MIKLÓS GELLÉRT

Az Európai Unió adatstratégiájához kapcsolódó jogszabályi keretrendszer áttekintése

Absztrakt

A cikk rövid áttekintést nyújt az Európai Unió gazdaságának digitális adatgazdasággá történő átalakulását elősegítő jogszabályi keretrendszerről. A cikkben bemutatásra kerülnek a személyes és nem személyes adatokra vonatkozó főbb jogszabályok, valamint az adatgazdasággal összefüggő jogszabálytervezetek. A cikk célja a személyes és nem személyes adatok gazdaságban betöltött szerepének, a kapcsolódó jogok és kötelezettségek, valamint az iparági trendek bemutatása.
Kulcsszavak: adat, személyes adat, biometria, adatvédelem, GDPR, kiberbiztonság

Abstract

The present article aims to provide a brief overview of the legal framework that facilitates the transformation of the European Union's economy into a digital data economy. The article presents the main legislation on personal and non-personal data as well as draft legislation related to the data economy. The purpose of this article is to present the role of personal and non-personal data in the economy, the associated rights and obligations, and to highlight the industry trends.

Keywords: data, personal data, biometrics, data protection, GDPR, cybersecurity

1. Bevezetés

Az információtechnológiai forradalom gyökeresen megváltoztatta az emberek életmódját, szokásait, a gazdaságot és a társadalmat. Mindennapi életünk során hihetetlen mennyiségű adatot generálunk, melyek kezelése, rendszerezése és elemzése az adattudomány és a gépi tanulás fejlődésével egyre hatékonyabb lesz. Ennek az átalakulásnak az egyik mozgatórugója az adat, és az adatok felhasználásához kapcsolódó innováció. Napjaink egyik meghatározó globális megatrendje a digitalizáció, amelynek egyik velejárója, hogy olyan eszközök is intelligenssé váltak, amelyeket korábban nem érintett a számítástechnikai fejlődés. A munkahelyeken és a háztartásokban egyre gyorsuló ütemben jelennek meg

a dolgok internetéhez (IoT – *Internet of things*) csatlakozó eszközök, az alkalmazások és az általuk generált adatok az egyre nagyobb része kerül át a számítástechnikai felhőbe.

A 2019 óta tartó koronavírus világjárvány és az arra adott kormányzati és munkáltatói válaszok csak tovább gyorsították a digitális transzformációt. A világon létrehozott adat mennyisége rendkívüli gyorsasággal növekszik; míg a világon létrehozott adatok mennyisége 2018-ban 33 zettabyte volt, addig az előrejelzések alapján ez a szám 2025-re elérheti a 175 zettabyte-ot is. A nagyságrend szemléltetése végett: egy zettabyte 1 000 000 000 000, azaz egybillió gigabyte. Ilyen volumenű növekedés szükségszerűen magával hozza a változást az adatok tárolásának és feldolgozásának módjában. Napjainkban az adatok 80 százalékának feldolgozása és elemzése adatközpontokban történik, míg összesen 20 százalék történik okoseszközökben, valamint peremhálózati számítástechnikai (*edge computing*) megoldások révén.[1] Ezek az arányok várhatóan jelentősen megváltoznak az évtized második felére. Ennek egyik oka, hogy a felhőszámítással (*cloud computing*) ellentétben a peremhálózati számítástechnika alkalmazásával javul az adatfeldolgozás sebessége, ami kritikus tényező olyan reakcióérzékeny rendszerek esetén, mint az önvezető gépjárművek, az egészségügy vagy a virtuális valósággal kapcsolatos fejlesztések. Az Európai Bizottság becslése szerint 2025-re az Európai Unió adatgazdaságának értéke 829 milliárd eurót fog kitenni a 2018-as 301 milliárd euróhoz képest, az adatgazdasággal kapcsolatos ágazatokban pedig 10,9 millióan fognak dolgozni a 2018-as 5,4 millióhoz képest.[2] Az Európai Bizottság célul tűzte ki az európai ipar és gazdaság versenyképességének növelése érdekében a digitalizációt elősegítő jogszabályi keretrendszer létrehozását és 2020-ban közzétette adatstratégiáját. Az adatstratégia és az abban megfogalmazottak illeszkednek az Európai Unió már korábban közzétett digitális stratégiájába, melynek célja a társadalom és a gazdaság digitalizálásában rejlő lehetőségek kiaknázása egy méltányos és versenyképes digitális gazdaság létrehozása érdekében. Az Európai Uniót azonban számos tényező hátráltatja abban, hogy kiaknázza ezeket a lehetőséget. Jelenleg még nem került elfogadásra az átfo-

[1] Európai adatstratégia.

[2] Európai adatstratégia.

gó szabályozás minden eleme, de problémák vannak többek között a felhőalapú számítástechnikai piac mind keresleti, mind kínálati oldalán is. Az uniós székhelyű számításifelhő-szolgáltatók részesedése a piacból elenyésző az amerikai és kínai szolgáltatókhoz képest. Ez egyrészt kiszolgáltatottá teszi Európát a külső fenyegetéseknek, másrészt azzal a kockázattal jár, hogy a tárolt adatokhoz olyan harmadik országbeli joghatóságok férnek hozzá, amelyek nincsenek összhangban az EU adatvédelmi keretével.[3] Keresleti oldalon pedig probléma, hogy a felhőszolgáltatások elterjedtsége alacsony mind a közszféra, mind a kis- és középvállalkozások körében, holott alkalmazásukkal jelentős költségcsökkentés lenne elérhető mindkét szektor számára. Az Európai Unió válasza a fenti problémákra és a piaci aszimmetriára egy sajátos, értékalapú szabályozás, amely alternatívát kínál a digitális gazdaság alulszabályozott, privatizált amerikai, valamint az államilag ellenőrzött, korlátozottan nyitott kínai modelljével szemben.[4]

Ennek részeként került elfogadásra az Európai Parlament és a Tanács 2016/679 rendelete, az általános adatvédelmi rendelet (GDPR), megerősítve az érintettek személyes adatok védelméhez fűződő jogait. Elfogadásra került továbbá a nem személyes adatok Európai Unióban való szabad áramlásának keretéről szóló 2018/1807 rendelet (FFD), a kiberbiztonságról szóló 2019/881 rendelet (CSA), valamint a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról szóló 2019/1024 irányelv. Jelenleg előkészítés alatt áll az adatrendelet (*Data Act*), valamint az elektronikus hírközlési adatvédelemről szóló 2002/58/EK irányelv modernizálására irányuló rendelet (ePrivacy rendelet) is. Az Európai Bizottság 2020. november 25-én közzétette továbbá javaslatát az adatkormányzási rendelet tervezetéről.

2. Európai Parlament és a Tanács 2016/679 rendelete (GDPR)

Az információtechnológiai forradalom következtében keletkező hatalmas mennyiségű adat egy jelentős része személyes adat, amely kapcsolatba

[3] COM(2020) 66 4.

[4] Tóth 2021.

hozható az azt létrehozó természetes személlyel. Érdemes ezért áttekinteni, hogy mi is az a személyes adat és mi az adatvédelmi szabályozás célja. Adatvédelmi jog alatt a személyes adatok kezelésével és az egyén magánszférájának védelmével összefüggő jogszabályok és rendelkezések összességét értjük. Az Európai Unió általános adatvédelmi rendeletének hatálybalépését megelőző és az azt követő médianyilvánosság emberek nagy tömegének figyelmét irányította az adatvédelemre és a személyes adatok védelmének fontosságára. Az adatvédelem története azonban nem a GDPR elfogadásával kezdődött, a magánszféra védelmének fontossága már jóval korábban megfogalmazódott. „Az azonnali fényképek, a sajtóvállalkozások behatoltak a háztartás és a magánélet szent területére, és számos mechanikus eszköz azzal fenyeget, hogy beváltja azt a jóslatot, miszerint »amit a szekrényben suttognak, azt a háztetőkről fogják hirdetni«." Az előbbi idézet akár napjainkból is származhatna, azonban Samuel Warren és Louis Brandeis már több, mint száz éve felhívták a figyelmet a technika fejlődésének veszélyeire és érveltek a magánszféra védelmének fontossága mellett. Az 1970-es évekre a technológiai fejlődése elérhetővé tette az automatizált adatfeldolgozó rendszereket, amelyek jelentősen megkönnyítették nagy mennyiségű személyes adat gyűjtését, kezelését, feldolgozását. A számítástechnika egyre gyorsuló ütemű fejlődése és a számítógépek széles körű elterjedése tovább egyszerűsítette az adatok feldolgozását, míg az internet és a nemzetközi hálózatok elhozták az adatkezelés globalizálódását.[5] A számítástechnikai fejlődés korai szakaszában a számítási kapacitás még drága és ezáltal korlátozott erőforrásnak számított, ezért több államban is felmerült a hatékonyság növelése érdekében nagy, integrált adatbázisok kialakításának szükségessége és egy univerzális azonosító, amellyel az érintettre vonatkozó különböző adatok összekapcsolhatók.[6] A folyamat kapcsán elindult diskurzus nyomán megszülettek Európa elsőgenerációs adatvédelmi törvényei, amelyek megteremtették az állami adatbázisok transzparenciáját. Magyarországon az általános és egységes személyazonosító jel (személyi szám) alkotmányellenességét az Alkotmánybíróság a 15/1991. (IV. 13.) AB határozatban mondta ki, meghatározva ezzel a magyar adatvédelmi jog fejlődését. Ha-

[5] Jóri et al. 2018, 24.

[6] Például az USA-ban, Franciaországban, Svédországban és a Német Szövetségi Köztársaságban.

tározatában az alkotmánybíróság elvi éllel rögzítette, hogy olyan integrált személyi adatbank létrehozása, amely az állampolgárok adatait a lehető legszélesebb körben tartalmazza, az egészségügyi adatoktól kezdve a vagyoni adatokon át a hivatali ügyekig alkotmányellenes. Egy ilyen adatbázis kezelője az egyes személyekre vonatkozó adatokat összességükben és összefüggésükben megismerné, és ez kiszolgáltatottá tenné az adatalanyokat, átvilágíthatóvá tenné magánszférájukat. A kiragadott adatok alapján összeállítható lenne az érintettre vonatkozó személyiségprofil.[7]

Az eltérő nemzeti adatvédelmi szabályozások azonban sokszor eltérő követelményeket és védelmi szintet írtak elő, növelve az adattovábbítás költségeit és ezáltal akadályozva a nemzetközi kereskedelmet. Az akadályok mérséklése érdekében 1980-ban elfogadásra kerültek a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) adatvédelmi irányelvei. Az OECD-Irányelvekben foglalt rendelkezések hatással voltak a később elfogadott Európa Tanács Adatvédelmi Egyezményére (1981) és az EU személyes adatok védelméről szóló 95/46/EK irányelvére (1995) is. Utóbbi célja a természetes személyek jogainak védelme mellett a tagállamok különböző adatvédelmi szabályainak közelítése és ezáltal a belső piaci akadályok lebontása volt. A személyes adatok védelmének joga az Európai Unióban először irányelvi szinten került szabályozásra. Az Európai Unió jogforrási hierarchiájában az irányelvek az alapító szerződésekhez és általános jogelvekhez képest másodlagos jognak minősülnek, hatályuk – bizonyos esetektől eltekintve – közvetett. Az irányelv olyan jogalkotási aktus, amely valamennyi uniós ország számára kötelezően elérendő célkitűzést állapít meg, annak megvalósításáról és a tagállami jogba történő átültetéséről azonban már a tagállamnak kell gondoskodnia.

Hosszú előkészítő munka után az Európai Bizottság 2016-ban kihirdette az általános adatvédelmi rendelet szövegének tervezetét, amelyet 2018. május 25. napjától kell kötelezően alkalmazni. A rendelet hatálybalépést fokozott médiafigyelem előzte meg, jelentős részben az az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (Infotv.) rögzített korábbinál jelentősen magasabb bírság összegek miatt. Valóban, az Infotv. alapján korábban kiszabható húszmillió forintos törvényi maximumtól a rendelet által meghatározott tíz- illetve

[7] 15/1991. (IV. 13.) AB határozat.

húszmillió eurós bírságösszegek nagyságrendekkel térnek el, ezzel együtt azonban számos egyéb téren hozott változást a rendelet elfogadása. A korábbi állapothoz képest az adatvédelem kérdése és szabályozása a tagállami szintről európai uniós szintre került, hozzájárulva a belső piac további egységesítéséhez a követelmények és a joggyakorlat összehangolása által. Az egységesített szabályozás azon túl, hogy azonos szintre emeli a személyes adatok védelméhez fűződő jog szintjét a különböző tagállamokban, a digitális versenyképességet is javítani hivatott, hiszen a korábbi 27 különböző tagállami adatvédelmi szabályozás helyett immár elég csak egy alkalmazandó szabályozásnak megfelelni.

A fentiek mellett egy további szempont, hogy az Európai Unió a digitalizációban lemaradásban van az Egyesült Államokhoz és Kínához képest, azonban az egységes és szigorú adatvédelmi szabályozással képes hatást gyakorolni a nagy technológiai cégek tevékenységére. Az Európai Fejlesztési Bank (EIB) 2019-es felmérése alapján az európai cégek hátrányban vannak az amerikai cégekkel összehasonlítva a 3D nyomtatás, a robotika, az IoT vagy a *big data* terén a gazdaság összes vizsgált ágazatában.[8] A legnagyobb hardver- és szoftvercégek kevés kivételtől eltekintve jellemzően amerikaiak vagy ázsiaiak. Egy átlagos ember amennyiben szabadidejében használja valamelyik közösségi hálózatot, akkor nagy eséllyel a Meta (korábban Facebook) valamelyik platformját választja, ugyanígy, ha rákeres valamire az interneten vagy megnézi az e-mailjeit akkor statisztikailag nagy eséllyel a Google valamelyik szolgáltatását fogja igénybe venni, egy olyan számítógépről, amelyen a Microsoft által nyújtott Windows operációs rendszer fut. A felsorolt cégek egyike sem európai sikertörténet. Az iménti tevékenységekben azonban közös, hogy adatot generálnak, amelyek jelentős része személyes adat, így tevékenységük – bizonyos esetekben – az általános adatvédelmi rendelet hatálya alá esik. A felsorolt technológiai vállalatok sikeréhez azonban nagyban hozzájárult ingyenességre épült üzleti modelljük, valamint agresszív felvásárlási politikájuk. A kínált szolgáltatások ingyenessége azonban ebben az esetben csak látszat, illúzió. A szolgáltatók ugyanis igényt tartanak a felhasználókra vonatkozó személyes adatok minél szélesebb körének kezelésére. Ez az üzleti modell a felhasználókban azt az érzést keltheti, mintha a szolgál-

[8] Who is prepared for the new digital age?

tatás valóban ingyenes lenne, természetesen erről azonban szó sincs, a technológiai vállalatok hatalmas infrastruktúrát és rengeteg munkavállalót foglalkoztatnak, amelyet jellemzően reklámbevételekből, valamint a felhasználók személyes adatainak továbbértékesítéséből tartanak fent. Ezzel azonban több probléma is van. A GDPR ugyan előírja az adatkezelők részére az érintettek tájékoztatását személyes adataikról, azonban a hosszú, nehezen érthető nyelven megfogalmazott adatvédelmi tájékoztatókat a felhasználók jellemzően nem olvassák el, emellett viszont nem is derül ki belőlük, hogy mekkora értéket képviselnek személyes adataik a vállalatok részére. A begyűjtött személyes adatok alapján létrehozott profil segítségével a vállalatok egyrészt személyre szabott reklámokat kínálnak, amelyek magasabb értéket képviselnek a hirdetők számára, mint a nem személyre szabott reklámok, másrészt pedig a közösségi média platformszolgáltatója releváns tartalmakat tud nyújtani a felhasználó részére, ezáltal hosszabb ideig lekötve figyelmét. A figyelem és a platformon eltöltött idő pedig több reklámfogyasztást és ezáltal magasabb bevételeket is jelent.[9] Az adatgazdaságban az adatok mennyisége és minősége a kulcskérdés. Minél több adathoz fér hozzá egy technológiai vállalat, annál jobban személyre tudja szabni szolgáltatásait, ezáltal pedig vonzóbbá tenni azt a felhasználók számára. A kör ezzel pedig be is zárult, hiszen a kevésbé személyre szabott reklámokat kínáló platformok hátrányba kerülnek a fogyasztókért folytatott piaci küzdelemben, és a piacon végül a monopolhelyzet alakulhat ki.

2.1 Személyes adat, a személyes adatok különleges köre

Az adatvédelmi jog egyik legfontosabb fogalma a személyes adat. Csak az adat személyes adat voltának meghatározását követően lehet eldönteni azt, hogy az adott adatkezelésre alkalmazandóak-e az általános adatvédelmi rendelet rendelkezései. A rendelet alapján „személyes adatnak minősül minden azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, pél-

[9] Tóth Á. 2021.

dául név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható".[10] Felmerülhet a kérdés, hogy például az internetre csatlakozó számítástechnikai eszközök azonosítására szolgáló IP-címek személyes adatnak minősülnek-e, különös tekintettel arra, hogy a dinamikus IP-címeket az internet szolgáltató meghatározott időközönként újraosztja az előfizetők között, és bizonyos esetekben egy IP-címhez tartozhat több informatikai eszköz is. A kérdést mind a hazai, mind a nemzetközi adatvédelmi szakirodalom behatóan vizsgálta, és 2016-ban az Európai Unió Bírósága ítéletében[11] is rögzítette, hogy bizonyos körülmények fennállása esetén a dinamikus IP-cím is személyes adatnak minősül. Ezt az értelmezést erősíti meg általános adatvédelmi rendelet 30. preambulumbekezdése is, amely alapján „természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és *cookie*-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel. Ezáltal olyan nyomok keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatóak a természetes személyes profiljának létrehozására és az adott személy azonosítására."[12]

A rendelet tárgyi hatálya kiterjed a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.[13] A GDPR területi hatálya extraterritoriális (határon átnyúló), tehát rendelkezéseit alkalmazni kell egyrészt az EU-ban tevékenységi hellyel rendelkező adatkezelők tevékenységeivel összefüggésben, másrészt abban az esetben, amennyiben az harmadik országbeli adatkezelő árut vagy szolgáltatást nyújt az Európai Unióban tartózkodó érintettek számára vagy az érintettek viselkedésé-

[10] GDPR 4. cikk 1.
[11] C582/14. sz. ügy.
[12] GDPR 30. preambulumbekezdés.
[13] GDPR 2. cikk (1).

nek megfigyeléséhez kapcsolódnak, feltéve hogy az EU területén belül tanúsított viselkedésükről van szó.[14] Megvalósul tehát a személyes adatok kezelése akkor is, amikor egy Európai Unióban tartózkodó érintett Európai Unión kívüli, például amerikai vagy ázsiai online kereskedelmi platformról rendel árut vagy szolgáltatás.

A rendelet a személyes adatok körén belül megkülönbözteti a személyes adatok különleges kategóriáit, amelyek az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok. Ezek a személyes adatok ezért egyedi védelmet igényelnek, mivel az alapvető jogokra és szabadságokra nézve a kezelésük körülményei jelentős kockázatot hordozhatnak.[15] A különleges adatok körébe tartoznak a digitalizáció szempontjából kiemelt jelentőségű biometrikus adatok is. Biometrikus adat a természetes személyek testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személyek egyedi azonosítását.[16] A fentiek alapján biometrikus adatnak minősül az arckép, a daktiloszkópiai adat (ujjnyomat), a hang, az írisz és a retina, a tenyérerezet, de ebbe a kategóriába tartozik az érintett járása is. A biometrikus tulajdonságok egyik előnye, hogy azok legtöbbször az azonosítandó személy tulajdonában – mondhatni mindig kéznél – vannak, és azok egy része jellemzően hosszú ideig változatlanul lehetővé teszi az érintett azonosítását, ennek köszönhetően a biometrikus adatok egyre szélesebb körben kerülnek felhasználásra. Ennek egyik kézenfekvő példája a modern telefonok zárolása, amelyet már ujjlenyomattal vagy arckép felismeréssel is fel lehet oldani. Természetesen egy sérülés – például egy vágás vagy égési sérülés – vagy egy betegség örökre megváltoztathatja az érintett bizonyos biometrikus jellemzőt. A biometrikus azonosítás menete két szakaszra osztható, egy regisztrációs és egy azonosítási szakaszra. Az első szakasz magában foglal minden olyan folyamatot, amely a biometrikus adat kinyeréséhez (pl. kép vagy hangfelvétel készítéséhez), annak biometrikus sablonná történő átalakításához és digitalizálásához, az érintettel történő összekapcsolásához, valamint tárolásához szükséges.

[14] GDPR 2-3. cikk.

[15] GDPR 51. preambulumbekezdés.

[16] GDPR 4. cikk 14.

A második szakasz során a kinyert biometrikus adatok a digitalizálást követően összehasonlításra kerülnek a korábban kinyert és a rendszerben eltárolt sablonnal. A biometrikus azonosítás során az élettani jellemzőkről készített sablonok és minták a hatályos adatvédelmi jogszabályok szerint személyes adatnak tekintendők, így az azonosítási eljárás kialakítása, valamint a minták kezelése során is érvényre kell jutnia az alkalmazandó alkotmányos és adatvédelmi jogi alapelveknek.[17]

A biometrikus adatok kezelésére vonatkozó előírások ismertetése előtt fontos tisztázni azt, hogy a jogszabály definíciója szerint mi számít adatkezelésnek. Az általános adatvédelmi rendelet alapján „adatkezelésnek minősül a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közléstovábbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés".[18] A fogalommeghatározás példálózó, azonban a definíció első feléből egyértelmű, hogy a személyes adatokon végzett bármely olyan művelet adatkezelésnek minősül, amely kiterjed a személyes adatok kezelésére. A GDPR 40. preambulumbekezdése és 6. cikke alapján a személyes adatok kezelése csak megfelelő jogalap fennállása alapján lehetséges, ezért mindenképpen szükséges legalább egy jogalap megjelölése a jogalapok zárt és véges felsorolásából.[19] A rendelet alapján az adatkezelők egy adatkezelést akár több jogalap megjelölésével is végezhetnek. Ebben az esetben, amennyiben az elsődleges jogalap bármely okból megszűnik – például az érintett hozzájárulását visszavonja –, úgy a másodlagosan megjelölt jogalap lép a helyébe. Erre egy gyakran tapasztalható példa a weboldalak adatkezelése, ahol a különböző adatkezelési célok vonatkozásában – alapvető funkciók, hirdetések személyre szabása, teljesítmény mérése stb. – a hozzájárulás mellett az adatkezelő jogos érdeke is megjelenik, mint jogalap. Természetesen az érintettnek jogában áll az adatkezeléshez hoz-

[17] Kovács–Miklós 2021, 9–21.
[18] GDPR 4. cikk 2.
[19] Buzás et al. 95.

zájárulását megtagadni, a jogos érdekre alapított adatkezelés ellen pedig tiltakozni ebben az esetben is.

A személyes adatok különleges kategóriáinak kezelésével kapcsolatban a szabályozás kiindulópontja az, hogy azok kezelése és így a biometrikus adatok kezelése is tilos. Erre tekintettel, a biometrikus adatok kezelése csak akkor történhet jogszerűen, amennyiben a rendelet 6. cikke szerinti jogalaptól függetlenül azonosításra és megjelölésre kerül legalább egy, a 9. cikk (2) bekezdésében felsorolt valamely speciális feltétel is. A 6. cikk szerinti választott jogalapnak és a 9. cikk szerinti speciális esetkörnek nem kell egymással összefüggésben állnia.[20] A rendelet lehetővé teszi továbbá a tagállamok számára, hogy további feltételeket – köztük korlátozásokat – tartsanak hatályban, illetve vezessenek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan. Az Európai Adatvédelmi Testület elődje, a 29. cikk szerinti Adatvédelmi Munkacsoport a biometrikus adatok kezelésének követelményeit részletesen elemezte a biometrikus technológiák terén történt fejleményekről szóló véleményében.[21] A Munkacsoport rögzítette, hogy a biometrikus adatok csak abban az esetben kezelhetőek, ha rendelkezésre áll megfelelő jogalap és a gyűjtésük, illetve további kezelésük célja szempontjából a kezelés megfelelő, releváns és nem túlzott mértékű.

2.2 Adatbiztonság

Az elmúlt években a kiberfenyegetések száma és az általuk okozott kár nagysága meredeken emelkedett. Egyes becslések szerint az internetes bűnözéssel okozott kár 2020-ban meghaladta a 4,2 milliárd dollárt.[22] A digitális eszközök számának növekedésével azonban nem nőtt együtt a felhasználók tudatossága. Egy adatvédelmi incidens rendkívül hátrányos következményekkel járhat az incidenssel érintett személyekre nézve, különösen akkor, ha a személyes adatok különleges kategóriái is érintettek. Erre tekintettel a GDPR már alapelvi szinten rögzíti az integritás és bizal-

[20] Buzás et al. 141.

[21] 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről.

[22] Stouffer 2021.

mas jelleg elvét, amely alapján a személyes adatok „kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve".[23] A biztonság fenntartása érdekében az adatkezelőnek kockázatelemzést kell végeznie, amely során felméri az adatkezeléssel összefüggő kockázatokat és gondoskodik a kockázatokkal arányos adatbiztonsági intézkedések meghozataláról. Az intézkedések mérlegelése során figyelembe kell venni a tudomány és technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit.[24] Az alapelveken túlmenően a GDPR a beépített és alapértelmezett adatvédelem kötelezettségével megköveteli az adatkezelőktől azt, hogy már az adatkezelés megkezdése előtt olyan technikai és szervezési intézkedéseket foganatosítsanak, amelyek ténylegesen érvényre juttatják az adatvédelmi alapelveket és garantáljak az érintettek jogait. Konkrétabban ez azt jelenti, hogy legyen szó bármilyen adatkezelésről, például egy vállalati folyamat, vagy egy IoT-eszköz tervezéséről, azokat már a tervezésnél úgy kell megalkotni, hogy az a szükségeshez képest a legkevesebb személyes adat kezelése történjen, és az adatkezelés kockázatához mérten megfelelően biztonságos legyen. A rendelet külön kiemeli az álnevesítést és a titkosítást mint intézkedéseket, de ebbe a körbe tartozik az adatok visszaállíthatósága és a meghozott intézkedések rendszeres tesztelése, felmérése is.

2.3 Harmadik országba történő adattovábbítás

A digitális gazdaságokban a személyes adatok útja jellemzően nincs tekintettel az országhatárokra, hanem összetett, gyakran több országot magában foglaló láncolat útján jut el a különböző adatkezelőkhöz és adatfeldolgozókhoz. A nemzetközi adattovábbítások egyre növekvő mennyisége azonban új kihívásokat állít a személyes adatok védelme elé. A rendelet

[23] GDPR 5. cikk (1) f).

[24] GDPR 83. preambulumbekezdés.

alapján olyan személyes adatok továbbítására, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, amennyiben az adatkezelő és az adatfeldolgozó megfelel a rendeletben foglalt, adattovábbításra vonatkozó követelményeknek.[25] A rendelet értelmező rendelkezései azonban nem határozzák meg a harmadik ország fogalmát. Erre vonatkozóan az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) nyújt meghatározást, amely alapján harmadik ország minden olyan állam, amely nem EGT-állam, EGT-államok pedig az Európai Unió tagállamai, valamint Izland, Liechtenstein és Norvégia.[26] A Magyarország és ezen államok között történő adattovábbítás jogi megítélése azonos, azokra úgy kell tekinteni, mint ha az adattovábbítás Magyarország területén belül történne.

Az egyik lehetséges módja a személyes adatok nemzetközi továbbításának, amennyiben az Európai Unió Bizottsága egy adott harmadik országról vagy nemzetközi szervezetről megállapította, hogy adatvédelmi szempontból megfelelő védelmi szintet biztosít. Az eljárás során az Európai Bizottság vizsgálja a jogállamiság és az emberi jogok helyzetét, az adatvédelmi szabályokat, valamint az érintettek közigazgatási és bírósági jogorvoslatot is magukban foglaló jogait. Fontos szempont továbbá, hogy a vizsgált harmadik országban létezik-e egy vagy több olyan független és hatékonyan működő felügyeleti hatóság, amely felelős az adatvédelmi szabályok betartásának biztosításáért és végrehajtásáért.[27] Az Európai Bizottság a védelmi szint megfelelőségéről végrehajtási jogi aktusok útján határoz és rendelkezik a legalább négyévente elvégzendő felülvizsgálati mechanizmusról. Jelenleg Andorra, Argentína, a Feröer-szigetek, Kanada, Guernsey, Izrael, a Man-sziget, Japán, Jersey, Új-Zéland, az Egyesült Királyság és Uruguay vonatkozásában került megállapításra, hogy biztosítják a személyes adatok megfelelő védelmének szintjét. Kanada vonatkozásában a megfelelőségi határozat csak azokra az adatimportőrökre vonatkozik, amelyek a személyes információk védelméről és az elektronikus

[25] GDPR 44. cikk

[26] Infotv. 3. § 24.

[27] GDPR 45. cikk.

dokumentumokról szóló törvény hatálya alá tartoznak. 2021. június 16. napján megkezdődött megfelelőségi határozat meghozatalához szükséges folyamat Dél-Korea vonatkozásában is.

A fenti országlistát áttekintve szembetűnő az Egyesült Államok hiánya mind gazdasági erejére, mind digitális gazdaságának fejlettségére tekintettel. 2000-ben az Európai Bizottság és az Egyesült Államok Kereskedelmi Minisztériuma között létrejött a *Safe Harbour* megfelelőségi határozat, amelyet később azonban az Európai Bíróság a Schrems I. ügyben hozott határozatával érvénytelennek nyilvánított. Az ügy alapját az képezte, hogy Maximilian Schrems adatvédelmi aktivista osztrák állampolgár panaszt nyújtott be a Facebook ellen az adatvédelmi biztosnál, kérve a Facebook Ireland – és a Facebook Inc. közötti adattovábbítás megtiltását, tekintettel arra, hogy a továbbított adatok az Egyesült Államok hírszerző szolgálatai által folyamatos megfigyelés és lehallgatás alatt álltak. A kérelem az Edward Snowden által az Egyesült Államok hírszerző szolgálatainak a tevékenységét bemutató kiszivárogtatott információkra hivatkozott.[28] A Bíróság döntése után az Európai Bizottság az Adatvédelmi Pajzs (*Privacy Shield*) elnevezésű új mechanizmust kötötte meg az Egyesült Államokkal. Ez továbbra is egy öntanúsítási rendszer volt, amelyben az egyesült államokbeli cégek önkéntesen vehettek részt, a sikeres regisztráció és tanúsítás esetén azonban a megfelelő védelmi szint megvalósultnak volt tekintendő a regisztrált cégek tekintetében. Adatvédelmi szempontból a 2020-as év egyik legjelentősebb fejleménye volt, hogy az Európai Bíróság a Schrems II. ítéletben megállapította az Adatvédelmi Pajzs érvénytelenségét is. [29] A határozat meghozatalának időpontjában az Adatvédelmi Pajzs mechanizmusban több, mint ötezer adatkezelő volt nyilvántartva, köztük a digitális gazdaság legnagyobb szereplőivel. A döntés természetesen nem zárta ki a személyes adatok Európából az Egyesült Államokba történő továbbításának lehetőséget, azonban a megfelelőségi határozat érvénytelensége miatt az adatkezelőknek más módot kell választaniuk. A Bíróság két döntése között csak öt év telt el, az eltelt időszak alatt azonban a világsajtó az egymást érő súlyos adatvédelmi incidensektől volt hangos. Az Európai Parlament Schrems

[28] C-362/14. sz. ügy.
[29] C-311/18. sz. ügy.

II. döntéssel kapcsolatos 2021. májusi állásfoglalásában külön is megemlíti a Cambridge Analytica-incidenst, amely során a Facebook 87 millió felhasználójának adataival élhettek vissza, amelyből 2,7 millió uniós állampolgárhoz volt köthető. A Parlament állásfoglalásában kiemeli, hogy az Egyesült Államokba történő adattovábbítások védelme terén fennálló komoly hiányosságokra tekintettel támogatni kell az európai adattárolási eszközökbe (például a felhőszolgáltatásba) irányuló beruházásokat annak érdekében, hogy az Európai Unió kevésbé függjön a harmadik országok tárolási kapacitásaitól, és nagyobb stratégiai autonómiával rendelkezzen az adatgazdálkodás és -védelem szempontjából.[30] Amennyiben az adott harmadik országra vonatkozóan nincs az Európai Bizottság által elfogadott megfelelőségi határozat, úgy az adattovábbítás más lehetőségeit kell alkalmazni a személyes adatok védelmi szintjének megfelelő biztosítása érdekében. A rendelet egy taxatív felsorolás keretében határozza meg azokat a lehetőségeket, amelyek esetében az adatvédelmi hatóság engedélye nélkül megvalósulhat az adattovábbítás.

Az egyik ilyen széles körben elterjedt lehetőség a kötelező erejű vállalati szabályok alkalmazása lehet. Ez a megoldás leginkább olyan vállalatcsoportok részére lehet előnyös, amelyek az Európai Unió valamely tagállamának területén rendelkeznek tevékenységi hellyel és a személyes adatok továbbítását ugyanazon vállalkozáscsoporton belül egy vagy több harmadik országba végzik. A szabályzatot a nemzeti felügyeleti hatóság hagyja jóvá, amely a döntéstervezetet a GDPR 64. § (1) f) pontja alapján, az egységességi mechanizmus keretében közli az Európai Adatvédelmi Testülettel véleményezés céljából. A globalizált gazdaságban egyre gyakoribb, hogy vállalatcsoportok egyes funkciókat csoportszinten bizonyos országokba, szakosított szolgáltató központokba szervezzenek. Ilyen esetekben jelentősen megkönnyítheti a cégcsoporton belüli adattovábbítást egy elfogadott és a felügyelő hatóság által jóváhagyott kötelező erejű vállalati szabály.

További módja lehet a személyes adatok harmadik országba történő továbbításának az általános adatvédelmi kikötések alkalmazása is. Az általános adatvédelmi kikötések (SCC – *standard contractual clauses*) az Európai Bizottság által előzetesen jóváhagyott szerződéses kikötések,

[30] Európai adatstratégia.

amelyek biztosítják a védelem megfelelő szintjét az adattovábbítás során. 2021. június 4-én az Európai Bizottság kibocsátotta a korábban már említett Schrems II. ítélet következtében felülvizsgált és módosított adatvédelmi kikötéseket. A felülvizsgált és modernizált kikötések a korábbi 95/46/EK adatvédelmi irányelv alatt elfogadott kikötések helyébe lépnek. Az új kikötések elfogadásával 2021. szeptember 27. napjától a korábban elfogadott kikötéseket már nem lehet használni új szerződések megkötése során, míg a korábban megkötött szerződések 2022. december 27. napjáig érvényesek, amennyiben a szerződés tárgyát képző adatkezelés nem változik. Az Európai Bíróság Schrems II. döntését követően számos egyesült államokbeli társaság létesített adatközpontokat és helyezte át adatkezelését az Európai Unió területére. Ezek a társaságok azonban továbbra is az Európai Bíróság által kifogásolt, korlátlan megfigyelést lehetővé tévő amerikai jogszabály (FISA – *Foreign Intelligence Surveillance Act*) hatálya alatt maradtak. Erre tekintettel ezen társaságok adatkezelése esetén az általános adatvédelmi kikötések nem elégségesek, az adatkezelés jogszerűségéhez szükséges kockázatelemzés végzése és a megfelelő garanciák szerződésbe foglalása is.

A harmadik országba történő adattovábbításhoz abban az esetben sem szükséges a felügyelő hatóság jóváhagyása, amennyiben az adattovábbítás akkreditált magatartási kódex hatálya alatt áll, vagy amennyiben valamilyen jóváhagyott tanúsítási mechanizmus keretében kiállított tanúsítvány áll az adatkezelő rendelkezésre. Jelenleg azonban sem a magatartási kódex, sem az öntanúsítási mechanizmus vonatkozásában nem áll még rendelkezésre széleskörű tapasztalat annak gyakorlati alkalmazásáról, ugyanis az első kérelmeket még csak 2021 májusában kezdte el véleményezni az Európai Adatvédelmi Testület.

2.4 A GDPR mérlege a digitális stratégia céljainak tükrében

Amint az már fentebb ismertetésre került, az európai adatok túlnyomó része felett néhány amerikai és kínai technológiai vállalat rendelkezik befolyással. Ez negatív hatással van az innovációra, valamint torzítja a piacot is. A GDPR rögzíti az érintettek rendelkezési jogát, valamint az adatkezelők adatkezeléssel kapcsolatos tájékoztatási kötelezettségét. Ez egy erős garancia az érintettek jogainak védelme érdekében, azonban jelen-

tőségét csorbítja, hogy a tájékoztatásból az érintettek számára sem a rendelkezésre bocsátott személyes adataik értéke, sem azok további útja és felhasználása nem derül ki világosan. Ebből adódóan a felhasználók nem tudják összevetni a kapott szolgáltatás értékét az általuk rendelkezésre bocsátott személyes adatok értékével és így a tranzakció értékarányosságát sem tudják megítélni. További probléma, hogy számos technológiai vállalat szolgáltatását csak ebben a látszólag ingyenes üzleti modellben kínálja a felhasználók számára, akik emiatt akkor sem tudnak fizetni érte – a kevesebb személyes adat rendelkezésre bocsátása mellett – amennyiben szeretnének.

A személyes adatok az Európai Unióból történő elszívására tehát a GDPR nincs hatással, az adatkizsákmányolást érdemben nem akadályozza.[31] Ebből a szempontból megállapítható, hogy az érintettek számára a GDPR rendelkezései ugyan magasabb védelmi szintet jelentenek, azonban az általános adatvédelmi rendelet az európai adatgazdaság megerősítéséhez nem járul hozzá.

3. Adatokkal kapcsolatos rendeletek

*3.1 Adatrendelet (**Data Act**)-tervezet*

A Bizottság 2020-ban közzétett adatstratégiájában a digitális gazdaság megerősítése érdekében kiemelt prioritásként kezeli az ehhez szükséges jogszabályi keretrendszer megteremtését. Az adatrendelet célja ösztönözni a vállalkozások közötti adatmegosztást az adatok felhasználása és az adatokhoz való hozzáférés megkönnyítése érdekében, elősegítve az EU adatgazdaságában rejlő lehetőségek teljes kihasználását. Tekintettel arra, hogy a felhőszolgáltatók jellemzően harmadik országokban regisztrált társaságok, a jogszabálytervezet a mikro-, kis és közepes vállalkozások támogatása céljából korlátozni kívánja az erőfölényes, egyoldalú szerződéskötési gyakorlatot, valamint szélesíteni kívánja az adatokhoz való hozzáférés jogát. Ezen túlmenően a tervek között szerepel

[31] Tóth Á. 2021.

az adatbázisok jogi védelméről szóló 96/9/EK irányelv felülvizsgálata, valamint a szellemi tulajdon fokozott védelmével kapcsolatos garanciák kialakítása, amennyiben az adatkezelés harmadik országban bejegyzett felhőszolgáltatók által történik. Végül a rendelet az adathordozhatóság megteremtése érdekében a felhasználó számára rögzítené az ehhez való jogot, míg a szolgáltatók irányából rögzítené az interoperabilitás követelményét. [32]

3.2 A nem személyes adatok Európai Unióban való szabad áramlásának keretéről szóló 2018/1807 rendelet (FFD)

Míg a személyes adatok kezelését az általános adatvédelmi rendelet szabályozza, addig a nem személyes adatok kezelésére az FFD rendelet vonatkozik. Nem személyes adatnak minősül minden olyan adat, amely kívül esik az általános adatvédelmi rendelet személyes adat meghatározásán. Az adatkezelés fogalmát a rendelet a legszélesebb körben használja, amely valamennyi típusú informatikai rendszer használatát magában foglalja függetlenül attól, hogy azok a felhasználó helyiségében vagy területén találhatóak-e, vagy kiszervezték-e azokat egy szolgáltatóhoz. A GDPR és az FFD rendelet koherens szabályrendszert biztosít a különböző típusú adatok szabad áramlásának biztosítására, egyik rendelet sem írja elő a különböző típusú adatok elkülönített tárolásának követelményét. Az egyre bővülő dolgok internete, a mesterséges intelligencia és a gépi tanulás a nem személyes adatok jelentős forrásainak számítanak. A nem személyes adatok egyik példája a nagy adathalmazok elemzéséhez használt összesített és anonimizált adatkészletek. Amennyiben a technológiai fejlődés lehetővé teszi az anonimizált adatok személyes adatokká történő átalakítását, az ilyen adatokat személyes adatoknak kell tekinteni, és ennek megfelelően azokra már az általános adatvédelmi rendelet lesz alkalmazandó.[33]

Az Európai Unió működéséről szóló szerződésben (EUMSZ) rögzített négy szabadság részét képző letelepedés és szolgáltatásnyújtás szabadsága az adatkezelési szolgáltatásokra is alkalmazandó. Ezen alapszabadsá-

[32] Európai adatstratégia 13–14.

[33] FFD 9. preambulumbekezdés.

gok érvényesülését azonban a különböző nemzeti, regionális vagy helyi adatlokalizációt előíró jogszabályi követelmények korlátozzák. A rendelet meghatározása alapján adatlokalizációs követelménynek minősül bármely olyan jogszabályban rögzített kötelezettség, tilalom, amely előírja, hogy az adatkezelési tevékenységeket egy adott tagállam területén kell végezni, vagy akadályozza, hogy az adatkezelés bármely másik tagállamban történjen.[34] Ezzel egyenértékű hatása van a közjogi intézmények közigazgatási gyakorlataiból eredő követelményeknek is. Ilyen előírás lehet például, amely az adott tagállamban tanúsított vagy jóváhagyott eszközök, létesítmények használatát írja elő. A rendelet alapján tehát a nem személyes adatok Európai Unión belül történő továbbításának korlátozása adatlokalizációs követelményekkel tilos, ez alól kivételt csak a közbiztonsági okok jelentenek és azok is csak annyiban, amennyiben összhangban állnak az arányosság elvével. A rendelet célja, hogy a vállalkozások és a közjogi intézmények számára lehetővé tegye, hogy az adatok tárolásának helye az Európai Unión belül az adatok keletkezésének helyétől függetlenül bárhol lehessen. Az átláthatóság megteremtése érdekében a tagállamoknak kötelező közzétenniük a naprakész információkat a hatályos adatlokalizációs követelményeikről vagy egy nemzeti online felületen, vagy pedig egy központi uniós információs ponton. Az Európai Bizottság a hatályos nemzeti adatlokalizációs követelményeket a saját honlapján közzéteszi.

A német és a francia gazdasági miniszter 2020-ban jelentette be a GAIA-X projektet, egy nonprofit szakmai szövetséget mely végül hivatalosan 2021. januárjában indult el. Célja az európai felhőökoszisztéma létrehozása és az európai felhőszolgáltatók megerősítése az interoperabilitás, az átláthatóság és az adatok hordozhatóságára vonatkozó szabványok kidolgozása által. A szabványok alapján nem egy új, nagyobb európai felhőszolgáltató jönne létre, hanem megvalósulna a fenti elvek mentén hálózatba szervezett felhőszolgáltatók közössége. A projektet azonban számos kritika érte elkésettsége, túlbürokratizált szervezete és a nagy amerikai szolgáltatók tagként történő felvétele miatt.[35] Beszédes adat, hogy az Európai Unió felhőszolgáltatási piacának 69 százaléka az Amazon, Microsoft és a Google kezében összpontosul, míg az európai szolgáltatók közül a maga 2 százalékos piaci

[34] FFD rendelet 3. cikk 5.

[35] Goujard–Cerulus 2021.

részesedésével a Deutsche Telekom rendelkezik. Ezek alapján kérdéses, hogy végül sikerül-e megvalósítani a kitűzött célokat és megvédeni az Európai Unió technológiai szuverenitását a külföldi befolyástól.

3.3 A kiberbiztonságról szóló 2019/881 rendelet (CSA)

Az uniós szintű kiberbiztonsági szabályozás szükségességének indoka az, hogy napjainkra a hálózati és információs rendszerek, a távközlési hálózatok és szolgáltatások létfontosságú szerepet töltenek be a társadalom működésében. Ezek a technológiák adják a gazdasági növekedés alapját az olyan ágazatokban, mint az egészségügy, az energiaügy, a pénzügy és a közlekedés.

A hálózati és információs rendszerek használatának mértéke jelentősen növekszik az Európai Unióban, mind a természetes személyek, mind a gazdaság szereplői körében. Folyamatosan nő azoknak a termékeknek és szolgáltatásoknak a száma, amelyek alapvető jellemzői a digitalizálás és az összekapcsoltság, illetve a dolgok internetének terjedésével a következő évtizedben várhatóan rendkívül magas számú összekapcsolt digitális eszközt fognak az Európai Unióban használatba venni.[36] Az eszközök mennyiségével arányosan azonban sem azok biztonsági színvonala, sem a felhasználók kiberbiztonsági tudatossága nem növekszik, amely jelentős veszélyeket rejt magában, hiszen kiszolgáltatottá teszi a társadalmat a kiberfenyegetésekkel szemben. Tovább súlyosítja a helyzetet, hogy jelenleg nincs olyan, az Európai Unióban kötelező vagy széles körben elterjedt önkéntes tanúsítási mechanizmus, amely megfelelő információval szolgálhatna a felhasználók részére az információs és kommunikációs termékek, szolgáltatások és folyamatok megbízhatóságáról és kiberbiztonsági jellemzőiről.

A kiberbiztonságról szóló rendelet két fő célja egyrészt az Európai Unió kiberbiztonságának erősítése és a belső piac megfelelő működésének érdekében megerősíteni az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA), másrészt az ENISA közreműködésével kialakítani az európai kiberbiztonsági tanúsítási rendszereket. Ennek érdekében a rendelet hatályon kívül helyezte az ENISA-ról szóló korábbi 526/2013/

[36] CSA rendelet 2. preambulumbekezdés.

EU rendeletet és 2019. június 27-től határozatlan időtartamra létrehozta az ENISA-t, mint az Európai Unió kiberbiztonsággal foglalkozó szakosított, jogi személyiséggel rendelkező szervét. Az ENISA rendkívül sokrétű feladatot lát el, többek között kiberbiztonsággal kapcsolatos szakértőként tanácsot ad, uniós információs és tudásközpontként működik, segítséget nyújt tagállami szintű kiberbiztonsági stratégiák kidolgozásához és aktualizálásához, valamint kidolgozza a rendeletben felvázolt kiberbiztonsági tanúsítási rendszereket.

A már elkészült tervezetek és a rendelet alapján a kidolgozás alatt álló tanúsítási rendszerek az „alap", a „jelentős" és a „magas" megbízhatósági szinteket fogják megkülönböztetni. A tanúsítás lehetőséget biztosít az „alap" megbízhatósági szint esetén megfelelőségi önértékelésre is, amely során a gyártó vagy szolgáltató fogja saját felelőssége alatt tanúsítani terméke megfelelőségét a kiberbiztonsági tanúsítási rendszer követelményeivel. Ebből a szempontból a tanúsítási mechanizmus hasonlítani fog a már létező CE jelölésre, amelynél a gyártó szintén saját felelőssége mellett tanúsítja terméke megfelelőségét az alkalmazandó Európai Uniós előírásoknak. A tanúsítványoknak való megfelelésről és ellenőrzések végrehajtásáról a tagállamok által kijelölt egy vagy több nemzeti kiberbiztonsági tanúsító hatóság gondoskodik. Az ENISA a tanúsítási mechanizmusra vonatkozó tervezetének legújabb, V1.1.1. változatát 2021. május 25-én tette közzé. A tanúsítási mechanizmus végleges, az Európai Bizottság által jogi aktusban történő kihirdetésére várhatóan 2022-ben kerül majd sor.

4. Az Európai Parlament és a Tanács 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

A jelenleg hatályos elektronikus hírközlési adatvédelmi irányelvet, vagy közismertebb nevén süti (angolul *cookie*) irányelvet még 2002-ben fogadták el a hírközlési piac szabályozásának részeként. 2009-es módosításától számítva is eltelt már több, mint egy évtized. Az Európai Bizottság a Digitális Európa

Stratégia részeként meghirdette az adatvédelmi szabályok modernizációját. Ennek részeként került a GDPR is elfogadásra, és az eredeti cél az ePrivacy irányelvet felváltó rendelet kapcsán is a 2018. május 25. napi hatálybalépés volt. Ehhez képest a tagállamok az első szövegtervezetet csak 2021. január 5. napján fogadták el, és ekkor kezdődött csak el a háromoldalú egyeztetés az Európai Parlament, a Bizottság és a Tanács között. Erre tekintettel a rendelet jelentős csúszásban van, és nem várható, hogy 2023 előtt elfogadják a végleges szövegtervezetet, vagy hogy 2025 előtt hatályba lépjen.

Mára az irányelv néhány szabálya elavultnak tekinthető, és az általános adatvédelmi rendelet maga utal 173. preambulumbekezdésében az irányelv felülvizsgálatának szükségességére, amikor rögzíti, hogy a GDPR elfogadását követően az irányelvet a két jogszabály közötti összhang megteremtése érdekében felül kell vizsgálni. Míg az általános adatvédelmi rendelet a személyes adatok kezelését általánosságban szabályozza, addig az elektronikus hírközlési adatvédelmi irányelv az elektronikus hírközlési ágazatban történő személyes adatkezelésekre vonatkozik, tehát a GDPR-hoz képest *lex specialis,* rendelkezései pontosítják és kiegészítik a GDPR rendelkezéseit. Amint arra fentebb már történt utalás, egy honlap látogatásakor adatkezelés történik, amelyre vonatkozóan az irányelv részletes útmutatással szolgál. A honlapok azonosításra szolgáló kódsorozatokkal – úgynevezett sütikkel (*cookie*) – biztosítják a honlap alapvető funkcióit, elemzik hirdetéseik hatékonyságát és azonosítják az egyedi látogatókat. A honlap látogatói az irányelv alapján jogosultak megtagadni a sütik vagy hasonló eszközök végberendezésükön – azaz számítógépükön, laptopjukon, telefonjukon – történő tárolását. A sütik használatára vonatkozó tájékoztatás és a megtagadás joga egy csatlakozás alkalmával egyszer ajánlható fel, a felhasználó választása azonban kiterjedhet a későbbi csatlakozások során történő használatára is.

5. Konklúzió

Az Európai Unió a digitális gazdasági versenyben Észak-Amerikához és Ázsiához képest lemaradásban van. Az unió lélekszáma, gazdasági ereje és a belső piac mérete okán a digitális gazdaság jelentős fejlődés előtt áll, és ezt az európai döntéshozók is felismerték. Az Európai Bizottság 2021.

március 9-én bemutatta az Európai Unió 2030-ig megvalósítandó digitális átalakulására vonatkozó jövőképét és megoldási javaslatait, amely alapján a megkésett digitalizációt a megfelelő jogszabályi keretrendszer megalkotásával, az európai értékek, valamint a személyek digitális jogainak érvényesítésével kívánja elősegíteni.

Az általános adatvédelmi rendelet jelentős előrelépés volt a személyek személyes adatok védelméhez fűződő jogainak megerősítésében és az adatvédelmi tudatosság növelésében mind az Európai Unión belül, mind a világ más részein. A rendelet elvei és szellemisége közvetetten mintaként szolgálnak harmadik országok jogalkotása számára, míg a megfelelőségi határozatok révén közvetlenül is befolyásolja számos állam adatvédelmi szabályozását. A határon átnyúló hatályának köszönhetően hatékony eszköz a harmadik országbeli adatkezelők tevékenységének befolyásolására is. A luxemburgi adatvédelmi hatóság, a *Commission Nationale de l'Informatique et des Libertés* által 2021-ben az Amazonra kiszabott 746 millió eurós, valamint az ír adatvédelmi hatóság által szintén 2021-ben a WhatsAppra kiszabott 225 millió eurós adatvédelmi bírság nagyságrendileg nagyobb a korábbi rekordnak számító 50 millió eurós Google-bírsághoz képest. A hatóságok mindkét esetben kifogásolták a hiányos és homályos adatkezelési tájékoztatást, valamint az Amazon esetében a sütik szabálytalan alkalmazását, amely jelentősen megnehezítette a felhasználók számára hozzájárulásuk megtagadását. Látható, hogy három évvel az adatvédelmi rendelet elfogadását követően mintha a szabályozó hatóságok is elkezdték volna komolyabban venni a rendeletben foglalt kényszerítő eszközök alkalmazását. A rendelet egységesítette az Európai Uniós adatvédelmi szabályozást és az egyablakos ügyintézés (*one stop shop mechanism*) alapján az a tagállami felügyeleti hatóság jogosult eljárni egy adott adatkezelő vonatkozásában, amely államban az adott szolgáltató székhellyel rendelkezik. A nagy technológiai cégek – jellemzően adózási megfontolásokból – általában néhány tagállamban, jellemzően Írországban vagy Luxemburgban alakították ki európai uniós székhelyüket. Ezek a cégek még a kedvezményes adókulcsok mellett is hatalmas összegekkel járulnak hozzá az adott tagállam költségvetéséhez. Ez a helyzet létrehozott egyfajta érdekellentét, hiszen a hatóságoknak érvényre kell juttatniuk a GDPR rendelkezéseit, azonban a tagállamok oldaláról nagy a nyomás, hogy ezek a társaságok továbbra is fenntartsák székhelyüket az adott tagállamban. Az ír adatvédelmi hatóság egyetlen bírságot sem szabott ki nagy technológiai cégekre

a GDPR elfogadását követő két évben. Többen – köztük a német adatvédelmi hatóság vezetője is – kritizálták emiatt a GDPR rendszerét, kiemelve annak nem hatékony voltát.[37] A 2021-es bírságok és azok nagysága egy lépés a rendszer működőképességének bizonyítása irányába és egy válasz a korábban megfogalmazott kritikákra.

A személyes adatok fokozott védelme azonban az európai digitális stratégiának csak egyik fontos eleme. Az okoseszközök elterjedése és az összekapcsoltság miatt a gazdaság és a társadalom egyre kiszolgáltatottabb a kibertérből érkező fenyegetésekkel szemben, ezt támasztja alá a kibertámadások egyre növekvő száma is. A 2021-es év sajnos bővelkedett példákban, azonban még azok közül is kiemelkedett az amerikai Colonial csővezeték megbénítása, amely következtében napokig akadozott az Egyesült Államok keleti partvidékének üzemanyag-ellátása. A támadás a csővezetéket üzemeltető társaság nem megfelelő technikai és szervezési intézkedései következtében lehetett sikeres. A kibertámadások ráadásul nem feltétlenül egy adott országon belül zajlanak, hanem bűnözői csoportok képesek határokon átnyúló támadások megszervezésére és végrehajtására is. A nemzeti hatóságok hatásköre nemzeti szintű, illetékességük csak az állam területére szól. A nemzeti hatóságok határon átnyúló együttműködése sokszor körülményes, ezért hatékony és összehangolt uniós szintű reagálásra és válságkezelésre van szükség, amelyhez a megfelelő jogszabályi keretrendszeren túl szükséges az Európai Unión belül a kölcsönös segítségnyújtás támogatása is.

Az egységes európai tanúsítási mechanizmus hatályba lépése remélhetőleg egy lépés a biztonságosabb IoT-eszközök irányába, amelyre a tapasztalatok alapján nagy szükség van. A gyártók sok esetben a legalapvetőbb technikai intézkedéseket sem alkalmazzák az IoT-eszközök biztonságossá tétele érdekében. Kutatók vizsgálata alapján az IoT-eszközök sérülékenysége továbbra is jelentős kockázatot rejt a felhasználókra nézve.[38] Könnyű belátni, hogy egy beszélő gyerekjáték, egy drón vagy egy kamerarendszer felett elvesztett irányítás rendkívül súlyos következményekkel járhat. Jelenleg a legtöbb állam nem rendelkezik

[37] Neurerer 2020.
[38] Hampson 2019.

IoT-specifikus szabályozással, biztonsági követelményekkel. A gyártók leginkább ágazati nonprofit és iparági szervezetek által kiadott különböző nem kötelező ajánlásokra, iránymutatásokra és legjobb gyakorlatokra támaszkodhatnak az IoT-eszközök fejlesztése során. Egyes államok azonban már felismerték a terület szabályozatlanságával járó kockázatokat. Szingapúr, Hongkong, Szaúd-Arábia és az Egyesült Arab Emírségek csak néhány olyan állam, amely rendelkezik dedikált IoT-stratégiával és vonatkozó jogszabályokkal, biztonsági előírásokkal. Európában az Egyesült Királyság már bejelentette a maga *Secure by Design* elnevezésű jogalkotási programját, amely célja egy IoT-specifikus jogszabályi keretrendszer és egy tanúsítási mechanizmus létrehozása. Ahogy egyre több állam fogadja el a maga IoT szabályozását, úgy fennáll a veszélye annak, hogy a különböző védelmi szintek és követelmények mentén a piac széttagolódik, amely visszafogja az innovációt. Erre tekintettel is előnyös, hogy az Európai Unió esetében közös, a 27 tagállamot magában foglaló tanúsítási mechanizmus kerül majd elfogadásra.

Az, hogy mely régiók, államok lesznek a digitális átállás legnagyobb nyertesei, majd csak évek múltán fog egyértelműen kirajzolódni. Az is igaz, hogy jogalkotói iránymutatás és megfelelő jogszabályi keretrendszer nélkül kicsi az esélye, hogy a piac magától érvényesítse azokat az értékeket és elveket, amelyek fontosságát az Európai Bizottság adatstratégiájában külön is kiemelte. Fontos azonban szem előtt tartani azt, hogy a túlszabályozás gyakran legalább annyira károsan hat az innovációra és a piac működésére, mint az alulszabályozottság.

Irodalom

Buzás, Péter – Péterfalvi, Attila – Révész, Balázs 2018: *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer.

Jóri, András – Soós, Andrea Klára – Bártfai, Zsolt – Hári, Anita 2018: *A GDPR magyarázata.* Budapest, HVG-ORAC Lap- és Könyvkiadó.

Kovács, Tibor – Miklós, Gellért 2021: A biometrikus rendszerek adatvédelmi szempontú elemzése. *Biztonságtudományi Szemle,* 3. évfolyam, 3, 9–21.

Tóth, András 2021: Az Európai Unió (szabályozási) útja a szuverenitás felé az adatalapú gazdaságban. *Európai Tükör,* 24. évfolyam, 2, 27–56.

Tóth, András 2021: A tisztességes adatkereskedelmet biztosító szabályozás szükségességéről. *Állam- és Jogtudomány,* 62 (3), 100–121.

Interneten megjelent források

29. cikk szerinti adatvédelmi munkacsoport 2012: 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf (letöltve 2021. 12. 13.).

Európai Befektetési Bank 2020: Who is prepared for the new digital age? https://www.eib.org/attachments/efs/eibis_2019_report_on_digitalisation_en.pdf (letöltve 2021. 12. 13.).

Európai Bizottság 2020: Európai adatstratégia. https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf (letöltve 2021. 12. 13.).

Goujard, Clothilde – Cerulus, Laurens 2021: *Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project.* https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/ (letöltve 2021. 12. 13.).

Hampson, Michelle 2019: *IoT Security Risks: Drones, Vibrators, and Kids' Toys Are Still Vulnerable to Hacking.* https://spectrum.ieee.org/iot-security-risks-drones-vibrators-iot-devices-kids-toys-vulnerable-to-hacking (letöltve 2021. 12. 13.).

Neurerer, Dietmar 2020: *Datenschützer Kelber bringt neue EU-Behörde gegen Facebook & Co. ins Spiel.* https://www.handelsblatt.com/politik/deutschland/datenschutz-verstoesse-datenschuetzer-kelber-bringt-neue-eu-behoerde-gegen-facebook-und-co-ins-spiel/25479302.html?ticket=ST-7473648-LaJqaLcCSdep5GGMKDre-cas01.example.org (letöltve 2021. 12. 13.).

Stouffer, Clare 2021: *115 cybersecurity statistics and trends you need to know in 2021.* https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html (letöltve 2021. 12. 13.).