyforrásokkal.[95] Mivel a GDPR lehetőséget ad arra, hogy ez egyes tagállamok eltérő korhatárt állapítsanak meg az egyes portálokon, így erre érdemes külön figyelmet fordítani. Például a Facebook-on való regisztráció már 13 éves kortól engedélyezett. Ez nem tekinthető biztonságosnak, hiszen öt adat megadásával már el is készíthetjük a fiókunkat, és senki nem ellenőrzi le, hogy hitelesek-e a megadott adatok, vagy sem. Amikor regisztrálunk kötelezően el kell fogadni az adatvédelmi és cookie szabályzatot. Abban az esetben, ha egy 10 évesnek van okostelefonja, akkor még email cím sem kell, mobiltelefonszámmal körülbelül két perc alatt regisztrálni tud magának egy érvénytelen fiókot. Kérdéses, hogy ezt mennyire lehet, vagy mennyire kell a közösségi oldalaknak, így a Facebooknak szabályozni, illetve megakadályozni.

A szülői felelősség kérdéskörében is tárgyalható ez a probléma, és a szülők feladataként is meghatározható az ellenőrzés. Azonban ezekről a regisztrációkról a szülők sem tudnak minden esetben, így a gyermek könnyen bajba kerülhet ezáltal és számos atrocitás célpontjává válhat az interneten. A Facebook oldaláról a szülővel összekapcsolt fiók megoldását már javasoltam az előző pontnál. A többi felmerülő kérdést a szülői felelősség kérdéskörébe helyezném, mivel, ha egy 13 éves gyermeket a szülő megfelelő neveltetésben részesíti, akkor tisztában kell lennie azokkal veszélyekkel, amelyek ezeken a portálokon előfordulhatnak. Esetleg a Facebook is követhetné a Gmail példáját, ahol a kiskorú is tud könnyedén regisztrálni, viszont meg kell hozzá adni a szülő email címét is, így a két adat összekapcsolásra kerül. A szülő mindezek segítségével láthatja a gyermek tevékenységét, vagy például a gyermek a Google Play áruházban sem tud semmit letölteni, amíg a szülő ehhez hozzá nem járul. A Facebooknál is hasonló megoldást tudnék elképzelni, hiszen így mégsem kellene a fiatalkorúaknak valótlan felhasználói fiókot létesíteni, hanem létrehozhatná a saját fiókját, amelyet a szülőéhez lehetne csatolni. Jelen megoldás mellé még be lehetne iktatni, hogy amíg el nem éri a 14. életévet, addig lenne számára egy „korlátozott" Facebook, amelyben a korának megfelelő szolgáltatásokat éri el. Miután betölti a megfelelő korhatárt (ez a 18. életév), abban az esetben nyílna meg számára a teljeskörű felhasználás lehetősége.

Teljesen megnyugtató megoldást az ügyben a fentiek sem nyújthatnak, csak a tudatos felhasználók, szülők esetében, viszont álláspontom szerint a gyermek sokkal jobb

[93] Chow-Miller, Ian: How Self-Driving Cars Work. Cavendish Square Publishing. New York, 2018. 2. p.
[94] Uo. 7. p.
[95] GDPR Preambulum (38) bekezdés.

helyzetbe kerülne, mivel nem kell egy valótlan profil mögé bújnia, vállalhatná saját magát ezáltal és egyúttal szülői felügyelet alatt is lenne egy reális mértékben.

VI. Megoldási javaslatok a GDPR tükrében a felvetett problémákra

1. A hatásvizsgálat mindenekelőtt a legfontosabb eszköz annak érdekében, hogy a problémára megoldást nyújtsunk, mivel ez mindennek az alapja. Ennek elkészítése az adatkezelő feladata, amelyet még az adatkezelést megelőzően kell elkészítenie, így a beépített és az alapértelmezett adatvédelem elvének megfelelően az adatkezelők számára feltétlenül ajánlott az előre tervezés és annak figyelembevétele, hogy egy tervezett adatkezelési tevékenység adatvédelmi hatásvizsgálat elkészítését teheti szükségessé, amely időbe telik.

Általában egy olyan új informatikai rendszer bevezetésénél, amely személyes adatot is kezel, az adatkezelés magas kockázattal járhat a természetes személyekre nézve.[96] Lényege, hogy az adatkezelők tevékenységük megkezdése előtt folytatnak egy vizsgálatot arra tekintettel, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.[97] Amennyiben rendelkeznek adatvédelmi tisztségviselőkkel, biztosokkal, akkor az ő szakmai tanácsukat ki kell kérni az adott ügyben. Alapos hatásvizsgálat szükséges ahhoz, hogy a problémák felszínre kerüljenek. Minden adatkezelőtől szükséges lenne az a hozzáállás, hogy felismerje az esetleges hibákat és a megoldásra törekedve eljárjon. Ahhoz, hogy szükséges-e a vizsgálat elvégzése, elsődlegesen tisztázni kell, mit jelent a személyes adatok védelme tekintetében a kockázat ill. a magas kockázat. Az Európai Unió szervezetében működő WP29-es munkacsoport[98] publikálta a WP248[99] tervezetét, amelyben leszögezte a hatásvizsgálatokra vonatkozó iránymutatásokat. Ebben elemzésre került a valószínűsíthetően magas kockázat fogalma is, amely alatt értendő az olyan adatkezelési tevékenység, ahol az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

További segítséget nyújt az adatkezelőknek az is, hogy a tagállamoknak ki kell dolgozniuk egy listát azokról az esetekről, amikor kell hatásvizsgálatot végezni, illetve el kell készíteniük egy olyan listát is, amelyben az szerepel, mikor nincsen szükség a hatásvizsgálat elvégzésére.

A hatásvizsgálatot különösen az alábbi területekre vonatkozólag kell elvégezni:

– Természetes személyekre vonatkozó jellemzők automatizált gyűjtése és értékelése,

---

[96] ITGP Privacy Team: EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide. IT Governance Publishing. 2016, 2017. 121–122. pp.

[97] GDPR 35. cikk.

[98] *29-es Munkacsoport:* A 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosaiból, illetve adatvédelmi hatóságainak képviselőiből álló független tanácsadó, véleményező és konzultatív fórum. Állásfoglalásaival és javaslataival segíti az Európai Bizottság munkáját az európai polgárok információs önrendelkezési jogának védelme érdekében.

[99] Article 29 Data Protection Working Party 17/EN WP 248- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

- Személyes adatok különleges kategóriáinak nagyszámban történő kezelése (pl. egészségügyi adatok),
- Nyilvános helyek nagymértékű, módszeres figyelésére.

A GDPR kimondja, hogy mely esetekben kell kötelezően elvégezni a hatásvizsgálatot. Ennek megvalósulása érdekében Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) közzétett egy listát[100] azokról az esetekről, amelyeknél kötelezően meg kell indítani a hatásvizsgálatot, illetve felhívta a figyelmet arra is, hogy nem csak ezekben az esetekben kell megindítani a hatásvizsgálatot, hanem akkor is, ha a GDPR 35. cikkének (1) és (3) bekezdését[101] kimeríti az adatvédelem lehetséges kockázatának köre, tehát akkor, ha valószínűsíthetően az adatkezelés magas kockázattal jár. Kötelezően kell hatásvizsgálatot folytatni például, ha az adatkezelés egy természetes személy biometrikus adatainak módszeres megfigyelésére irányul, vagy ha az adatkezelés egy természetes személy genetikai adataihoz való hozzáférést biztosít mások számára.[102] Nincsen szükség hatásvizsgálatra azonban abban az esetben, ha az adatkezelés nem jár valószínűsíthetően magas kockázattal, vagy ha egymáshoz hasonló típusú adatkezelési műveleteket végez a kezelő, ilyen esetben a GDPR szerint elegendő egyetlen vizsgálatot elkészíteni. Lehetőséget biztosít arra a magyar hatóság, hogy egy francia szoftver[103] segítségével végezzenek adatvédelmi hatásvizsgálatot.

A hatásvizsgálat elemei közé tartozik az is, hogy a tervezett adatkezelési műveletet kidolgozzák, céljait ismertessék. Az érintettek jogait és szabadságait vizsgálják, hogy milyen mértékben valósul meg és szükséges-e a korlátozás. A kockázatok kezelését célzó intézkedések rövid bemutatását is tartalmaznia kell, ideértve a rendelettel való összhang vizsgálatát és a természetes személyek érdekeinek megvalósulásának garanciáit. Végezetül tartalmaznia kell az esetleges adatvédelmi incidensekre szolgáló megoldásokat, javító mechanizmusokat és azokat a hatóságokat, amelyekhez fordulhatnak az érintettek.[104]

A hatásvizsgálatot nem elég csak azt megelőzően elkészíteni, hanem fontos az, hogy mindig naprakészen kell tartaniuk az adatkezelőknek. A WP29 is kimondja, miszerint az adatkezelőknek nem egyszer szükséges hatásvizsgálatot végezni, hanem folyamatosan.[105]

2. A Privacy by Design (beépített adatvédelem) irányzat lényege, hogy az adatvédelmet bele kell építeni a technológiába.[106] Előtérbe helyezése és elsődleges alkalmazása megfelelő lenne arra, hogy már eleve úgy kerüljön kialakításra egy új működési szervezet (technológia, szoftver, stb.), hogy az adatvédelmi szempontokat már az egyes

[100] A Nemzeti Adatvédelmi és Információszabadság Hatóság jegyzéke a kötelező adatvédelmi hatásvizsgálat eseteiről: https://www.naih.hu/files/GDPR_35_4_lista_HU.pdf, Utolsó letöltés ideje: 2018. 12. 06.
[101] GDPR 35. cikk.
[102] A Nemzeti Adatvédelmi és Információszabadság Hatóság jegyzéke a kötelező adatvédelmi hatásvizsgálat eseteiről. i. m.
[103] Commission Nationale de l'Informatique et des Libertés- PIA software.
[104] ITGP Privacy Team: i. m. 121–122. pp.
[105] WP29 Guidlines i.m.
[106] Klitou, Demetrius: Privacy-Invaliding Technologies and Privacy by Design- Safeguarding Privacy, Liberty and Security in the 21st Century. Centre for Law in the Information Society, Faculty of Law, Leiden University, 2012. 260. p. https://openaccess.leidenuniv.nl/handle/1887/20288, Utolsó letöltés ideje: 2018. 12. 05.

elemek kialakításakor maximális figyelembevétellel készítsék el.[107] E mögött nyilvánvalóan az szerepel, hogy mindenki sokkal jobban betartaná a szabályokat, amennyiben úgy lenne létrehozva a rendszer és nem pedig utólag formálják rá a működést. Nem elegendő egy szervezetnek az alapvető adatvédelmi szabályoknak egyszerűen csak megfelelni, hanem már az elkészítése sorát, tehát a kezdetekkor integrálni kell a személyes adatok védelmére vonatkozó protokollokat. Ezen elv megvalósítása azonban hiányos, hiszen nem minden tagállamban hajtják végre egyformánt. Ennek oka részben, hogy nem minden tagállamban tart ugyanott a technológia, a szolgáltatók gazdasági megfontolásai és érdekei játszák továbbra is az elsődleges szerepet, illetve fontos szempont a működési mechanizmus kialakítására szánt költségvetés. A beépített adatvédelemnek ki kell terjednie egyrészről az informatikai rendszerekre (IT systems), másrészről az üzleti gyakorlatra és a hálózati infrastruktúrákra.[108] Az adatkezelő tehát köteles az automatikus adatfeldolgozás körében az adatfeldolgozás folyamatát úgy megtervezni és a hozzáférés szabályait úgy meghatározni, hogy a személyes adatok jogellenes felhasználásának lehetőségét elkerülje.[109]

3. Privacy by Default (alapértelmezett adatvédelem) az előbb említett irányzat testvére, hiszen mind a kettő elengedhetetlen részét képezi egy olyan biztonságos világ kialakításának, amelyben az adatalany irányít. Hiszen mind jelentésében is, mind tartalmát tekintve azt jelenti, hogy az adatalany kifejezett kérésére lehetne csak bármilyen személyes adatot gyűjteni. Másként fogalmazva az adatkezelő alapértelmezett hozzáállása kell ahhoz, hogy mindig, minden körülmények között a GDPR rendelkezéseivel összhangban történjen az adatkezelés folyamata. A GDPR egy „kényszer" volt az adatkezelők számára, mivel éles váltást hozott számukra, rendkívüli felkészülést igényelt és nagy anyagi forrásokat ölelt fel. Azok, akik a GDPR hatályba lépését követően terveznek kialakítani bármilyen céget, vagy szolgáltatást, számukra már az lesz az alapvető működési forma, hogy a rendelet értékeit szem előtt tartva szervezzék meg működésüket.

4. Szolgáltatók érdekeltté tétele abban, hogy ne csak azért tartsák be a rendelet, mert jogkövetkezmények fűződnek hozzá, hanem azért, mert tényleg az ő érdekeiket is szolgálja. A dolgozatom korábbi pontjában a Bizottság munkájánál említettem, hogy egy egységes digitális piacot kívánnak létrehozni a tagállamok között, ahol az emberek bizalmát erősítik, így bátran mernek rendelni, akár másik országból is termékeket. Mennyivel kifizetődőbb lenne az a cégek számára is az, hogyha a természetes személyeknek nem jelentenének korlátokat az országhatárok, hiszen bizalommal állnának ahhoz, hogy más tagállamokból vásároljanak. Amennyiben létrejönne a kellő bizalom a fogyasztók és szolgáltatók között, sokkal szélesebb világ tárulhatna egy-egy fogyasztó elé. A *Cambridge Analytica* ügyben az ICO az Egyesült Királyság Adatvédelmi Hivatala a lehető legmagasabb bírságot szabta ki a Facebook-ra, amely 500.000 £ (183 millió forintot). Az ügy lényege, hogy az előbb említett politikai tanácsadó cég jogtalanul

[107] ITGP Privacy Team: i. m. 137. p.; GDPR-Privacy by Design, Forrás: https://gdpr-info.eu/issues/privacy-by-design/, Utolsó letöltés ideje: 2018. 12. 06.

[108] *Privacy by Design.* Forrás: https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/, Utolsó letöltés ideje: 2018. 12. 06.

[109] ITGP Privacy Team: i. m. 299.

szerezte meg 90 millió Facebook felhasználó személyes adatait, és ezeket felhasználva irányított hirdetésekkel próbálták befolyásolni a természetes személyeket olyan ügyekben, mint például az amerikai elnökválasztás vagy a Brexit.[110] Amíg nem áll arányban a büntetés azzal, amekkora hasznot hajtanak be egy-egy szabályszegésért, addig nem is fogják betartani teljes mértékben. Az egyes vállalatoknak kell azt előtérbe helyezni, hogy fontosabb legyen számukra a bizalom a felhasználók felől, mint az a nyereség, amelyet kaphatnak egy szabály megszegért.

5. A felhasználói tudatosságot említem legutoljára, azonban véleményem szerint ennek a megoldásnak kiemelkedő jelentősége van a javaslatok között. Nem lehet elégszer hangsúlyozni azt, hogy a felhasználónak mekkora szerepe van abban, hogy személyes adatai biztonságban legyenek. A felhasználó gondolkodásának át kell fognia azt, hogy ez mekkora adatvédelmi kockázattal is járhat, illetve másik oldalról meg kell tudnia különböztetni a manipulatív reklámokat és hirdetéseket, a valódiaktól. Úgy gondolom egy gyakorlott számítógép felhasználó könnyedén el tudja különíteni mi az igazi és mi a valótlan tényállítás ezekkel kapcsolatban. Sokan nincsenek azzal tisztában, hogy az internetre feltöltött információknak milyen következménye lehet. A felelősségnek nagyon szűk köre jogi probléma, a nagyrésze inkább társadalmi kontextusba helyezhető el. A gyorsan fejlődő technológiára nagyon nehéz jogi megoldásokat találni, hiszen a jog sokkal lassabban képes követni a fejlesztéseket, mint ahogyan azok fejlődnek. Mivel nagyon sok olyan kérdés van, amelyre csak a társadalmi tudatossággal lehetne megoldást nyújtani szakszerűen, ezért a cél mindenképpen az, hogy ezt a tudatosságot növelni kell, amelynek számos módszere elképzelhető. Fontos megemlíteni egy fogalmat, amely ezen témához kapcsolódik, amely nem más, mint a médiaműveltség. A médiaműveltség olyan ismeret- és készségkészletet feltételez, amely felelős, autonóm döntéshozatalt, az információs környezetben rejlő lehetőségek maximalizálását és a veszélyek minimalizálását eredményezi.[111]

Egyrészt mivel sokszor a szülők már idősebb korosztályból kerülnek ki, így nem feltétlenül ők a megfelelőek arra, hogy a fiatalabb generációt felvilágosítsák az adtavédelmi kockázatokkal kapcsolatban, másrészt pedig sokszor a szülő maga sem látja át ennek a reális veszélyeit. Ennek kiküszöbölése lehetne az, hogy iskolai keretek között valódi adatvédelmi szakértők, vagy ehhez a területhez értő tanárok adnák át a tudást. Kétféleképpen valósulhatna meg, egyrészt tanóra keretében, másrészt esetlegesen vendégelőadók előadása keretében kaphatnának arról egy képet, hogy hogyan „kell" kezelni például a közösségi médiát helyesen és biztonságosan. Nem feltétlenül csak a fiatalkorúakhoz kellene ennek a tudásnak eljutni, hanem azokhoz a felnőttekhez is, akik nincsenek ezen veszélyekkel tisztában. Rengeteg felhasználó el sem olvassa az adatkezelési tájékoztatókat, vagy a cookie-k tartalmát, inkább mindent elfogad, csak hamarabb „túl legyen" rajtuk. Fel kellene bennük ébreszteni a tudatot, hogy ez a saját érdeküket szolgálja. Önmagában attól, mert egy honlapon szembesülnek azzal, hány adatkezelőhöz jut el a személyes adatuk, még nem fogják kihagyni az oldal megtekintését. Azonban, ha belátják azt, hogy a közösségi oldalakra való kisgyermekes képek feltöltésének mennyi

[110] SUMPTER, DAVID: *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles – The algorithms that control our lives.* Bloomsbury, 2018. Chapter 5. e-book.
[111] NAGY KRISZTINA: *Literacy és felhasználói tudatosság*. In: Infokommunikáció és Jog. 2016/1 (65.) 17–21 pp.

negatív hatása lehet, akkor átgondolják, milyen képeket és milyen tartalommal osztanak meg a nagyvilággal. A felhasználók számára lehetővé kellene tenni, hogy teljes mértékben kiaknázhassák az interneten a tudatosságnövelő szolgáltatásokat a saját és a szolgáltatók érdekében.[112]

VII. Összefoglaló

Dolgozatomban az Európai Unió új jogi eszközére, a személyes adatok védelmét szolgáló általános adatvédelmi rendelet, vagyis az ún. GDPR rendelkezéseire koncentráltam az okoseszközök világára vetítve. Ennek keretében először bemutattam az okoseszközöket és azok veszélyeit a személyes adatokra tekintettel. Az eszközöket három csoportra osztottam azon szempontok alapján, hogy az élet mely területén van jelen velünk. Első csoportba azok az eszközök kerültek, amelyek mindig velünk vannak, a második csoportba a háztartás eszközei, a harmadikba pedig a közvetlen környezetünkben fellelhető okoseszközök kerültek.

Ezt követően az Európai Bizottság munkásságát és törekvéseit figyeltem meg annak tükrében, hogyan próbálja meg felvenni a lépést a technológiai fejlődés rendkívül gyors előre haladásával. A legfőbb válasz a technológia fejlődésére egyértelműen a GDPR megalkotása volt, amely dolgozatom központi témája. A rendelet rövid bemutatása elengedhetetlen ahhoz, hogy a gyakorlati oldalát megértsük pontosan. A GDPR-nak való megfelelés nem döntés kérdése, nem egy lehetőség, hanem kötelező. Világosan látható, hogy ez az elmúlt évek egyik legjelentősebb szabályozása adatvédelemi területen.

A rendelet bemutatását követően elérkeztem dolgozatom központi részéhez, amelyben a rendelet releváns szakaszait mutatom be annak fényében, hogy az okoseszközök való életben való működésük során miként valósítják meg a rendelet pontjait és hogyan tudnak ennek megfelelni. Szerepel számos hiányosság és kérdés ezekkel kapcsolatosan, amelyekre igyekszem rámutatni. Ezek felismerésekor megoldási javaslatokat is próbáltam tenni több problémára, annak érdekében, hogy hogyan lehetne javítani a személyes adatok védelmén egy-egy esetkörben. Sajnos számos hiányosság van még így is, hogy a rendelet megalkotásra került. Egyelőre inkább népszerűbb az utólagos korrekció az adatvédelmi szabályozásoknál, mint sem a megelőzés, de már pozitívum, hogy megjelentek olyan irányzatok, ahol a megelőzés a fontos. Ahogyan a rendelet is részletezi, az adatvédelmi hatásvizsgálat az egész adatvédelem alapja. Az lenne a legfontosabb, hogy mindig előre gondolkodjunk, és ne utólagosan próbáljuk orvosolni a már-már megalkotott technológiákkal járó adatvédelmi problémákat. Utólagos megoldásként GDPR fontos lehetőséget ad a természetes személyek számára, hogy fellépjenek adataik védelmében, és komoly bírságok is kiszabhatók. Azonban ekkor már hiába lehet fellépni utólagosan, mivel megtörtént az adatvédelmi incidens, a személyes adatokkal való visszaélés. Ahhoz, hogy ilyen incidens ne is tudjon megvalósulni, már a rendszerek kialakításánál bele kell építeni a jogot a technológiába, ami a Privacy by Design irányzat jelenté-

[112] Ina Fourie, (1999) ″Empowering users –current awareness on the Internet", The Electronic Library, Vol. 17 Issue: 6. 379–388. pp.

se is. Amíg a felhasználók nem képesek átlátni a biztonsági réseket és az adatvédelmet a saját előnyeikre fordítani, addig a biztonság is hagy kivetnivalót maga után, mivel a technológia mindig fejlődni fog, ez nem kérdés. Véleményem szerint az adat manapság hatalom, legyen szó akár egy cégről, akár politikáról. Ezzel irányítóvá válnak a reklámok, hirdetések, és ezáltal az információt célzottan el tudják juttatni a természetes személyekhez, amelyekkel hatalmas erőfölényt tudnak generálni versenytársaikhoz képest. A fentiek alapján megállapíthatjuk, valóban az „adat a 21.század olaja”.[113]

REGINA HORVÁTH

ARE WE SAFE IN THE AGE OF SMART-TECHNOLOGY DEVICES UNDER PROVISIONS OF THE GDPR?

(Summary)

In my work I analysed the relevant provisions of the European Union’s General Data Protection Regulation (GDPR) entered into force on 25th of May 2018, regarding different info-communication systems (ICT), especially smart-technology devices. These were my main research questions: to what extent the new regulation keeps up with the development of technology and most importantly, how much our personal data are in safe in the world of complex technical solutions? The protection of personal data raises numerous questions in lawyers, legal experts and in us, law students as well, mainly because the application of the relevant legislation to technological innovations is not always clear and easy in practice.

In my research I focused on the application of the GDPR to the smart-technology devices. Therefore, I delivered a comprehensive picture of smart-technology devices, which are available nowadays by providing the emerging data protection challenges. Then, I revealed the European Union’s and more specifically, the European Commission’s data protection measures from which I analysed the provisions of the GDPR in detail. Through this method, on the one hand, possible risks of the usage of smart-technology devices could be identified. On the other hand, it can shed light on appropriateness of the GDPR provisions or on its possible flaws. The aim of my research was to reveal these flaws and imperfections. At the end of my work, I made practical proposals in context of the results of my research to improve the safety of personal data processing above all. As a conclusion I can state that data controllers should improve the personal data protection, but the data subjects (users) awareness is crucial regarding this aspect.

[113] Idézet PETER SONDERGAARD-tól: Hansen, Marit – Kosta, Eleni – Nai-Fovino, Igor – Fischer-Hübner, Simone (edsi) i. m. 78. p.