JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

A GDPR múltja, jelene, és jövője

Szerző:

dr. Vörös Viktor

Kaposvár, 2022. június 22.

I. Bevezetés

Négy betű, amely már több mint hat éve lázban tartja a digitális, és a „való” világot egyaránt. De mi is az a GDPR?

Nem más, mint az Európai Unió 2016. május 24-én hatályba lépett, (de csak 2018. május 25-től alkalmazandó) új általános adatvédelmi rendelete, teljes nevén „Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről”.

A GDPR mozaikszó a rendelet angol elnevezésének (General Data Protection Regulation) kezdőbetűiből áll össze.

Amint az a rendelet teljes címéből is látszik, a GDPR egy több, mint 20 esztendős szabályozást nyugdíjazott. A 95/46/EK irányelv gyakorlatilag akkor született, amikor az adatvédelem, mint alapjog épp csak kikristályosodni kezdett. Az azóta eltelt több mint két évtized alatt azonban a technológia olyan gyors ütemben fejlődött, digitális világunk oly mértékben kitárult, hogy a korai szabályozás már közel sem volt alkalmas arra, hogy ellássa fő rendeltetését, a digitális adatbázisokba be- ,a világhálóra pedig kikerülve gyakorlatilag védtelenül bolyongó személyes adataink védelmét.

Elég csak belegondolni abba, hogy életünk jelentős részét már a digitális világban éljük. Nem könyvtárba járunk már tudásért és információért, hanem a világhálón böngészve csillapítjuk tudásvágyunkat. Egyre inkább elmaradnak a pár évtizede még a piros betűs ünnepek alatt postaládáinkat megtöltő képeslapok, helyette valamelyik közösségi platform csevegőprogramjában, jobb esetben e-mail címünkre kapunk egy körlevélben elküldött üdvözlőlapot. Számláinkat már nem a postán sorban állva, csekken, hanem online regisztrációt követően a szolgáltatónk által, de nem ritkán egy harmadik fél által üzemeltetett fizetési portálon át fizethetjük be. Személyi adatainkat minden hatóság, egészségügyi intézmény számítógépen tárolja, és ezen intézményekhez rendszerint ügyfélkaput is létesítünk. Nem is emlékszünk már, hogy hány honlapon, webshopban regisztráltunk és adtuk meg személyi adatainkat, az esetek többségében ráadásul ugyanazon felhasználónévvel és

jelszóval. Digitális lábnyomunk tehát folyamatosan növekszik, eltüntetése pedig nem hogy egyre nehezebbé, de gyakorlatilag lehetetlenné vált.[1] Olyan fogalmak és technológiák születtek meg és terjedtek el a betárcsázós internet óta, aminek az átlagos uniós polgár nem hogy a nevét nem tudja, de még a létezéséről sem tud. Az Unioban 2021-ben a közösségi oldalak használata jelentette az egyik leggyakoribb online tevékenységet. A 16–74 éves lakosság több mint fele (54%) használta az egyes közösségi hálózatokat (például a Facebook, Twitter és társaik) böngészésük során, amely mutató egyes tagállamokban ezt jócskán meg is haladja. Azoknak az aránya pedig akik még soha életükben nem használtak internetet, csupán 8 %-ra tehető.[2]

Mindezen körülményeket figyelembe véve már laikusként is megállapítható, hogy személyi, nem ritkán szenzitív adataink védelme, saját nézőpontunkból biztonságban tudása, adatkezelői szempontból pedig a szabályoknak megfelelő kezelése növekvő prioritást élvez az élet minden területén. A fenti folyamatok miatt kiemelten fontos, hogy a jogalanyok kontrollal rendelkezhessenek adataik, illetve azok áramlása felett, hiszen a személyes adatokkal való visszaélésnek a magánszféra sérelmén túl számos kézzelfogható, súlyos következménye is lehet. (pl. egy magyar példát említve: Egységes Tanulmányi Rendszerben tantárgyak leadása, vizsgákról való lejelentkezés.) [3]

Jelen tanulmány fő célja a GDPR elektronikus világra gyakorolt hatásainak feltárása, amire remek alkalmat szolgáltat a rendelet nemrég ünnepelt 4. születésnapja. Ennek során arra a kérdésre is keresem a választ, hogy az új szabályozás alkalmas-e az előbb említett cél elérésére, azaz a személyes adatok védelmének hatékonyabb ellátására. Ezen kérdések megválaszolásához elsősorban összehasonlító, komparatív, illetve részben jogtörténeti módszerekhez folyamodtam.

Az összehasonlító elemzéshez elkerülhetetlen a korai Uniós adatvédelmi szabályozás áttekintése a fő különbségek, illetve a fejlődési irányok feltérképezése érdekében, az Uniós, illetve a hazai szabályozás összevetése, azaz annak megállapítása, hogy mennyire „EU-konform” az adatvédelmi

[1] A „digitális lábnyom” (más néven kiber- vagy digitális árnyék) kifejezést azon nyomokra használják, amelyek a felhasználó online jelenléte után maradnak, és amelyekből következtetni lehet a tevékenységére. A kifejezést, annak első használatát legalábbis Nicholas Negropontenak tulajdonítják, aki a jelenségről „Digitális létezés” című 1995-ös megjelenésű könyvében írt először.
Nicholas Negroponte : Digitális létezés, Typotext Elektronikus Kiadó, Budapest, 2002. Eredeti megjelenés: Negroponte, N.: Being Digital, Coronet Books, 1995.

[2] Eurostat: Az információs társadalomra vonatkozó statisztika – háztartások és magánszemélyek https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage Letöltés dátuma: 2022. június 20.

[3] Szabó, M. D. (2005). Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs társadalom*, *2*, 44-54.

vagy „info” törvény. Meg kell ismerkednünk a személyi adataink hatékonyabb védelmét szolgáló új szabályozási módszerekkel, fogalmakkal, szankciókkal, amiről sokan a mai napig csak hiányos ismeretekkel rendelkeznek.

Mindezek előtt ugyanakkor – röviden - fel kell frissíteni az adatvédelem tárgyáról, magának a személyes adatokról, azok védelméhez való alapjogunkról korábban szerzett ismereteinket is. Tekintve, hogy a személyiségi jogok, amelyen belül rendszertanilag megtalálhatóak a személyes adatok védelméhez fűződő jogok, alapvetően polgári jogi jellegűek – már ha szabad ilyet mondani egy alapjogra – elsősorban civiljogi megközelítéssel lenne célszerű a vizsgálathoz hozzálátni.

Azonban, mint azt látni fogjuk, az adatvédelem alkotmányos, valamint hazai és nemzetközi jogszabályok általi intézményes védelmének térnyerése miatt az adatvédelmi jog egyre inkább „elközjogiasodik”.[4] Ennek az alapjogi áttekintésnek azonban távolról sem az a célja, hogy részletes alkotmányjogi okfejtésekbe és rendszerezésbe kezdjen. Csupán megpróbál rávilágítani arra, hogy miért is került az utóbbi időben előtérbe ez a viszonylag új keletű alapjog.

A tanulmány végén pedig röviden összegezni kívánom a GDPR első négy évének általános tapasztalatait, tendenciáit, valamint a gyakorlat során kikristályosodott problémák miatti módosításokat.

[4] Mészáros, J. (2017). *Adatvédelem a XXI. században és az internet világában* (Doctoral dissertation, szte). http://doktori.bibl.u-szeged.hu/3998/1/Meszaros_Janos_ertekezes.pdf Letöltés dátuma: 2022. június 20.

II. A személyes adat, és az adatvédelem mibenléte

A személyes adatok védelme, mint alapjog tehát a személyiségi jogok védelmén belüli speciális kategória. Abszolút szerkezetű jogviszony, mely a konkrét jogosult és a végtelen számú ismeretlen kötelezett között áll fent. Valamennyi személyiségi jogot felsorolni természetesen lehetetlen, és fontos szem előtt tartani azt is, hogy folyamatosan bővülő kategóriáról van szó, a technológiai evolúció során kifejlődő új alapjogokra pedig automatikusan kiterjed a fenti védelem. Az általános személyiségi jog generális jellegére az Alkotmánybíróság is rámutatott:
„Az általános személyiségi jog „anyajog", azaz olyan szubszidiárius alapjog, amelyet mind az alkotmánybíróság, mind a bíróságok minden esetben felhívhatnak az egyén autonómiájának védelmére, ha az adott tényállásra a konkrét, nevesített alapjogok egyike sem alkalmazható."[5]

Lenkovics Barnabás és Székely László az alábbiak szerint határozta meg a személyiségi jogok fogalmát: „A személyiségi jogok az embernek és a jogi személyeknek a társadalmi rendeltetésük betöltéséhez szükséges nem vagyoni értelemben vett integritást, háborítatlanságot, beavatkozástól mentes mozgásteret hivatott biztosítani, átlagosan tipizáltan a közfelfogáshoz igazodva, a konvenció által szükségtelennek minősített illetéktelen beavatkozások ellen."[6]

Elsőként határozzuk meg a személyes adat fogalmát. Ehhez segítségül kell hogy hívjuk az általános adatvédelmi törvényt, azaz az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt. (továbbiakban: Infotv.) E jogszabály 3. §-nak 2. pontja szerint személyes adat:
„az érintettre vonatkozó bármely információ."

Ezen igencsak általános megfogalmazást szerencsére a törvény az 1a. pontban kissé pontosítja, amikor is az azonosítható természetes személyről beszél:

„azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító

[5] 8/1990. (VI.23.) AB határozat
[6] Lenkovics, B. & Székely, L. (2000). *A személyi jog vázlata*. Eötvös József Könyvkiadó.

vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható."

Lényegében az Info tv. itt megpróbál egy kvázi taxatív felsorolást adni a legjellemzőbben előforduló személyes adatok köréről is, illetve hogy azok megsértése milyen élethelyzetekben, tevékenységek során lehetséges elviekben. A teljes felsorolás azonban természetesen lehetetlen, tekintve, hogy személyes adatnak minősül bármely, az érintettre vonatkozó információ.

Korábbi adatvédelmi törvényünk ennél sokkal részletesebben határozta meg a személyes adat fogalmát:
„Személyes adat bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet."[7]

Végül az új adatvédelmi rendelet az alábbiak szerint határozza meg a személyes adat fogalmát:
„személyes adat: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható."

Nehéz helyzetben van az is, aki egzakt fogalommeghatározásra adja a fejét az adatvédelem kapcsán. Elsősorban azért, mert az adatvédelem lényegében sokkal több, mint amit a neve sejtetni enged. A védelem tárgya ugyanis csak közvetlenül az adat, közvetve – és ténylegesen - az adatvédelem az érintett természetes személy személyiségi jogait védi.

[7] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról 2.§ 1.pont

Majtényi László meghatározása szerint „Az adatvédelem a személy, az ember, más szóval az adatalany védelmét, nem pedig magának az adatnak a védelmét jelenti."[8]

Jóri András így vélekedik az adatvédelem mibenlétéről:

„Az adatvédelem jellemzője, hogy a magánszféra védelmén belül értelmezhető az alábbiak szerint:
a) Az adatvédelem minden esetben a személy magánszférájának jogi védelmét jelenti, amely
b) az 1970-es évektől az elektronikai forradalom által egyre általánosabbá váló automatizált adatfeldolgozás veszélyeire válaszul jelent meg európában, és
c) általa nyújtott jogi védelem tartalma a fogalom megjelenése óta többször is jelentősen változott, illetőleg jelenleg is folyamatosan változásban van."[9]

Gyakorlatilag lehetetlen – és indokolatlan - feladat lenne valamennyi vonatkozó nemzetközi, uniós, illetve nemzeti szabályozásbeli megfogalmazást felsorolni jelen értekezés keretei között, ezért csak a legalapvetőbb jogszabályokra koncentrálok.

Az adatvédelemről szóló jogszabályok körében elsőként említendő az Európai Unió Alapjogi Chartája, ami a 8. cikkben rendelkezik a személyes adatok védelméről, és az információs önrendelkezési jogról.[10]
„(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.
(2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.
(3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie."

Lényegében ugyanezen rendelkezéseket erősíti meg az Európai Unió Működéséről Szóló Szerződés (EUMSZ) is, azzal, hogy nem részletezi a természetes személyek információs önrendelkezési jogának

[8]Majtényi, L. (1997) *Adatvédelem, információszabadság*, Alkotmány- és Jogpolitikai Intézet, Budapest
[9]Jóri, A. (2010). Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése. https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/jori-andras/jori-andras-vedes-ertekezes.pdf Letöltés dátuma: 2020. június 20.
[10]Az Európai Unió Alapjogi Chartája 8. cikk - A személyes adatok védelme

tartalmát, e helyett a személyes adatok jogszabályi illetve intézményi védelmére koncentrál:

„(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

(2) A természetes személyeknek az uniós intézmények, szervek és hivatalok által, illetve az uniós jog alkalmazási körébe tartozó tevékenységeik során a személyes adataiknak a tagállamok által végzett feldolgozása tekintetében történő védelmére, valamint az ilyen adatok szabad áramlására vonatkozó szabályokat rendes jogalkotási eljárás keretében az Európai Parlament és a Tanács állapítja meg. E szabályok tiszteletben tartását független hatóságok ellenőrzik."[11]

A Chartához és az EUMSZ-hez képest szűkszavúbban fogalmaz Alaptörvényünk, ami a VI. cikk (3) és (4) bekezdésében rendelkezik a személyes adatok védelméhez fűződő, valamint a közérdekű adatok megismeréséhez való jogról, melyeket együttesen információs önrendelkezési jogként ismer a jogirodalom.

„(3) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

(4) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi."[12]

Az alaptörvény a két alapjog védelmét is egy közös, sarkalatos törvényben rendezi, ami nem más, mint a fent hivatkozott Info tv.

Az adatvédelem tágabb kategória, mint az információs önrendelkezési jog, melyet az első adatvédelmi törvények még nem biztosítottak az érintett számára, ugyanakkor az információs önrendelkezési jognak is vannak olyan aspektusai, melyek nem fedhetőek le az adatvédelmi joggal.

Ez a fajta elkülönítés jelenik meg az Alkotmánybíróság joggyakorlatában is, amikor kimondja hogy az önrendelkezési jog alapján megilleti az egyént az a jog, hogy döntsön a rá vonatkozó információk nyilvánosságra hozataláról, míg az adatvédelmi jog elsősorban az adatkezelőnek állít korlátokat az adatok kezelésével kapcsolatosan.[13]

---

[11] 2012/C 326/01 számú, az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata 16. cikk.

[12] Magyarország Alaptörvénye VI. cikk

[13] 15/1991. (IV. 13.) AB határozat, 20/1990. (X. 4.) AB határozat

Az EU Adatvédelmi irányelve is a magánszféra védelméből kiindulva, azon belül jelöli meg az adatvédelem helyét:

"A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében."[14]

A GDPR, azaz az új adatvédelmi rendelet azonban némileg szűkíti a fogalom meghatározását, és az adatvédelmet kiemeli a magánszféra védelmének tágabb kategóriájából.

„Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.”[15]

Végül nem maradhat ki a felsorolásból „új” polgári törvénykönyvünk sem, ami némileg eltér a „régi” Ptk-tól, ami kifejezetten passzív oldalról közelítette meg a személyiségi jogok - akkor még személyhez fűződő jogok – védelmét.[16]

Az új civilkódex ugyanis a személyiségi jogok, az azokkal való rendelkezés aktív oldalát emeli ki elsőként:

„2:42. § (1) Mindenkinek joga van ahhoz, hogy törvény és mások jogainak korlátai között személyiségét, így különösen a magán- és családi élet, az otthon, a másokkal való - bármilyen módon, illetve eszközzel történő - kapcsolattartás és a jóhírnév tiszteletben tartásához való jogát szabadon érvényesíthesse, és hogy abban őt senki ne gátolja.

(2) Az emberi méltóságot és az abból fakadó személyiségi jogokat mindenki köteles tiszteletben tartani. A személyiségi jogok e törvény védelme alatt állnak.

(3) Nem sért személyiségi jogot az a magatartás, amelyhez az érintett hozzájárult.

2:43. § A személyiségi jogok sérelmét jelenti különösen

---

[14]Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (1995. október 24.), I. Fejezet, 1. cikk, (1) bek.

[15]

[16]1959.évi IV. törvény a Polgári törvénykönyvről, 75. § (1) A személyhez fűződő jogokat mindenki köteles tiszteletben tartani. E jogok a törvény védelme alatt állnak.

a) az élet, a testi épség és az egészség megsértése;

b) a személyes szabadság, a magánélet, a magánlakás megsértése;

c) a személy hátrányos megkülönböztetése;

d) a becsület és a jóhírnév megsértése;

e) a magántitokhoz és a személyes adatok védelméhez való jog megsértése;

f) a névviseléshez való jog megsértése;

g) a képmáshoz és a hangfelvételhez való jog megsértése."[17]

A polgári törvénykönyv tehát külön nevesíti a személyes adatok védelméhez való jogot, mint személyiségi jogot, és az érintett hozzájárulását, mint a személyiségi jogsértés megállapítását kizáró tényezőt. Ez utóbbit azonban, mint azt később látni fogjuk, fenntartásokkal kell kezelni.

Ha jobban belegondolunk, nehéz a személyes adatok védelméhez való jog szabad érvényesítéséről beszélni, ugyanis a szabad érvényesítés egyfajta aktivitást feltételez: Ez könnyen elképzelhető a szabad mozgáshoz, munkavállaláshoz való jog esetében például, amikor az alapjog gyakorlása és érvényesítése valóban aktív magatartást feltételez az érintett jogalanytól. Ugyanez mondható el a politikai szabadságjogok között megtalálható gyülekezési jogról, de még a hagyományosan külön aktív és passzív alapjogra felosztott választójogról is. A passzív választójogot gyakorló jogalany is aktív és tudatos magatartással indul a választáson jelöltként.

Még a kifejezetten olyan típusú alapjogok között is amelyek fő funkciója az, hogy azt mások tiszteletben tartsák, vannak olyanok, amelyek sokkal jobban „szem előtt" vannak. A legtöbben napi szinten törődnek például életük, egészségük megóvásával, és teljes joggal elvárják napi szinten azt is, hogy azt mások tiszteletben tartsák. Ezzel szemben – és talán nagyon óvatlanul is – személyes adataink biztonságáért nem aggódunk a nap huszonnégy órájában.

Ennek a látszólagos nemtörődömségnek több oka is van. Mindenekelőtt az, hogy a személyes adataink védelméhez fűződő jog korántsem korlát nélküli. Számtalan korlátja létezik, mint pl.a közérdek, közbiztonság, illetve a leggyakoribb és legáltalánosabb korlát, a jogalany saját hozzájárulása, amit

[17]2013.évi V. törvény a polgári törvénykönyvről 2:42 és 2:43. §

rendszerint meg is ad, ha kell, ha nem.

Gondoljunk csak bele, napjában többször kitárulkozunk a világhálón, és ehhez nem kell pl. a vallási meggyőződésünkről hangot adó, a személyes adatainkat hiánytalanul tartalmazó posztot közzétenni valamelyik közösségi oldalon. Elég egy online vásárláshoz két perc alatt végrehajtott regisztráció, de akár egy internetes keresés is, amelyek alapján a google gyakorlatilag egy komplett személyiségi profilt is kiállít rólunk. Tudatosan adjuk meg tehát adatainkat, kérdés azonban, hogy egy átlagos jogalany, de akár még a jogban valamennyire járatos, tudatosabb felhasználó is, mennyire van tisztában azzal, hogy az általa megadott személyes adatokat pontosan mire fogja felhasználni a vele szemben álló szolgáltató, illetve adatkezelő. Ez a jelenség az úgynevezett „knowledge-gap".[18]

Általánosságban elmondható tehát, hogy személyi adataink a szürke hétköznapokban mit sem sejtve a rájuk leselkedő veszélyekről, lábukat lógatván élik mindennapjaikat. És e tekintetben tesszük ezt mi is.

Egészen addig, amíg valami hiba nem csúszik a gépezetbe.

[18]Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vand. L. Rev.*, *52*, 1607.

III. Az adatvédelem rövid története

Bár jelen értekezés elsőrendű alanya a GDPR, aminek személyes és közvetlen története legfeljebb a leköszönő irányelvig vezethető vissza, nem árt, ha ennél kissé távolabb merészkedünk visszafele az időben hogy felismerhessük, nem is annyira új keletű kérdés a magánszféra, azon belül pedig a személyes adataink védelme.

A személyes adatok valamilyen – kezdetleges - szintű nyilvántartása, rendszerezése gyakorlatilag egyidejű az írás megjelenésével. Elég csak belegondolni, hogy például egy egyszerű sírfelirat is mennyit elárulhat az elhunytról. A legnyilvánvalóbb és már valóban tudatos, valamilyen célhoz kötött gyűjtése és feljegyzése a személyes adatok bizonyos körének az egyes ősi birodalmak uralkodóházai családfájának feljegyzése volt a vérvonal tisztán tartása érdekében.

Lényegében a személyes adatokon belüli speciális kategóriának minősülő szenzitív adatok védelméről van szó magában a hippokratészi esküben is:
"Amit kezelés közben látok vagy hallok – akár kezelésen kívül is a társadalmi érintkezésben, – nem fogom kifecsegni, hanem titokként megőrzöm. Ha ezt az eskümet megtartom és nem szegem meg: örvendhessek életem fogytáig tudományomnak, s az életnek, de ha esküszegő leszek, történjék ennek ellenkezője.[19]"

Az adatok regisztrációja aztán a népesség növekedésével, és a technológia fejlődésével párhuzamosan egyre szélesebb körben terjedt el, kiemelt jelentőségük azonban a betegségek, járványok kezelésében és megelőzésében, illetve háborúk során volt.

Az első, kifejezetten a magánszféra védelmét is biztosító jogszabály az Angliában 1361-ben elfogadott, kiegészítésekkel a mai napig hatályos Justices of the Peace Act, amit kukkolók tettenérése esetén is alkalmaztak.[20]

[19] A hippokratészi eskü (latinul Hippocratis Jusjurandum) az ókori Görögországban keletkezett orvosi eskü, amelynek emelkedett szelleme a mai orvosi esküket is áthatja, az orvosi etika máig ható hivatkozási alapja. Gyakran hivatkoznak rá mint a primum nil nocere elvre.
https://hu.wikipedia.org/wiki/Hippokrat%C3%A9szi_esk%C3%BC Megtekintés dátuma: 2022. június 20.
Az eskü teljes szövege olvasható: Hippokratészi eskü – Magyar katolikus lexikon: http://lexikon.katolikus.hu/H/hippokrat%C3%A9szi%20esk%C3%BC.html Megtekintés dátuma: 2022. június 20.

[20] http://www.legislation.gov.uk/aep/Edw3/34/1/section/I Megtekintés dátuma: 2022. június 20.

Szintén az egyén magánszférája, de azon túl az érintett beleegyezése, illetve annak hiánya lett kidomborítva az Egyesült Államokban egy 1888-as eset kapcsán, amikor egy fotóstúdió az egyik vendégről készített képét képeslapra helyezte, és azt sokszorosítás után árulni kezdte. A bíróság ítéletében eltiltotta a stúdiót a kép további engedély nélküli felhasználásától.[21]

A 20. század ugrásszerű technológiai és népességi növekedése következtében az egyének nyilvántartása, adataik rendszerezése kiemelten fontos állami igénnyé, és egyben feladattá is vált. A számítástechnika fejlődésének köszönhetően pedig az 1960-as, 70-es évekre már lehetőség volt addig elképzelhetetlen mennyiségű adathalmazból álló nyilvántartások létrehozására is.

Ennek következtében az addig jobbára csak a szenzitív adatok védelmére koncentráló adatvédelem egyre inkább az adatok és adatalanyok szélesebb körére kezdett kiterjedni, az életviszonyok egyre szélesebb terét lefedve.[22]

Nem véletlen hogy ekkor született meg az első, kifejezetten adatvédelmi tárgyú nagy nemzetközi dokumentum, a Nemzetközi Gazdasági és Együttműködési Szervezet (OECD) Irányelvei.[23] A 70'-es évekre a globalizáció, a személyek-, és a munkaerő szabad áramlása következtében a gazdasági életben is egyre fontosabbá vált az adatvédelmi szabályok lefektetése. Ezt felismerve születtek meg az OECD irányelvei, melyeknek alapelvei a mai napig az adatvédelem aktuális pilléreit képezik.

Ezek az alapelvek, összefoglaló jelleggel, a következők:
A korlátozott adatgyűjtés elve: Főszabály szerint („megfelelő esetben") az alany tudtával és beleegyezésével, korlátozottan és tisztességes eszközökkel van lehetőség az adatgyűjtésre.

Adatminőség alapelve: Lényegében a célhoz kötöttség elvét ismerhetjük fel, tehát kifejezetten csak az adatgyűjtés céljának megfelelő adatokat szabad gyűjteni, amik azonban e minőségükben teljesek, pontosak és folyamatosan aktualizáltak.

---

[21] Prosser, WL (1960) *Privacy* in: California Law Review, Vol. 48, No. 3 https://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1/ Letöltés dátuma: 2022. június 20.

[22] Mészáros, 2017

[23] OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, áttekintés http://www.oecd.org/sti/ieconomy/15590228.pdf Letöltés dátuma: 2022. június 20.

Szándékmegjelölés alapelv: A személyes adatok gyűjtésének szándékát legkésőbb az adatgyűjtéskor meg kell határozni és azok későbbi felhasználását csak ezen célokra, vagy azokkal nem összeegyeztethetetlen célokra kell korlátozni és amint ezek minden egyes szándékváltozás során meghatározásra kerülnek. Ez esetben azonban ismételten szükséges az alany hozzájárulása, mint azt a későbbiekben látni fogjuk.

Felhasználási korlátozás alapelve: A személyes adatokat nyilvánosságra hozni tilos, kivéve ha abba az adatalany beleegyezik, vagy törvény kifejezetten így rendelkezik.

Biztonsági garancia alapelve: Az adatokat védeni kell a kockázatokkal szemben, különösen azok elveszítése, megsemmisülésem felhasználása, megváltoztatása, nyilvánosságra hozatala, vagy az engedély nélküli hozzáférés ellen.

Nyitottság alapelve: Általános nyitottsági politikát kell folytatni a személyes adatokra vonatkozó fejleményekkel, gyakorlatokkal és vezérelvekkel kapcsolatban. Könnyen hozzáférhetővé kell tenni olyan eszközöket, amelyek meghatározzák a személyes adatok létezését és természetét, valamint azok felhasználásának főbb céljait, valamint az adatellenőrző személyét és szokásos fellelhetőségét.

Egyéni részvétel alapelv: Az adatalanynak joga van ahhoz, hogy a) tájékoztassák arról, hogy róla adatokat tárolnak. b) azokba ésszerű időn belül, ésszerű számára érthető módon betekinthessen, c) jogorvoslattal megtámadható indokolást kapjon az első két pontban foglalt jogának megtagadásáról d) illetve hogy a róla tárolt hibás/téves adatok módosítását, kijavítását kérje.

Felelősségre vonhatóság alapelv: Az adatellenőrző legyen felelősségre vonható, hogy azon intézkedések szerint jár-e el, melyek a fenti alapelveknek érvényt szereznek.

Bár az OECD Irányelvei nem kötelezőek, a bennük kimunkált adatvédelmi intézmények, alapelvek komoly hatással voltak a későbbiekben létrejövő adatvédelmi szabályozásoknak, így az EU adatvédelmi jogára, közvetetten tehát a hazai adatvédelmi jogra is.

1981-ben fogadták el az Európa Tanács Adatvédelmi Egyezményét[24], aminek fő tárgyai a személyes adatok automatizált állományai, illetve a személyes adatok gépi feldolgozása. Az Egyezmény különlegessége, hogy a tagállamok nyilatkozhatnak arról, hogy szabályait a nem gépi eszközökkel feldolgozott adatállományokra is alkalmazni fogják. Az egyezmény 1998-ban vált a magyar jog részévé, és Magyarország elfogadó nyilatkozatot tett a nem automatizált adatállományokra való alkalmazásra is.[25]

Az Egyezmény adatkezelési alapelvei lényegében megismétlik az OECD Irányelvekben lefektetett alapokat:

a) az adatokat csak tisztességesen és törvényesen szabad megszerezni és feldolgozni,

b) az adatokat csak meghatározott és törvényes célra szabad tárolni, és attól eltérő módon nem szabad felhasználni,

c) az adatoknak tárolásuk céljával arányban kell állniuk, és meg kell felelniük e célnak, azon nem terjeszkedhetnek túl,

d) az adatoknak pontosaknak, és ha szükséges, időszerűeknek kell lenniük,

e) az adatok tárolási módjának olyannak kell lennie, amely az adatalany azonosítását csak a tárolás céljához szükséges ideig teszi lehetővé.

Eme teljesség igénye nélküli áttekintést követően már látható, hogy 1995-re, az adatvédelmi irányelv megszületéséig már széles körben elterjedt az adatvédelem, és a jogalanyok/adatalanyok jogtudatossága is feléledt, ennek eredményeképpen pedig a modern adatvédelmi jog alapjait is sikerrel munkálták ki a különféle nemzetközi szervezetek.

[24]Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során

[25]1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

IV. A modern adatvédelmi jog az Európai Unióban: Az adatvédelmi (95/46/EK) irányelv és az adatvédelmi rendelet

IV.1. Az Európai Parlament és a Tanács 95/46/EK irányelve:

Az EU adatvédelmi jog egészen a közelmúltig regnáló tartóoszlopa, a 95/46/EK, közkeletű nevén az adatvédelmi irányelv tehát korántsem a semmiből született meg, hiszen, mint azt láttuk, illetve tapasztalni fogjuk, főbb elveit, intézményeit gyakorlatilag az előző fejezetben ismertetett nemzetközi dokumentumokból halászta ki, azokat céljának és az EU politikájának megfelelően átdolgozta, kiegészítette „csak". Témánk szempontjából azonban ennek ellenére is kihagyhatatlan mérföldkőről van szó, hiszen számos megoldása, céljai a mai napig aktuálisak, mi sem bizonyítja ezt jobban hogy rohamosan változó világunkban is több, mint két évtizedig volt érvényben. Éppen ezért a GDPR-el való összehasonlítása előtt indokoltnak tartom, hogy összefoglaló jelleggel bár, de áttekintsük főbb szabályait, ily módon még jobban kiemelve a két szabályozás közötti különbségeket és hasonlóságokat egyaránt.

Az 1995-ös évekre a belső piac megvalósításával biztosítottá vált az áruk, a személyek, a szolgáltatások és a tőke szabad mozgása. Ezzel párhuzamosan szükséges lett az is, hogy a személyes adatok is szabadon áramolhassanak egyik tagállamból a másikba, mindezt úgy, hogy közben az egyének alapvető jogai is biztosítva legyenek. Mindeközben a gazdasági és társadalmi tevékenység számos területén is egyre elterjedtebb lett az adatok gyűjtése és felhasználása, amit az informatika rendkívül gyors fejlődése nagyban megkönnyített. Ezen felül a növekvő tudományos és műszaki együttműködés és az új telekommunikációs hálózatok összehangolt bevezetése is szükségessé tette, és megkönnyítette a személyes adatok határokon keresztül történő áramlását.

Az Unió a fenti folyamatokra tekintettel közösségi szinten kívánta szabályozni a személyes adatok védelmét, felismerte ugyanis, hogy az egyes tagállamokban végzett személyesadat-feldolgozás terén az egyének jogai és szabadságai, különösen a magánélet tiszteletben tartásához való jog védelmének szintjei közötti eltérések akadályozhatják az ilyen adatok egyik tagállamból a másikba történő továbbítását. Ezek az eltérések pedig akadályt jelentenek számos közösségi szintű gazdasági tevékenység elvégzésében, torzíthatják a versenyt, és hátráltatják a hatóságokat a közösségi jog

szerinti feladataik teljesítésében. Elengedhetetlenné vált tehát a tagállami adatvédelmi szabályozás egységessé tétele.

Bár senki nem vitatta az irányelv fő célkitűzéseit, és az egységesítés szükségességét, annak mértékével nem minden tagállam értett egyet, különösen az Egyesült Királyság ódzkodott az elfogadás ellen, mert komoly módosításokat tett szükségessé a jogrendszerükben.

Az Európai Parlament három alkalommal, 1976-ban, 1979-ben és 1982-ben is felkérte a Bizottságot az adatvédelmi szabályok megalkotására, ami a fent említett nehézségek miatt sem ment zökkenőmentesen. 1990-ben született az első tervezet ami elsősorban német és francia alapokra épül, aminek magyarázatát az adja, hogy a tervezetért felelős bizottság elnökének szerepét Németország Hessen tartományának akkor adatvédelmi biztosa töltötte be. Ezt követően elhúzódó viták alakultak ki a tudományos élet szereplői, a tagállamok, de még az EU egyes szervei között is.

Míg a Parlament az alapvető jogok védelmét látta elsődlegesnek, addig a Tanács és a Bizottság az adatok szabad áramlását priorizálta, elsősorban gazdasági szempontok alapján. Ez a kettősség egyébként vissza is köszön az irányelvben, ami mindkét célt igyekszik elérni, amelyhez azonban sok esetben az Unió Bíróságának a segítsége is kellett. [26] 1992-ben készült el a módosított tervezet, amit 1995. októberére sikerült is elfogadni

Végül 1995. december 13-án hatályba lépett az adatvédelmi irányelv, amelynek átültetésére a tagállamok 1998. október 24-ig kaptak határidőt. Az irányelv egy olyan szabályozási keretrendszert hozott létre, amelynek célja az egyének magánéletének magas szintű védelme és a személyes adatok Európai Unión (EU) belüli szabad áramlása közötti egyensúly megteremtése. Ennek érdekében az irányelv szigorúan feltételekhez kötötte a személyes adatok gyűjtését és felhasználását, és minden tagállam számára kötelezővé tette egy, a személyes adatok védelméért, az adatkezelési tevékenységek felügyeletéért felelős független nemzeti szerv létrehozását.

Az irányelvet, bár elsősorban az automatizált módon feldolgozott adatokra kellett alkalmazni, számos rendelkezését a hagyományos papír alapú adatkezelés során is kötelezővé tette, ezen adatoknál is

[26]Az egyes jogeseteket az Irányelv áttekintése során a releváns rendelkezéshez érve fogom ismertetni.

fennállt már ugyanis annak lehetősége, hogy azokat később egy automatizált nyilvántartási rendszer részévé kívánnák tenni, és ennek a módszernek köszönhetően az eredetileg a hagyományos módon begyűjtött és kezelt adatokat csak digitalizálni kellett az átállás során.

Az irányelv saját maga tartalmazott olyan rendelkezéseket, amelyek személyi és tárgyi hatályát szűkítik. Nem terjedt ki a hatálya azon esetekre, amikor a természetes személy kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett adatfeldolgozást. Ezen kitétel vizsgálata képezi a középpontját a *Lindqvist ügy*nek.[27]

Lindqvist asszony egy svéd egyházközségben dolgozott, melynek keretében honlapot hozott létre hívőtársaival kapcsolatosan, melyen több személyes adatot is közzétett róluk, például hogy az egyik felekezeti tag lábát törve betegszabadságon tartózkodott otthonában. A helyi adatvédelmi hatóság komoly bírsággal sújtotta Lindqvist asszonyt tevékenységéért. A Bíróságnak az ügyben arról kellett állást foglalnia, hogy alkalmazható-e az irányelv ezen tevékenységre, amelynek üzleti célja nem volt, a honlap működtetése társadalmi, vallási célokat szolgált. A Bíróság azonban nem értelmezte kiterjesztően ezen rendelkezést, hanem kimondta, hogy Lindqvist asszony tevékenysége nem volt kizárólag személyes célból és háztartási körben végzett, figyelemmel arra, hogy az általa közzétett adatokat bárki bárhol elérhette a világon.

Nem terjedt ki az Irányelv hatálya a közösségi jog hatályán kívül eső tevékenységekre, mint például a közbiztonság, a védelem és a nemzetbiztonság keretében végzett feldolgozási műveletek. Az irányelv éppen az volt a célja, hogy a személyes adatok feldolgozása vonatkozásában biztosítsa az egyének jogainak és szabadságainak védelmét azáltal, hogy megállapította a jogszerű feldolgozás fő feltételeit, valamint az adatok minőségére vonatkozó elveket.

A ***jogszerű adatfeldolgozás*** -vagylagos -feltételei az alábbiak:

a.) az érintett egyértelmű hozzájárulása;

b.) az adatfeldolgozás olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél;

[27]A Bíróság 2011.november 06-án kihirdetett C-101/01 ítélete

c.) az adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges;

d.) az érintett adatok feldolgozása az természetes személy létfontosságú érdekei védelméhez szükséges;

e.) az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve

f.) harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges;

g.) az adatfeldolgozás az adatkezelő vagy a harmadik fél jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek az alapvető jogokhoz és a szabadságjogokhoz fűződő, védelmet élvező érdekei.

Az irányelv kidolgozta, összegyűjtötte továbbá az ***adatok minőségére vonatkozó elvek***et, amelyeket valamennyi jogszerű adatfeldolgozó tevékenységre alkalmazni kellett:

A személyes adatok feldolgozását tisztességesen és törvényesen kell végezni, és gyűjtésük csak meghatározott, egyértelmű és törvényes célból történhet. Ezenfelül az adatoknak megfelelőeknek, relevánsaknak és nem túlzott mértékűeknek, pontosaknak, és ha szükséges, időszerűeknek kell lenniük, és csak a szükséges ideig és gyűjtésük céljainak megfelelően tárolhatók.

Tiltott az irányelv értelmében az olyan személyes adatok feldolgozása, amelyek a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkoznak. Ez a rendelkezés fenntartásokkal alkalmazandó például akkor, ha az adatfeldolgozásra az érintett létfontosságú érdekeinek védelméhez, illetve megelőző egészségügyi és orvosi diagnosztikai célból van szükség.

Az érintett természetes személy, akinek az adatait feldolgozzák, ***az alábbi jogokat gyakorolhatja*** az irányelv értelmében:

Információkérés joga: az adatkezelőnek bizonyos információkról (az adatfeldolgozó személye, az adatfeldolgozás célja, az adatok címzettjei stb.) tájékoztatnia kell az érintettet, akitől a rá vonatkozó adatokat gyűjti.

Adathozzáféréshez való jog: minden érintett számára biztosítani kell a jogot, hogy korlátozás nélkül, ésszerű időközönként, túlzott késedelem vagy költség nélkül megerősítést kapjon arról, hogy rá vonatkozóan adatok feldolgozása folyamatban van-e, érthető formában értesítést kapjon az adatfeldolgozás alatt álló adatokról és azok forrásával kapcsolatos minden rendelkezésre álló információról. Kérheti az olyan adatok helyesbítését, törlését vagy zárolását, amelyek feldolgozása nem felel meg ezen irányelv rendelkezéseinek, különösen az ilyen adatok hiányos vagy hibás volta miatt.

Adatfeldolgozás elleni tiltakozás joga: az érintett számára biztosítani kell, hogy jogos érdekből tiltakozhasson a rá vonatkozó adatok feldolgozása ellen. Ezenfelül biztosítani kell számára, hogy kérelemre és térítésmentesen tiltakozhasson az olyan adatok feldolgozása ellen, amelyek célja közvetlen üzletszerzés. Végezetül az érintettet tájékoztatni kell személyes adatainak harmadik személyeknek közvetlen üzletszerzés céljából történő közlése előtt, valamint számára az ilyen közlés elleni kifogás jogát biztosítani kell.

Az érintett jogainak korlátozása kizárólag nemzetbiztonsági, honvédelemi, közbiztonsági érdekből, a bűncselekményekkel kapcsolatos eljárások lefolytatása, valamely tagállam vagy az Európai Unió fontos gazdasági vagy pénzügyi érdeke, illetve az érintett védelme érdekében korlátozhatóak.

A közérdek és a személyes adatok védelméhez fűződő alapjog csap össze a Bíróság *Bavarian Lager* ügyben [28] született ítéletében is. Az alapeset tulajdonképpen egy „egyszerű", az áruk és szolgáltatások szabad áramlásáról szóló ügy volt, amely akkor került a reflektorfénybe, amikor a Bavarian Lager kérvényezte a Bizottságtól, hogy betekinthessen az ügy megbeszélésén készített jegyzőkönyvbe, mely megbeszélésen az Egyesült Királyság és a Confédération des Brasseurs du Marcheurs Commun [29] képviselői vettek részt. A Bizottság megküldte ugyan a kérvényezett jegyzőkönyvet, azt azonban anonimizálta, és minden személyes adatot kihúzott a jelenlévők magánszférájára hivatkozva. A jelenlévők közül ketten kifejezetten megtagadták hozzájárulásukat, míg hárman nem nyilatkoztak adataik feltüntetésével kapcsolatban.

[28] A Bíróság 2010. június 29-én kihirdetett C-28/08.sz. ítélete
[29] Confederation of Common Market Brewers, (Egységes Piaci Sörfőzők Szövetsége)

A Bíróság végül kétfokú eljárásban mondta csak azt ki, hogy elsőbbséget az adott esetben a megbeszélésen jelenlévők személyes adatainak védelme élvezett. A Bavarian Lager ugyanis nem tudta alátámasztani, hogy számára miért lett volna fontos a hiányzó 5 név megismerése, így a Bizottság dokumentumaihoz való hozzáférésben megnyilvánuló közérdek nem tudta legyőzni a személyes adatok védelmét.

A személyes adatok védelme sok esetben ütközik össze továbbá a sajtószabadsággal is, mint esetleges korlátozásra okot adó tényezővel. E tekintetben az egyik legjelentősebb ítélet a *Tietosuojavaltuutettu v Satakunnan Markkinapörssi* ügyben született meg.[30] Az ügy alapját az képezte, hogy Finnországban az adóhatóság publikálta, hogy az egyes állampolgárok mennyi adót fizettek be az adott évben. Ezt követően a publikált adatokból egy magáncég(Satakunnan Markkinapörssi) összeállítást készített régiók és adózók alapján csoportosítva, melyet egy helyi lapban meg is jelentetett. A Bíróság az ítéletében megállapította, hogy a cég publikációs tevékenysége személyes adatok feldolgozásának minősül, és az irányelv hatálya alá esik, még akkor is, ha előtte a személyes adatok már nyilvánosan publikálásra kerültek egy állami szerv által. Kiemelte, hogy a sajtószabadság ugyan számos esetben kivételt képez az irányelv alkalmazása tekintetében, az általános kivételként való kezelése kiskaput jelenthetne, mivel elég lenne minden esetben a személyes adatok tagállam általi publikálása a kibúváshoz a rendelet hatálya alól.

Rendelkezett az irányelv ***az adatfeldolgozás titkosságáról és biztonságá***ról is. Az adatkezelő vagy az általa meghatalmazott személy, beleértve magát az adatfeldolgozót is, aki a személyes adatokhoz hozzáféréssel rendelkezik, kizárólag az adatkezelő utasítása alapján dolgozhatja fel a személyes adatokat. Az adatkezelőnek végre kell hajtania a megfelelő intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében.

Fontos garanciális szabályként jelent meg ***a felügyelőhatóság előzetes értesítése az adatfeldolgozásról***. Ennek értelmében az adatkezelőnek az adatfeldolgozást megelőzően értesítenie kell a tagállami felügyelőhatóságot. A felügyelőhatóság az értesítés kézhezvételét követően előzetesen felméri az érintettek jogait és szabadságait fenyegető esetleges kockázatokat. Biztosítani

[30]A Bíróság 2008. december 16-án kihirdetett C-73/07.sz. ítélete

kell az adatfeldolgozási műveletek nyilvánosságát, a felügyelőhatóságoknak pedig nyilvántartást kell vezetniük a bejelentett műveletekről.

Az irányelv valamennyi természetes személy számára biztosítja a ***jogorvoslathoz való jog***ot bármely olyan jogának megsértése esetén, amelyet a szóban forgó adatfeldolgozásra alkalmazandó nemzeti jog biztosít számára. Ezenfelül azok a személyek, akik személyes adataik jogellenes feldolgozása eredményeképpen kárt szenvedtek, az elszenvedett károkért kártérítésre jogosultak.

A személyes adatok a tagállamokból kizárólag olyan harmadik országba továbbíthatóak, amely megfelelő védelmi szintet tud biztosítani, ezen szabály alól azonban kivételt képez ha az érintett beleegyezik adatainak továbbításába, ha szerződéskötésről van szó, ha a közérdek szükségessé teszi azt, illetve akkor is, ha az adott tagállam kötelező erejű vállalati szabályok vagy általános szerződési feltételek alkalmazását teszi lehetővé.

Az irányelv kötelezővé tette a tagállamok részére a ***független felügyelőhatóságok*** felállítását, amennyiben azok még nem működtek.

Gyakorlatilag tehát az Irányelv nem azért tekinthető úttörőnek, mert vadonatúj fogalmakat, adatvédelmi eszközöket vezetett volna be, hiszen, mint láthatjuk a legtöbb rendelkezését az előző fejezetekben ismertetett nemzetközi dokumentumokban már megismerhettük, legfeljebb kisebb eltérések fedezhetőek csak fel. Ami miatt az Irányelv mégiscsak kiemelkedik a többi adatvédelmi dokumentum közül, azt az alábbiakban lehet összefoglalni:

- Kihirdetésének pillanatában valamennyi adatvédelmi elvet, fogalmat naprakészen tartalmazott

- Irányelvként az Unio tagállamainak kötelezővé vált nemzeti adatvédelmi szabályozásuk hozzáigazítása a közösségi szabályokhoz

- Egységesen, valamennyi tagállamban kötelezővé vált a független adatvédelmi hatóságok felállítása

- Az Európai Unió Bírósága általi kontroll.

Az irányelv elfogadásával tehát a természetes személyek személyi adatai több évtized után modern, jogszabályi, intézményi (független hatóságok), közösségi jogvédelmet kaptak, ami fölött még bírói kontroll is érvényesült. Nem véletlen, hogy az irányelv több mint két évtizedig hatályban volt.

Első ízben 2003-ban készült bizottsági jelentés végrehajtásáról, mely jelentés összefoglalta a kormányok, az intézmények, a vállalkozási és fogyasztóvédelmi szövetségek, valamint a polgárok közreműködésével a 95/46/EK irányelv értékeléséről folytatott bizottsági konzultációk eredményét. E konzultációkból az derült ki, hogy kevés közreműködő kérte az irányelv felülvizsgálatát. Továbbá a tagállamokkal folytatott konzultációt követően a Bizottság tudomásul vette, hogy többségük, valamint a nemzeti felügyelőhatóságok többsége is úgy ítélte meg, hogy nincs szükség az irányelv módosítására. A végrehajtás során tapasztalt késedelmek és hiányosságok ellenére az irányelv elérte fő célját, vagyis felszámolta a személyes adatoknak a tagállamok közötti szabad áramlása előtt álló akadályokat. A Bizottság továbbá úgy vélte, hogy megvalósult a Közösségen belüli magas szintű védelem biztosítására irányuló célkitűzés, mivel az irányelv világviszonylatban is az egyik legszigorúbb adatvédelmi előírásokat fogalmazta meg. A belső piaci politika egyéb céljainak megvalósítása ugyanakkor kevésbé volt eredményes. Az adatvédelmi jogszabályok terén az egyes tagállamokban továbbra is komoly eltérések voltak megfigyelhetőek, márpedig ezek megakadályozzák, hogy a multinacionális szervezetek összeurópai adatvédelmi eljárásokat dolgozzanak ki.

A 2007-es bizottsági jelentés arról számolt be hogy további fejlődés tapasztalható a végrehajtásban, ugyanis minden tagállam sikerrel ültette át az Irányelvet saját nemzeti jogába, és hogy továbbra sem szükséges annak módosítása.

Az irányelv hosszú regnálását segítette elő, hogy ha egy adott szektorban jelentős technológiai ugrás ment végbe, úgy a közösség intézményei ágazatspecifikus közösségi jogszabályokat hoztak létre. Ilyen ágazatspecifikus jogszabályoknak tekinthetjük a 2002-es elektronikus hírközlési adatvédelmi irányelvet[31], vagy a személyes adatok közösségi intézmények és szervek védelméről szóló 45/2001/EK

[31]Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes

rendeletet[32] is. Idővel elkerülhetetlenné vált azonban, hogy az időszakosan kialakuló joghézagok „betömése” helyett új, átfogó közösségi jogszabályt alkosson az Unió.

adatok kezeléséről, feldolgozásáról és a magánélet védelméről

[32]Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről , valamint az ilyen adatok szabad áramlásáról

IV.2. Út az adatvédelmi rendelethez

Az idő múlása, a korábbi fejezetekben már több esetben említett technológiai fejlődés, és az ezzel párhuzamosan egyre gyakrabban jelentkező joghézagok együttesen oda vezettek, hogy 2010-re egyre sürgetőbbé vált egy új átfogó szabályozás létrehozása. Míg 1995-ben az Irányelv kihirdetése idején világszerte (!) 16 millióan használtak rendszeresen internetet, addig ez a szám 2016-ra több mint 4 milliárdra emelkedett. Ma már elképzelhetetlen egy háztartás internet, asztali számítógép vagy laptop, notebook, tablet, okostelevízó és okostelefon nélkül. Az okostelefonoknak hála pedig gyakorlatilag a zsebünkben hordozzuk az életünket, a legtöbb szolgáltató pedig ezt felismerve leegyszerűsített formában is tálcán kínálja annak lehetőségét, hogy még a számítógéphez képest is pofonegyszerűen, pár kattintással elvégezzünk egy online regisztrációt, ismételten kiadva kezeink közül személyi adatainkat. Ezen folyamatokkal párhuzamosan természetesen az adatkezelők száma is ugrásszerűen megnőtt a két évtized alatt.[33] Szükségessé vált tehát az adatvédelmi reform annak érdekében, hogy az EU a 21. században is megfelelőképp tudja biztosítani a személyes adatok védelmét.

Az öregedő adatvédelmi irányelv érdemeit senki nem vitatta ugyan, célkitűzései és elvei továbbra is érvényesek a mai napig is. Azonban az irányelv nem akadályozta meg teljes körűen *„sem azt, hogy az Unió tagállamaiban az adatvédelem végrehajtása széttagolt módon valósuljon meg, sem a jogbizonytalanságot, sem pedig azt, hogy széles körben az a benyomás alakuljon ki, hogy természetes személy védelme – különösen az online tevékenységek esetében – jelentős kockázatoknak van kitéve.”*[34]

A természetes személyek jogai és szabadságai egyes tagállamokban továbbra is eltérő szintű védelmet élveztek, különösen, ami személyes adatok védelméhez való jogot illeti. Ehhez nagyban hozzájárult az is, hogy az Irányelvet minden tagállam önállóan adoptálta, így nem volt feltétlenül egységes még az alapfogalmak értelmezése sem. Az egyes tagállamok önállóan hoztak ágazatspecifikus jogszabályokat is, amelyek még tovább színesítették a képet. Ez a fajta sokszínűség a személyes adatok Unióban történő szabad áramlásának útjában állt, ezáltal zavarta a belső piac működését, torzította versenyt, és hátráltatták a hatóságokat az uniós jog szerinti feladataik ellátásában.

---

[33]Forrás: Internet World Stats https://www.internetworldstats.com/stats.htm Letöltés dátuma 2020. június 20.
[34]A GDPR preambulumának (9) bekezdése

Nyilvánvalóvá vált, hogy az irányelvnél szigorúbb, azaz rendeleti szabályozásra van szükség, ami által a személyes adatok az Unió egész területén hatékony védelemben részesülhetnek. Ismételten le kell fektetni az érintettek jogait, meg kell szigorítani a személyes adatokat kezelő kötelezettségeit és valamennyi tagállamban egyenértékű hatáskört kell biztosítani a vonatkozó szabályok betartásának ellenőrzéséhez amihez szükséges az is, hogy a jogsértőkre azonos szankciókat kell alkalmazni.

2011. június 22-én az akkori adatvédelmi biztos, Peter Hustinx véleményt fogalmazott meg az EU adatvédelmi status quo-járól, mely véleményben összefoglalóan fejtette ki a fentiekben leírt problémákat, kiemelte azonban azt is, hogy az adatvédelem általános alapelveit megváltoztatni nem kell és nem is szabad. Szorgalmazta továbbá, hogy a Bizottság lehetőség szerint 2011 végéig fogadjon el európai uniós szintű javaslatot.[35]

Ez, a következő lépcsőfok minimális késéssel, 2012. január 25-én következett be, amikor is a Bizottság elfogadta az adatvédelmi irányelv átfogó reformjáról szóló javaslatot az egyének online magánszférája és az Unió digitális gazdaságának megerősítése érdekében. Végül, egy hosszas egyeztetési folyamat lezárásaként a Parlament 2014. március 12. napján 621 igen, 10 nem és 22 tartózkodó szavazattal támogatta a GDPR megalkotását. A Rendelet végleges szövegének elfogadására 2016. április 27-én, kihirdetésére pedig 2016. május 04-én került sor. A Rendelet az ezt követő huszadik napon, 2016. május 24-én lépett hatályba azzal, hogy a tagállamok két évet kaptak a felkészülésre, aminek így végső határideje 2018. május 25-e lett.

A kihirdetést követően a digitális Európa olyan mértékben zúdult fel amire már hosszú ideje nem volt példa. Ez érthető is, ha belegondolunk, hogy a GDPR-ről szóló első hírek a 20 millió, azaz húszmillió Euróig, vagy a cég éves bevételének 4%-ig terjedő bírságok kiszabásának lehetőségét emelték ki a legfontosabb újításként. Ezt követően gyakorlatilag külön üzletág, a *„GDPR compliance”* jött létre a kötelezett intézmények – valamennyi unión belüli, adatkezelést folytató intézmény, legyen az uniós szerv vagy tagállami hatóság, cég – GDPR-re való felkészítésére. Egy magára valamit is adó cég nem létezhetett, és a mai napig sem látezhet GDPR compliance manager nélkül, egyes ügyvédi irodák

[35]Az európai adatvédelmi biztos véleménye „A személyes adatok Európai Unión belüli védelmének átfogó megközelítése” című, az Európai Parlamenthez, a Tanácshoz, az Európai Gazdasági és Szociális Bizottsághoz és a Régiók Bizottságához intézett bizottsági közleményről (2011/C 181/01)https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_hu.pdf Letöltés dátuma: 2022. június 20.

pedig kizárólagos profiljukká tették az egyre sürgetőbbé vált új adatvédelmi szabályozások kidolgozását. Ha az internet keresőjébe beírjuk hogy GDPR, több tucat előzetes és utólagos GDPR-hatásvizsgálatot kínáló cég ajánlataiba futhatunk bele.

Természetesen a nem megfelelő adatkezelésért kapható magas bírságtól való félelem indokolt és érthető is egyben, kérdés azonban, hogy a GDPR valóban olyan szintű és mértékű változásokat mutat-e be az adatvédelmi irányelvhez képest, amire ráillik a hangzatos „adatkezelési forradalom” jelző. Amint azt hamarosan látni fogjuk, nem igazán.

IV.3. A GDPR főbb szabályai:

Az összehasonlítás előtt indokolt az adatvédelmi rendelet főbb szabályainak áttekintése is, amelyeket főbb témakörök szerint igyekszem csoportosítani.

A rendelet ***általános cél***ja lehetővé tenni az uniós polgárok számára személyes adataik megfelelőbb kezelését. Korszerűsíti és egységesíti továbbá azokat a szabályokat, amelyek a vállalkozások számára lehetővé teszik az adminisztratív terhek csökkentését és a fogyasztói bizalom fokozását.

A ***személyes adatok kezelésére vonatkozó általános elvek***et az alábbiak szerint rendszerezi a rendelet:
Jogszerűség,tisztességes eljárás és átláthatóság elve: A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

Célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon.

Adattakarékosság elve: a tárolt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.

Pontosság elve: A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

Korlátozott átláthatóság elve: Az adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak a személyes adatok közérdekű archiválása céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, természetesen mindezt a rendeletben meghatározott feltételek teljesülése esetén.

Integritás és bizalmas jelleg elve: Az 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.

Elszámoltathatóság elve: Az adatkezelő felelős a rendelet céljának való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. Nem elég tehát GDPR kompatibilisnek lenni, annak is kell látszani.

A ***jogszerű adatkezelés***re vonatkozó rendelkezések egy-az-egyben átültetésre kerültek a nyugalmazott irányelvből, ami megfelel annak az általános konszenzusnak, miszerint az adatkezelés már kidolgozott elveit nem szabad bolygatni.

A rendelet az adatvédelmi irányelvhez hasonlóan szedi csokorba ***a természetes személyek jogai***t is, melyek közül a szembetűnőbb változásokat mutató jogokat emelem csak ki:[36]

Az adatokhoz való egyszerűbb hozzáférés joga: beleértve az adatkezelés módjára vonatkozó információnyújtást, illetve annak biztosítását, hogy az adatokhoz való hozzáférési mód egyértelmű és érthető legyen;

Az adathordozhatósághoz való új jog: A személyes adatok szolgáltatásnyújtók közötti továbbításának megkönnyítésére szolgál. Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta.

A törléshez való jog: Önmagában nem új keletű, azonban új dimenzióval „az elfeledtetéshez való jog”-al bővült ki arra az esetre amikor egy természetes személy már nem kívánja adatai feldolgozását, azok tárolására pedig nincs jogos indok.

[36]A felsorolásból kimaradt jogok, mint pl. a helyesbítéshez való jog gyakorlatilag csak megismétlik az adatvédelmi irányelv rendelkezéseit, lényegi változást tehát nem fedezhetünk fel bennük.

A személyes adatok feltöréséről való tájékoztatáshoz való jog: A vállalkozások és szervezetek kötelesek haladéktalanul tájékoztatni a természetes személyeket a súlyos adatvédelmi incidensekről. Ezen túlmenően értesíteniük kell az érintett adatvédelmi felügyeleti hatóságot.

Konkrétan felvázolt szankciórendszer: A Rendelet szabályozza a felügyeleti hatóságok hatáskörét, illetve az általuk megtehető egyes intézkedéseket, nevesíti a közigazgatási bírságot, mint lehetséges szankciót és részletes szempontrendszert állít fel a bírság összegének megállapításához.

A GDPR nem titkolt célja az adatvédelmi akadályok elhárítása által a határokon átnyúló gazdaság és kereskedelem élénkítése és hogy ezáltal üzleti lehetőségeket teremtsen és élénkítse az innovációt. Ehhez az alábbi, ***vállalkozásokra vonatkozó rendelkezések***et vezette be:

A legnagyobb adatkezelőknek (hatóságok és a vállalkozások) kötelezővé teszi az *adatvédelmi tisztviselő* kijelölését.

Egyablakos ügyintézés: A vállalkozásoknak csak egy felügyeleti hatósággal kell kapcsolatot tartaniuk (a fő székhelyükként szolgáló uniós országban).

Globalitás: Az EU-n kívül székhellyel rendelkező vállalkozásokra ugyanazon szabályok vonatkoznak, amennyiben az EU-n belül nyújtanak szolgáltatásokat vagy kínálnak árukat, illetve természetes személyek magatartását figyelik meg.

Beépített és alapértelmezett adatvédelem: Biztosíték arra, hogy az adatvédelmi garanciák a termékek és szolgáltatások fejlesztésének már a legkorábbi szakaszába beépüljenek.

Értesítések eltörlése: Az új adatvédelmi szabályok eltörlik a legtöbb, értesítésre vonatkozó kötelezettséget, illetve az ezekkel járó költségeket. Az adatvédelmi rendelet egyik célja a személyes adatok EU-n belüli szabad áramlása előtt álló akadályok felszámolása.

Az Unió az előzetes hatásvizsgálatok alapján úgy számolt, hogy az adatvédelemre vonatkozó egységes

uniós szintű jogszabályok várhatóan 2,3 milliárd EUR megtakarítást eredményezhetnek évente.

V. Az adatvédelmi irányelv és a GDPR összevetése

Az eddigiekben a két nagy adatvédelmi uniós jogszabály legfőbb szabályait, erényeit ismerhettük meg külön-külön, de eljött végre annak is az ideje, hogy a két titánt „beengedjük a ringbe", hogy tisztábban láthassuk a kettejük közötti különbségeket, és - előzetes várakozásainknak megfelelően- lássuk beigazolódni azon felvetésünket, hogy a GDPR olyan forradalmi szintű változásokat vezet be aminek segítségével könnyedén kiüti az adatvédelmi irányelvet.

Elöljáróban le kell szögezni azt, hogy a két jogszabály megszületése között 20 év telt el, így az adatvédelmi irányelv komoly hátrányból indul. Mindenképpen a GDPR esélyeit erősíti az a tény is, hogy rendeleti mivoltából fakadóan a tagállamoknak egy-az-egyben át kell azt ültetniük saját belső jogukba, ezáltal a korábbihoz képest egységesebb adatvédelmi szabályozást hozva létre Európa-szerte.

Ennek az első hozadéka az, hogy ha nem is lesznek teljesen elkerülhetőek – egészen egyszerűen nyelvi, fordítási okokból kifolyólag – az értelmezésbeli eltérések, a rendeleti szabályozás következtében az EU valamennyi tagállamában egységes fogalmakat kell majd használni, azaz az olyan fogalmak mint pl. „adatkezelő" szó szerint ugyanazt fogja jelenteni Spanyolországban mint Magyarországon. Garanciaként ráadásul a GDPR úgy rendelkezik, hogy az esetleges értelmezési nehézségek esetén az egyetlen autentikus jogforrás a Bíróság lesz.

Maguk az ***alapfogalmak*** nem változtak meg az adatvédelmi rendeletben, inkább csak pontosította, aktualizálta azokat az Irányelvben foglaltakhoz képest. Ez a fajta modernizáció figyelhető meg a két jogszabály *„személyes adat"*-ra vonatkozó fogalommeghatározásában is. A Rendelet megtartja az eredeti definíciót, de a példálózó jellegű felsorolásba már beépíti a technológiai fejlődés következtében, és a Bíróság joggyakorlatában kialakult további szükséges elemeket:

V.1.Irányelv

„személyes adat" az azonosított vagy azonosítható természetes személyre („érintettre") vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági,

kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén.[37]

V.2. Rendelet

„személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, ***helymeghatározó adat*****,** ***online*** *azonosító vagy a természetes személy testi, fiziológiai,* ***genetikai****, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.*[38]

A példálózó felsorolásba tehát belekerült az online azonosító, a helymeghatározó adat és a genetikai adat. Fontos változás az is, hogy a Rendelet preambuluma kifejezetten kijelenti, hogy az IP-cím vagy a cookie-azonosító is azonosításra alkalmas, ezen értelmezés pedig a Bíróság joggyakorlatából került bele a Rendeletbe. A Bíróság a *Patrick Breyer kontra Németország* ügyben hozott ítéletében [39] rámutatott ugyanis, hogy a technológiai fejlődés által lehetővé vált a profilalkotás és az érintett azonosítása, a tényleges személyazonosság ismerete nélkül is, akár egy egyszerű IP-cím lekérdezésével, vagy a látogatott oldalakon használt „sütik" megismerése által is.

Ugyanez a modernizáció figyelhető meg a Rendelet 9. cikkében, ugyanis a GDPR különleges védelmet biztosít, és beemeli a *különleges adatok* közé genetikai, a biometrikus és az egészségügyi adatot.

Nem változott az *adatkezelés* definíciója sem, az továbbra is a személyes adatokon végzett bármely műveletet jelenti. A Rendelet továbbra is elkülöníti az adatkezelőt és az adatfeldolgozót. *Adatkezelő* az, aki meghatározza az adatkezelés céljait és eszközeit, míg az *adatfeldolgozó* az, aki az adatkezelő nevében kezeli a személyes adatokat. A Rendelet újítása e téren hogy bevezeti az ún. *közös adatkezelő* fogalmát: Ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg az e
rendelet szerinti kötelezettségek teljesítéséért fennálló, különösen az érintett jogainak gyakorlásával

[37]Adatvédelmi Irányelv 2. cikk a) pont
[38]Adatvédelmi Rendelet 4.cikk 1. pont
[39]A Bíróság 2016. október 19-én kihirdetett C-582/14.sz. ítélete

kapcsolatos feladataikkal összefüggő felelősségük megoszlását.[40]

Máig kérdéses azonban, hogy a gyakorlatban hogy érvényesül ez a fajta kettős felosztás, amely az Irányelv elfogadása idején még helytálló volt, azonban az internet korában már idejétmúlt, hiszen felhasználók, vállalkozások, kormányok és eszközök milliói kezelnek adatokat világszerte. A Rendelet megalkotásában komoly részt vállaló Adatvédelmi Munkacsoport [41] szerint a *közösségi oldal üzemeltetője* is adatkezelőnek minősül, hiszen ő határozza meg az oldal alapvető szolgáltatásait (pl.: hogyan lehet profilt létrehozni), valamint ő dönt arról, hogy milyen célra használhatóak fel az adatok (pl.: hirdetések reklámozása). A különféle *alkalmazások üzemeltetői* szintén minősülhetnek adatkezelőnek. A kérdés azért lényeges, mivel ha valaki adatkezelőnek minősül, akkor az adatkezelőt terhelő kötelezettségeknek eleget kell tennie. Ugyanakkor tisztán látható az is, hogy a közösségi oldal illetve az alkalmazás üzemeltetője nemcsak adatkezelő, hanem adatfeldolgozó is egyben.

A közösségi oldal üzemeltetője első ízben ugyanis meghatározza az oldal működési struktúráját és a technológiát. Ezt követően a felhasználó eldöntheti azt, hogy használja-e a közösségi oldalt, ha igen melyiket, milyen célból, milyen adatokat oszt meg magáról vagy harmadik személyekről. Onnantól fogva azonban, hogy a felhasználó megadta az adatait, az oldal üzemeltetője már adatfeldolgozónak fog minősülni, mivel a felhasználó akaratának megfelelően tárolja és teszi közzé a felhasználó által megadott adatokat. [42]

Módosult a Rendeletben a ***jogszerű adatkezelés*** egyik fő feltételének számító *hozzájárulás fogalma*. Míg az Irányelv a jogszerű adatkezeléshez elegendő volt az érintett önkéntes, kifejezett és tájékozott kinyilvánítása[43], addig a Rendelet értelmében a hozzájárulás akkor tekinthető megadottnak, hogy az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. [44]

---

[40]GDPR 26. cikk (1) bekezdés

[41]WP29 Adatvédelmi Munkacsoport, amit az adatvédelmi irányelv 29. cikke alapján jött létre. A munkacsoport adatvédelemmel, valamint a magánélet védelmével kapcsolatos kérdésekkel foglalkozó, a tagállamok összes adatvédelmi hatóságának képviselőiből és az európai adatvédelmi biztosból álló független tanácsadó szerv. Feladatait a 95/46/EK irányelv 30. cikke és a 2002/58/EK irányelv 15. cikke határozza meg.

[42]Van Eecke, P., & Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, *26*(5), 535-546. https://www.sciencedirect.com/science/article/abs/pii/S0267364910001093 Megtekintés dátuma: 2022. június 20.

[43]Adatvédelmi irányelv 2. cikk h) pont

[44]GDPR 4. cikk 11.pont

Bár első ránézésre a módosítás csak egyfajta finomhangolásnak tűnik, a GDPR a preambulumban több esetben is érinti a hozzájárulás kérdését, ami jelentősen kibővíti annak tartalmát. A Rendelet egyértelművé teszi, hogy az internetes oldalakon az előre „bepipált" hozzájárulás az adatkezeléshez nem elfogadható. Vita esetén az adatkezelőnek kell bizonyítania, hogy az érintett az adatkezeléshez valóban hozzájárult. Kimondja a rendelet azt is, hogy nem tekinthető önkéntes hozzájárulásnak, ezért az nem lehet az adatkezelés jogalapja, hogyha a felek között egyenlőtlen viszony áll fent, különösen ha az adatkezelő közhatalmi szerv, és az adott helyzet valamennyi körülményét figyelembe véve ezért valószínűtlen, hogy a szóban forgó hozzájárulás megadása önkéntesen történt. Hasonló a helyzet akkor is, ha egy szolgáltatási – szerződés teljesítését a hozzájárulástól teszik függővé, annak ellenére, hogy a hozzájárulás nem szükséges a szerződés teljesítéséhez. A hozzájárulás megadása ugyanis nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna. A hozzájárulás iránti kérelemnek érthetőnek és hozzáférhetőnek kell lennie, világos és egyszerű nyelvezettel kell rendelkeznie, fontos továbbá, hogy az érintett bármikor visszavonhatja hozzájárulását.

Ezen, a Rendelet preambulumában lefektetett részletszabályok a való élet tapasztalataiból vezethetők le, és rendeletben való szabályozásuk ellenére is igencsak kérdéses érvényesülésük. Elég csak felidéznünk bármelyik csatlakozásunkat egy közösségi oldalra, ami nem engedi a regisztrációt, ha nem fogadjuk el annak adatvédelmi szabályzatát. Felmerül a kérdés, hogy a több száz millió felhasználó közül hányan olvasták el ténylegesen a kérdéses szabályzatot? És ha még el is olvasták volna, vajon egy átlagos felhasználó az olvasottak mekkora részét képes megfelelően értelmezni? Hiába követelmény ugyanis a közérthető, egyszerű nyelvezetű leírás, egy adatvédelmi szabályzat, ha tetszik, ha nem, jogi szöveg, annak minden szakkifejezésével és fordulatával együtt. Bár a legtöbb közösségi oldal rendelkezik egyfajta „súgó" vagy „helpdesk" jellegű szekcióval, amit „FAQ"-nak vagy „GYIK"-nak rövidítenek legtöbbször, amik valóban „konyhanyelven" magyarázzák el a tudnivalókat az oldal egy-egy funkciójáról, ezeket a segédleteket azonban a felhasználók már csak akkor kezdik el böngészni amikor javában használják az adott oldalt. Az önkéntesség más oldalról is megközelíthető. A Facebook, mint a világ legszélesebb körben használt közösségi oldala, gyakorlatilag nem enged választási lehetőséget azok számára akik csak online tudják tartani kapcsolatot a világban mára már

szétszóródott családtagjaival, barátaival, ismerőseivel.

A ***tárgyi hatály*** kérdését az Irányelv és a Rendelet azonosan szabályozza, azzal, hogy a kivételek körét képező eseteket a Bíróság gyakorlatában már több esetben értelmezte, ezáltal pontosította azokat. (lsd: Lindquist-ügy)

Tágabb ugyanakkor a Rendelet ***területi hatály***a az adatvédelmi irányelvhez képest. Az Irányelv az olyan adatkezelőre volt alkalmazandó, aki letelepedett valamelyik tagállamban vagy nem telepedett le a tagállamban, de a tagállam területén olyan eszközt alkalmaz, amely adatkezelést végez, leszámítva azt az esetet, ha az eszközt kizárólag az EU-n átmenő adatforgalom céljából használja. A Rendelet azonban *nem csak az adatkezelő, hanem az adatfeldolgozó EU-ban található tevékenységi helye alapján is alkalmazandó*. Ha az adatkezelő vagy adatfeldolgozó nem rendelkezik az EU-ban tevékenységi hellyel, de az EU-ban tartózkodó érintettekre vonatkozó személyes adatokat kezel, akkor is a Rendeletet kell alkalmazni az EU-ban tartózkodó érintettek számára történő szolgáltatásnyújtás esetén. A gyakorlatban ez annyit tesz, hogy a közösségi oldalak üzemeltetőinek is eleget kell tenniük a Rendelet által megfogalmazott követelményeknek, azaz ha a Facebook meg kívánja tartani 376 millió európai felhasználóját[45] akkor adatvédelmi szabályzatának meg kell felelnie a GDPR rendelkezéseinek. Bár az oldal ennek kétségkívül megpróbált eleget tenni, 2012 első negyedéve óta 2018. második negyedévében először volt megfigyelhető a felhasználók számában történő csökkenés, amit Mark Zuckerberg, a Facebook megalkotója egyértelműen a GDPR bevezetésének tulajdonított.

Az ***adatkezelés jogalapja és alapelvei*** körében szintén nem figyelhető meg szignifikáns különbség a két jogszabály között, annyira, hogy a Rendelet ugyanazt a klasszikus hatos felsorolást (érintett hozzájárulása, szerződés teljesítése, jogi kötelezettség teljesítése, érintett vagy másik természetes személy létfontosságú érdekei, közérdek, adatkezelő vagy harmadik fél jogos érdekei) tartalmazza, mint az Irányelv, mint a jogszerű adatkezelés feltételeit. Megtartotta a Rendelet az Irányelv alapelveit is (tisztességesség, adatminőség és pontosság, célhoz kötöttség) , bevezette ugyanakkor az *átláthatóság , az adatbiztonság* elvét, és külön pontban rendelkezik az adatkezelő felelősségéről,

[45]statista.com: Facebook's monthly active users (MAU) in Europe from 4th quarter 2012 to 2nd quarter 2018 (in million MAU) https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ Megtekintés dátuma: 2018. szeptember 22.

azaz az *elszámoltathatóság*ról.

Szintén kérdéses a pontosság, naprakészség valamint az átláthatóság elvek érvényesülése az online tevékenységek során. Gyakorlatilag elvárhatatlan az egyes közösségi oldalak üzemeltetőitől, hogy naprakész adatokkal rendelkezzenek valamennyi felhasználójukról, azon egyszerű oknál fogva, hogy jelentős részüket a regisztráció pillanatában adja meg számukra a felhasználó, amit aztán a felhasználó utóbb vagy frissít, vagy nem. Az átlagos felhasználó ugyanis lusta, és előbb áll neki a facebookon frissíteni az adatait, mint a gyakorlati szempontokból sokkal fontosabb szolgáltatóknál. (pl.számlát vezető banknál, vagy közüzemi szolgáltatónál elérhetőségek módosítása) Úgyszintén nincs reális kontrollja a szolgáltatónak a felett, hogy az adott felhasználó mit oszt meg magáról oldalain. Az utóbbi években bevett szokássá vált pl. a leendő munkavállalók valamelyik, vagy valamennyi közösségi profiljának előzetes megtekintése a munkáltató által. Így esetlegesen egy évekkel azelőtti családi állapotot tükröző, vagy azóta megszűnt baráti társaságot ábrázoló fotó az új munkahelyen akár elutasítással is járhat.[46] Ennél is kellemetlenebb perceket okozhat, ha belegondolunk, hogy a rendvédelmi szervek világszerte sikerrel használják bűnesetek felderítéséhez a közösségi oldalakat. Egy évekkel ezelőtti „bulis" kép alapján órákat egy meghallgató szobában tölteni például semmiképpen sem kellemes időtöltés.

Az *átláthatóság* elvének érvényesülése (illetve annak hiánya) az érintett hozzájárulásának kérdésénél már kifejtett problémákból vezethető le. Az átláthatóság alapján ugyanis az érintettnek tisztában kell lennie az adatkezelés legfontosabb jellemzőivel (ki, hogyan milyen módszerrel gyűjti az adatokat, stb.), kérdéses azonban hogy egy valóban részletes és teljes körű tájékoztató mennyire világosítja fel az átlagos felhasználót.

Bár a GDPR egyik jelentős újításaként – egészen pontosan úgy, hogy nem EU tagállamokra nézve is kötelező a GDPR - hivatkoznak rá a kevésbé pontos híradásokban, a ***harmadik országokba való adattovábbítás***ra már az Irányelv is tartalmazta azon szabályt, hogy a fogadó harmadik országnak megfelelő védelmi szintet kell biztosítania. Egészen pontosan az Irányelv külön fejezetben (IV. fejezet

[46]Egy, a Microsoft által készített felmérés alapján a munkaközvetítő cégek és a HR-esek a jelentkezők 75%-ánál megtekintik a weben róluk található információkat közösségi oldalakon, keresőkön, blog oldalakon, online játék oldalakon. Az munkaközvetítők 70% úgy nyilatkozott, hogy utasítottak el már jelentkezőt az interneten róla található információk miatt. The New York Times: The Web Means the End of Forgetting http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=1& Megtekintés dátuma: 2018. szeptember 23.

– A személyes adatok harmadik országokba irányuló továbbítása) rendelkezett a kérdésről. Ami miatt mégis reflektorfénybe került ezen újnak mégsem mondható szabályozás, Snowden-botránynak, illetve az ezt követően mérföldkőnek számító, a Bíróságnak a „safe harbor"-t felszámoló, Schrems-ügyben[47] hozott ítéletének köszönhető.

Mivel az USA és az EU adatvédelmi szabályozásai, elvárásai jelentősen különböznek egymástól, ezért a két rendszer áthidalására és az USA-ba történő adattovábbításmegkönnyítése céljából jött létre a „Safe Harbor – Biztonságos Kikötő" rendszer. A Safe Harbort *a Bizottság 2000. július 26-i 2000/520/EK határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről* hozta létre. Amennyiben egy USA-ban székhellyel rendelkező vállalat teljesítette az Európai Unió által is elfogadott adatvédelmi elveket és regisztrált a Safe Harbor programra, akkor az adott vállalat biztonságosnak számított adatvédelmi szempontokból.

A biztonságos kikötő álló vizét azonban jelentősen felkavarta a 2013-as Snowden-botrány[48], aminek következménye a fent hivatkozott Schrems-ügy is. Az ügy felperese, Maximilan Schrems, osztrák állampolgár a botrány kirobbanása után panaszt nyújtott be az Ír Adatvédelmi Hatósághoz, melyben leírta, hogy az Egyesült Államokba küldött személyes adatok nem részesülnek megfelelő védelemben. A Safe Harbor csak az adatokat kezelő cégekkel szemben védi a személyes adatokat, az Egyesült Államok titkosszolgálati szervei ellen azonban nem. Az EU Bírósága határozatában egyértelművé tette, hogy az olyan szabályozást, amely lehetővé teszi a hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, sérti a magánszféra sérthetetlenségéhez fűződő jogot. Az EU állampolgárainak nem volt lehetősége arra, hogy tudomást szerezzenek a róluk folyó adatkezelésről, abba betekinthessenek, helyesbítést kérjenek, vagy bármilyen jogorvoslattal

[47] A Bíróság 2015. október 06-án kihirdetett C-362/14.sz. ügyben hozott ítélete

[48] Edward Joseph Snowden amerikai számítógépes szakember, a Booz Allen Hamilton tanácsadó cég volt munkatársa, az amerikai Nemzetbiztonsági Ügynökség (NSA) volt vezető tanácsadója, a Központi Hírszerző Ügynökség (CIA) volt műveleti tisztviselője és az Egyesült Államok Védelmi Hírszerzési Ügynökségének (DIA) volt oktatója, aki azzal vált közismertté, hogy nyilvánosságra hozott szigorúan titkos dokumentumokat, amelyekből kiderül, hogy az amerikai titkosszolgálatok széles körben figyelik az emberek mobiltelefon-hívásait és internetes tevékenységét az Egyesült Államokban és világszerte. Nyilvánosságra került, hogy az NSA világszerte több mint egy milliárd ember telefonos és internetes kommunikációját követi figyelemmel és nem csak a terrorizmusról, hanem külpolitikai, gazdasági, konkrét kereskedelmi témákról is adatokat gyűjt. Az NSA kiterjedt kémtevékenységet folytatott az Európai Unió, az Egyesült Nemzetek Szervezete és számos olyan kormányzat ellen is, amelyek egyébként az Egyesült Államok szoros szövetségesei, így például Angela Merkel volt német kancellár telefonját is lehallgatták. A kiszivárgott dokumentumok szerint az NSA-nak hozzáférése van a Google, a Microsoft, a Facebook, a Yahoo, a YouTube, az AOL, a Skype, az Apple és a Paltalk rendszeréhez.

éljenek, így gyakorlatilag az Irányelv által biztosított valamennyi joguk sérült. A Bíróság megerősítette továbbá, hogy a tagállamok adatvédelmi hatóságai még a 95/46/EK irányelv 25. cikkének (6) bekezdése szerinti megfelelőségi határozat[49] megléte esetén is hatáskörrel rendelkeznek arra vonatkozóan, és kötelesek teljes függetlenséggel eljárva megvizsgálni, hogy a harmadik ország felé irányuló adattovábbítás megfelel-e a 95/46/EK irányelvben megállapított követelményeknek. (Az adatvédelmi hatóság ugyanis épp azzal érvelt, hogy nincs hatáskörük a kérdés vizsgálatára.)

Az ítéletet követően az Európai Parlament Állampolgári Jogok, Bel- és Igazságügyi Bizottsága (LIBE) megvizsgálta a Safe Harborba jelentkező vállalatokat, és megállapította, hogy hétből egy kérelem valótlan volt, és a már regisztrált társaságok 30%-a sem felelt meg maradéktalanul az Irányelv rendelkezéseinek, mert nem nyújtottak megfelelő tájékoztatást a lehetséges vitarendezési módozatokról.

A Safe Harbor bukása után tehát új védelmi rendszer kialakítására volt szükség, ezért jött létre 2016. július 22-én az EU-US adatvédelmi pajzs[50].

Jelentős ráncfelvarráson esett át az Irányelv érintetti jogosultságokra vonatkozó cikke is. Bár a GDPR alapvetően megtartotta a korábbi szabályozás által biztosított jogokat (tájékoztatáshoz, adathozzáféréshez, törléshez, helyesbítéshez való jog stb.) azokat bővítette, illetve a már meglévő szabályokat tovább finomította. A *tájékoztatáshoz való jog* kapcsán jelentősen nőtt azon információk köre, amelyre vonatkozóan tájékoztatni kell az érintettet. Ide kapcsolódik, és a nehezen érthető adatkezelési tájékoztatók miatt jelent meg az *átláthatóság* követelménye is, melynek érvényesülése kiemelten fontos, hiszen ez a feltétele annak, hogy az érintettek valóban rendelkezni tudjanak a személyes adataikról. Így az adatkezelésre vonatkozó tájékoztatásnak könnyen hozzáférhetőnek, érthetőnek, valamint világosnak és közérthetőnek kell lennie.

Új jogként került rögzítésre, és a törléshez való jogot bővíti ki a *„feledéshez" vagy „elfeledtetéshez való jog"* (right to be forgotten). Ennek a rendelkezésnek a gyakorlati megvalósulását a szintén új keletű jogként bevezetett adatok továbbításához való jog ismeretében láthatjuk majd át. A

[49]Eszerint a Bizottság határozatban megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít-e.

[50]A Bizottság 2016/1250 VÉGREHAJTÁSI HATÁROZATA (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről.

feledtetéshez való jog lényegi funkciója abból a mára már közhellyé vált (ami a valóságtartalmát nem csorbítja) szabályból ered, hogy „az internet nem felejt."[51] Ami valaha felkerült a világhálóra, az valahol, valamilyen formában megmarad, hiszen technológiailag a digitális adatok teljes eltüntetése lehetetlen, hála a mára elterjedt gigantikus tárkapacitással rendelkező szervereknek és a gyakorlatilag határtalan mennyiségű adat tárolására alkalmas felhő alapú szolgáltatásoknak. Egy kép elég ha pár percig fent van valakiről az interneten, ha azt letölti valaki, onnantól fogva nincs az a szolgáltató aki ezt 100%-os biztonsággal fel tudná deríteni és törlésre kényszerítené az illetőt. Tovább színezi a képet hogy a XX. század végére világszerte elterjedté váltak a digitális hatósági nyilvántartások. Erre talán a legkézenfekvőbb példa az egyes digitális adatbázisok összekapcsolásán alapuló Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS)[52], amely 2012 áprilisában kezdte meg működését.

Az Irányelv az adathozzáféréshez való jogon belül szabályozta az érintett azon jogát, hogy kérje az Irányelv rendelkezéseinek nem megfelelő adatok helyesbítését, zárolását vagy törlését.[53]

Ehhez képest a Rendelet[54] egyrészt pontosabban körülírja, mely esetekben nem megfelelő az adatkezelés, másrészt leírja, hogy az adatkezelő az egyszerű törlésen túl *„az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket - ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését."* Szintén az elfeledtetéshez való jogot erősíti, hogy szélesebb körben érvényesül az érintett tiltakozáshoz való joga is, aki jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, különösen ha az adatkezelés üzletszerzés érdekében történik.[55] Fontos megjegyezni, hogy a feledtetéshez való jog sem korlát nélküli, az folyamatosan ütközik az

[51] Viviane Reding, a José Manuel Barroso által (2004-2014 között) vezetett Bizottság alelnökének (feladatköre: igazságszolgáltatás, alapvető jogok és uniós polgárság) az EU adatvédelmi rendeletének tervezetével kapcsolatban híressé vált idézete „God forgives and forgets but the Web never does!", vagyis „Isten megbocsát és felejt, azonban a Web soha"

[52] Az ECRIS-t (Európai Bűnügyi Nyilvántartási Információs Rendszer) 2012 áprilisában hozták létre a bűnügyi nyilvántartásokkal kapcsolatos információk EU-szerte történő cseréjének megkönnyítése érdekében. Az ECRIS elektronikus összeköttetéseket hoz létre a tagállamok között, és szabályokat állapít meg annak biztosítása érdekében, hogy a tagállamok bűnügyi nyilvántartási rendszerében szereplő, büntetőítéletekre vonatkozó információk szabványosított elektronikus formátumban, egységes és gyors módon, valamint rövid törvényi határidőkön belül kicserélhetők legyenek.

[53] Adatvédelmi Irányelv 6. cikk (1) bekezdés és 12. cikk b) pont.

[54] GDPR 17. cikk.

[55] GDPR 21. cikk

információszabadság másik összetevőjével, az adatok szabad áramlásához, és a tájékozódáshoz való joggal, közérdekkel.

Szorosan kapcsolódik az elfeledtetéshez való joghoz az *adathordozhatósághoz való jog*, melyet a GDPR egyes rendelkezéseiről szóló fejezetben részletesen ismertettem. Két fő összetevője az érintett joga arra, hogy másolatot szerezzen a rá vonatkozó személyes adatokról széles körben használt, géppel olvasható formátumban, a második pedig, hogy ezeket a személyes adatokat egy másik adatkezelőnek továbbítsa, illetve hogy az aktuális adatkezelőtől kérje adatainak közvetlen továbbítását egy új adatkezelőhöz. A gyakorlatban ez a fajta átfedés évek óta működik egyes szektorokban (legjellemzőbben a banki, biztosítási szektorban).A két újonnan bevezetett jog gyakorlati funkciója az, hogy az egyes szolgáltatók/adatkezelők közötti adattovábbítások esetén az adatok útja jobban követhető, így a feledtetéshez való jog jelentősen hatékonyabban: gyorsabban és olcsóbban érvényesíthető, illetve teljesíthető.

Az Irányelvhez képest jelentős előrelépés az Adatvédelmi Rendelet által bevezetett új ***eszközök az adatvédelem hatékonyabbá tétele érdekében***. Az Irányelv nem tartalmazott konkrét szankciórendszert, csupán arról rendelkezett, hogy a tagállamok megteszik az irányelv rendelkezéseinek teljesülését elősegítő intézkedéseket, megállapítják a rendelkezések megsértése esetén kiszabható szankciókat.

A Rendelet ezzel szemben már konkrét szankciókat, illetve a *felügyeleti hatóságok által megtehető intézkedések*et[56] (figyelmeztetés, elmarasztalás, utasítás kötelezettség teljesítésére, adatkezelés korlátozása, tanúsítvány visszavonása stb.) nevez meg. Nevesíti a az egyes rendelkezései megsértése miatt, az egyes intézkedésekkel párhuzamosan *kiszabható közigazgatási bírságot* , mint lehetséges szankciót, és meghatározza azon kereteket is, amelyek közt az ellenőrzést végző hatóságok mozoghatnak a fizetendő összeg meghatározásakor. Kisebb jelentőségű rendelkezések megsértése 10.000.000,- EUR összegű, illetve vállalkozások esetén az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb2 %-át kitevő bírsággal sújtható, azzal, hogy a kettő összeg közül a magasabb összeget *kell* kiszabni. Súlyosabb esetekben azonban 20.000.000,- EUR összegű, illetve az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő bírság is kiszabható. A Rendelet

[56]GDPR 58. cikk (2) bekezdés a felügyeleti hatóság korrekciós hatásköreiről

egy konkrét szempontrendszert is felvázol amiket kellőképpen figyelembe kell vennie a bírságoló hatóságoknak, ami nem sokban különbözik a büntetőügyek során alkalmazott szempontrendszertől:

a) a jogsértés jellege, súlyossága és időtartama, érintettek száma, az általuk elszenvedett kár mértéke
b) a jogsértés szándékos vagy gondatlan jellege;
c) az adatkezelő vagy az adatfeldolgozó részéről az érintettek által elszenvedett kár enyhítése érdekében tett bármely intézkedés;
d) az adatkezelő vagy az adatfeldolgozó felelősségének mértéke,
e) az adatkezelő vagy az adatfeldolgozó által korábban elkövetett releváns jogsértések;
f) a felügyeleti hatósággal a jogsértés orvoslása és a jogsértés esetlegesen negatív hatásainak enyhítése érdekében folytatott együttműködés mértéke;
g) a jogsértés által érintett személyes adatok kategóriái;
h) az, ahogyan a felügyeleti hatóság tudomást szerzett a jogsértésről, különös tekintettel arra, hogy az adatkezelő vagy az adatfeldolgozó jelentette-e be a jogsértést, és ha igen, milyen részletességgel;
i) ha az érintett adatkezelővel vagy adatfeldolgozóval szemben korábban – ugyanabban a tárgyban – alkalmazták a Rendeletben megtalálható intézkedések valamelyikét, a szóban forgó intézkedéseknek való megfelelés;
j) az, hogy az adatkezelő vagy az adatfeldolgozó tartotta-e magát a jóváhagyott magatartási kódexekhez vagy tanúsítási mechanizmusokhoz; valamint
k) az eset körülményei szempontjából releváns egyéb súlyosbító vagy enyhítő tényezők, például a jogsértés közvetlen vagy közvetett következményeként szerzett pénzügyi haszon vagy elkerült veszteség.[57]

Továbbra is lehetőséget biztosít ugyanakkor a Rendelet arra, hogy a tagállamok megállapítsák az egyes rendelkezések megsértése esetén alkalmazandó további szankciókra vonatkozó szabályokat, különösen azon jogsértések tekintetében, amelyek nem tartoznak a 83. cikkben meghatározott, közigazgatási bírságokkal sújtható jogsértések közé, és meghoznak minden szükséges intézkedést ezek végrehajtására. E szankcióknak is hatékonynak, arányosnak és visszatartó erejűnek kell

[57]GDPR 83.cikk (2) bekezdés a)-k) pontjai

lenniük.[58]

További újdonságnak tekintendő végül a szintén a Rendelet által bevezetett ***személyes adatok hatékonyabb védelmét szolgáló módszerek***, a beépített adatvédelem (data protection by design), az alapértelmezett adatvédelem (data protection by default) és az előzetes adatvédelmi hatásvizsgálat (data protection impact assessment), melyek együttesen azt hivatottak biztosítani, hogy a tervezett adatkezelés a kezdetektől, azaz az adetkezelés tényleges megkezdésének pillanatától megfeleljen a Rendelet rendelkezéseinek. A *beépített adatvédelem* lényege, hogy az adatkezelésbe már a tervezés során is adatvédelmet segítő megoldások kerüljenek beépítésre (pl.álnevesítés). Az *alapértelmezett adatvédelem* alapján az adatkezelő köteles megtenni minden olyan intézkedést annak biztosítására, hogy az adatkezelés (legyen az valamilyen szolgáltatás, program) alapbeállításai automatikusan az adatvédelmet szolgálják. Ez a közösségi oldalak esetében annyit tesz, hogy az alapértelmezett adatvédelmi beállításokat - elvileg- privátra állítja a rendszer, amit utólag módosíthat csak a felhasználó, ha úgy kívánja. Az *adatvédelmi hatásvizsgálat* pedig azt jelenti, hogy már az adatkezelés előtt fel kell mérni a lehetséges kockázatokat, és meg kell tenni mindent annak érdekében hogy azok az adatkezelés megkezdése előtt kiiktatásra kerüljenek, ennek érdekében az adatkezelő akár konzultációt is folytathat az illetékes felügyelő hatósággal.

Összegzésképpen megállapítható, hogy az Irányelv és a GDPR között nem tapasztalható markáns különbség. Köszönhető ez az Irányelv – megalkotáskori – modern szabályainak, időtálló megoldásainak, valamint annak, hogy a Rendelet sok esetben gyakorlatilag az Irányelvnek az Unió Bírósága által tartalommal megtöltött rendelkezéseit használja fel újra. Az egyes finomításokat e fejezetben részletesen elemeztük, és szintén kitértünk a szembetűnőbb újításokra is, mint pl. az egységesebb és ezáltal hatékonyabb rendeleti formában történő szabályozás, valamint a részletesebben kidolgozott szankciórendszer. Nincs más tehát hátra, mint hogy megpróbáljuk levonni a konzekvenciákat, és áttekinteni, hogy a GDPR immáron általunk ismert, és azóta gyakorlatban is kipróbált újításai milyen hatással voltak digitális világunkra.

[58]GDPR 84.cikk

VI. A GDPR hatásai a digitális világra

Bár a Rendelet mindössze 2018.május 25-én lépett effektíve hatályba Európa-szerte, az ezt megelőző két éves türelmi időszaknak köszönhetően az egyes tagállamoknak lehetőségük volt a Rendeletre való felkészülésre. Finoman szólva is naivitás lett volna azonban azt feltételezni, hogy az átállás mindenki számára zökkenőmentes lesz, és minden adatkezelő és feldolgozó „megússza" az előzetesen is rettegett bírságokat. Ennek alátámasztására nem kell túl messzire mennünk, ugyanis rendelkezésünkre áll az igencsak sokat mondó elnevezésű gdprbirsagok.hu oldal, aminek rövid átpörgetése után láthatjuk, hogy a GDPR négy éve tartó regnálása óta Magyarországon több tucat, a jelképes összegű 100.000,- Ft-os bírságtól kezdve igencsak komoly, 300 millió Ft-os bírságig terjedő büntetés került kiszabásra az adatvédelmi hatóság által. [59] Ez utóbbi bírság is eltörpül az eddigi rekordernek számító, 746 millió EUR összegű bírság mellett, ami a világ egyik legnagyobb vállalata, az *amazon*-nal szemben került kiszabásra. A bírságok azonban csak a jéghegy csúcsát képezik, bár kétségtelen, hogy a legkézzelfoghatóbb következményei az adatvédelmi rendeletnek. a GDPR hatásainak vizsgálata azonban ennél sokkal szélesebb körű vizsgálatot kíván meg.

Maga a rendelet írja elő az önvizsgálatot a 97. cikkében, ennek megfelelően az első bizottsági jelentés is már két éve elkészült, 2020. júniusában.[60] A jelentés általánosságban sikeresnek ítélte meg a GDPR első két évét, nem meglepő módon azonban felhívta a figyelmet a nem egységes értelmezés problémájára az egyes tagállamokban, valamint hogy a tagállamok nem használják ki maradéktalanul a GDPR által felkínált eszközöket, mint pl. a tagállami adatvédelmi hatóságok közötti közös műveletek lehetőségét, ami előmozdíthatná a ténylegesen egységes adatvédelmi kultúra létrehozását.

Külön kiemelték már ekkor, hogy szükség van az általános szerződési feltételek átfogó szabályozására, emellett pedig az elkövetkező évekre vonatkozó stratégiai irányvonalakat is kimunkálták az alábbiak szerint[61]:

---

[59] gdprbirsagok.hu Megtekintés dátuma: 2022. június 20.

[60] A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK:
A polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0264&from=EN Megtekintés dátuma: 2022. június 20.

[61] Összeállítás a jelentés 3. pontja alapján

A tagállamok feladatául tűzte ki az ágazati jogszabályok GDPR-ral való összehangolásának befejezését, az adott esetben széttagoltságot létrehozó és az adatok EU-n belüli szabad áramlását veszélyeztető specifikációs előírások használata korlátozásának fontolóra vételét, és annak értékelését, hogy a GDPR-t végrehajtó nemzeti jog minden tekintetben a tagállami jogszabályok számára előírt kereteken belül van-e.

A Bizottság vállalta, hogy folytatja a tagállamokkal folytatott kétoldalú tárgyalásokat a nemzeti jogszabályok GDPR-nak való megfeleléséről, ideértve a nemzeti adatvédelmi hatóságok függetlenségét és erőforrásait; kihasználja a rendelkezésére álló valamennyi eszközt, beleértve a kötelezettségszegés megállapítására irányuló eljárást, hogy biztosítsa a tagállamok GDPR-nak való megfelelését, támogatja a vélemények és nemzeti gyakorlatok tagállamok közötti további cseréjét olyan témákkal kapcsolatban, amelyek további nemzeti szintű pontosítást igényelnek az egységes piac széttöredezettségének csökkentése érdekében, például az egészségüggyel és kutatással kapcsolatos személyesadat-kezelés, vagy amelyek esetében más jogokkal, például a véleménynyilvánítás szabadságával való egyensúlyra kell törekedni.

-

Vállalta továbbá, hogy támogatja az adatvédelmi keret egységes alkalmazását az új technológiákkal kapcsolatban, hogy segítse az innovációt és a technológiai fejlődést, igénybe veszi a GDPR-ral foglalkozó tagállami szakértői csoportot (amely a GDPR hatálybalépése előtti átmeneti időszak alatt jött létre), hogy megkönnyítse a tagállamok és a Bizottság közötti megbeszéléseket és tapasztalatcserét, feltárja, hogy a további tapasztalatok és a vonatkozó ítélkezési gyakorlat fényében célszerű-e a GDPR egyes rendelkezései esetleges jövőbeli célzott módosításának javaslata, különös tekintettel a személyes adatok kezelését nem fő üzleti tevékenységként végző (alacsony kockázatú) kkv-k által végzett adatkezelés nyilvántartására, és az információs társadalommal összefüggő szolgáltatások tekintetében a gyermekek hozzájárulási életkorának esetleges összehangolására.

Fontos célnak ítélte meg a jelentés az új irányítási rendszerben rejlő teljes potenciál kiaknázásának biztosítása aminek érdekében felszólította az adatvédelmi hatóságokat arra, hogy hatékony megállapodásokat alakítsanak ki az adatvédelmi hatóságok között az együttműködési és egységességi mechanizmus működésével kapcsolatban, valamint hogy minden lehetséges módon, a GDPR-ban előírt

valamennyi eszköz használatával biztosítsák a GDPR egységes alkalmazását. Felhívta továbbá az adatvédelmi hatóságokat az egymás közötti együttműködés fokozására, például közös vizsgálatok lefolytatásával.

Ennek érdekében gyakorlati jellegű és könnyen érthető – és folyamatosan felülvizsgált iránymutatásokra van szükség, amelyek egyértelmű válaszokat adnak és mellőzik a kétértelműséget a GDPR alkalmazásával kapcsolatos kérdések tekintetében, például a gyermekek adatainak kezelésével és az érintettek jogaival kapcsolatban, beleértve a hozzáféréshez és az adatok törléséhez való jog gyakorlását, valamint az érdekelt felekkel való konzultációt a folyamat során.

A Bizottság további célként jelölte még meg az innováció ösztönzését, az adattovábbításokra vonatkozó eszköztár továbbfejlesztését, a konvergencia előmozdítását és a nemzetközi együttműködés kialakítását is.

Mint látható, az első bizottsági jelentés még számos olyan területet feltárt, aminek további pontosítása, és erősítése szükséges. Kétségkívül vannak azonban olyan hatások is, amik szinte azonnal, de legalábbis rövid idő belül jelentkeztek. A Rendelet hatásait célszerű az adatkezelők/feldolgozók oldaláról megközelíteni, tekintettel arra, hogy nekik a kitűzött határidőre fel kellett készülniük adatvédelmi szabályzatuk naprakésszé, GDPR-kompatibilissá tételére. Azért is kézenfekvő továbbá erről az oldalról megindítani a vizsgálódást, mert a felhasználói oldalon tapasztalható hatások/előnyök gyakorlatilag a kötelezetti oldal tükörképei, és nem realizálódhatnak az adatkezelők/feldolgozók számára előírt kötelezetségek teljesedése hiányában. Az összeállítás elsősorban az üzleti szektorban várható hatásokra koncentrál, ami azonban összhangban áll az Irányelvben is lefektetett, és a Rendeletben továbbvitt azon alapvető elvvel, hogy az egységes és fejlett adatvédelem lényegében az Egységes Piac érdekeit kell hogy szolgálja. A GDPR létrejöttéről szóló fejezetben már érintett „új üzletág” következtében a legtöbb adatkezelő fenti kihívásoknak meg is próbált felelni, időt és költségeket nem kímélve. Kérdés, megérte-e a befektetett idő, energia, és nem utolsósorban: pénz? Az alábbiakban erre a kérdésre próbálok meg választ adni.

VI.1. Adatvédelem-tudatosság, fokozott kibervédelem:

Az előzetes felkészülésnek, és a GDPR által bevezetett, esetleges regulációsértés miatt kilátásba helyezett bírságok következtében az adatkezelők kötelessé váltak adatvédelmük modernizálására minden lehetséges szempontból. Az új adatvédelmi rendszerben a szolgáltatók nem engedhetik meg maguknak azt a luxust, hogy ignorálják az egyes szabályokat, ugyanis az jelentős pluszköltségeket eredményezhet, akár a bírság megfizetésére, akár a felügyelő hatóságok által alkalmazott intézkedések, mint pl. az adatkezelés korlátozása/tiltása miatti leállásra gondolunk. A legnagyobb vállalkozások, szolgáltatók fokozott és állandó veszélynek vannak kitéve. Az egyik legnagyobb internetes szolgáltató, a yahoo 2016-ban nyilvánosságra hozta hogy egy 2014-es hacker támadás következtében legalább 500 millió felhasználói fiók került feltörésre, míg egy évvel korábban 2013-ban egy még nagyobb, 1 milliárd felhasználói fiókot érintő támadás érte a rendszert, és azonnali hatállyal felszólította felhasználóit fiókjaik, jelszavaik frissítésére. A jelentést 2017 októberében frissítették, és az immár 3 milliárd felhasználói fiókot érintő hackertámadás máig a legnagyobb kibertámadásnak számít az internet történetében.[62] és a fokozott védelem kialakítása jelentősen csökkentheti a sikeres támadások számát a jövőben.

VI.2. Általánosan fejlettebb adatkezelés:

A GDPR következtében az egyes adatkezelők kénytelenek voltak naprakésszé tenni adatbázisaikat, megszabadulni a feleslegessé vált adatoktól, egységesíteni és rendszerezni a megmaradó adathalmazt. Ennek következtében átláthatóbb, könnyebben kereshető és karbantartható, költséghatékonyan exportálható modern adatbázisok jönnek létre európa- és világszerte. Ez jelentősen csökkenti az adatok tárolásának és feldolgozásának költségeit, egyúttal megelőzi azt is, hogy a vállalati/üzleti/hatósági értékkel nem rendelkező adatok miatt feleslegesen „főjjön az adatkezelő feje". A modernizált adatbázisok sokkal kevesebb gyengébb ponttal rendelkeznek, ezáltal kisebb rizikófaktort jelentenek a vállalkozásoknak. A fejlett adatkezelés megkönnyíti továbbá a Rendelet által bevezetett „elfeledtetéséhez való jog" adatkezelők általi teljesítését is, mivel sokkal könnyebb lesz megtalálni a törölni kért adatokat. A könnyebb kereshetőségnek további pozitív hatása lehet az

[62] https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/ Megtekintés dátuma 2022. június 20.

adatkezelő saját munkavállalói szempontjából, akik saját feladatiakat is hatékonyabban láthatják majd el a rendezettebb adatbázisnak köszönhetően.

Pontosabb felhasználói/vásárlói visszajelzések:

A GDPR egyik újítása az, hogy már nem elegendő az egyszerű „kipipálás", és nem lehet feltételezni sem az adatalanyok hozzájárulását, épp ellenkezőleg, főszabály szerint az adatkezelőknek úgy kell kialakítani a rendszereiket, hogy a felhasználóknak kifejezetten hozzá kell járulniuk ahhoz, hogy kívánnak-e egyáltalán a továbbiakban hallani az adott szolgáltató felől. Ez a gyakorlatban annyit tesz, hogy nem „leiratkozni" kell a rendszerint a kéretlen levél postafiókban landoló hírlevelekről, hanem épp ellenkezőleg, „feliratkozni" kell rájuk.[63] Közösségi oldalak tekintetében pedig ennek úgy kellene kinéznie, hogy alapbeállítások szerint minden opciónak privátnak kell lennie, és csak a felhasználó, a regisztrációt követően szabhassa testre saját adatvédelmi beállításait. Ez a módszer szintén minimalizálja az esetleges, és nehezebben megelőzhető jogsértéseket. Üzleti szempontból pedig nem elhanyagolható azon szempont, hogy ily módon a szolgáltatók pontosabb képet kapnak arról, hogy hány „valódi" vásárlójuk, ügyfelük van, ezáltal sokkal testre szabottabb szolgáltatásokat kínálhatnak.

VI.3. Fokozott felhasználói bizalom és hűség

A fenti hatékonyabb és biztonságosabb működés egyenes következményeként várhatóan növekedni fog a vállalkozásokba vetett bizalom, aminek kézzelfogható anyagi előnyein túl számos más pozitív hatása is lehet. Tekintve, hogy a GDPR körüli médiafelhajtásnak köszönhetően (is) egyre inkább megfigyelhető az adatvédelmi tudatosság felhasználói oldalról is, egy vállalkozás, szolgáltatás presztízsét jelentősen növelheti, ha GDPR kompatibilisként hirdeti szolgáltatásait, hasonlóan ahhoz, mint amikor a környezettudatosság globális szintűvé válásakor külön „bio"-üzletág alakult ki. Vigyázni kell azonban, hogy a „GDPR-cégér" ne kétélű fegyverként funkcionáljon, hiszen az önmagát GDPR-kompatibilisnek feltüntető szolgáltatóknak valóban annak is kell lenniük. Fontos figyelembe venni azt a körülményt is, hogy nagy számú vásárlótól/felhasználótól eshet el az a szolgáltató, akiről olyan híradások jelennek meg, hogy adatbázisát feltörték. A fejlettebb adatvédelembe fektetett pénz tehát itt fog megtérülni hosszabb távon, így azt egyfajta biztosításként is fel lehet fogni.

[63] „Opt-in" rendszer a korábbiakban használatos „opt-out" rendszerekkel szemben.

VII. Összegzés

Összegzésképpen megállapítható, hogy a GDPR az első négy éve alatt jelentősen felkavarta az adatvédelem állóvizét. Elsősorban nem is az általa kimunkált forradalmi újításoknak (bár ilyenekkel is rendelkezik) köszönhetően, hisz mint láttuk, az adatvédelem alapelvei több évtizedes múlttal rendelkeznek, hanem azért, mert bevezetése óta mind felhasználói, mind adatkezelői/feldolgozói oldalról jelentősen nőtt az adatvédelmi „aweraness"-szintje Európában.

A tudatosság fokozódása pedig mindenképpen együtt jár az érintettek alapvető jogainak fejlettebb és hatékonyabb védelmével, akkor is, ha az alapjog bevezetőben körüljárt látenciája miatt ennek nem is feltétlenül vagyunk tudatában. A bizottság által az előző fejezetben részletezett irányvonalak mentén az Unioban, és az egyes tagállamokban is folyamatos a GDPR, illetve az a tagállami jogszabályok monitorozása, fejlesztése. Magyarországon pl. 2022. január 01-től több ponton is módosult az Info tv. A módosítások az eljárási határidők számítását, az „elfeledtetéshez való jog" kérelemhez való kötöttségének eltörlését is érintette. Unios szinten a – az első, két év utáni jelentést követően – négyévenkénti Bizottsági jelentésen túl egy állandó testület, az European Data Protection Board (EDPB) is felállításra került a GDPR-el kapcsolatos fejlemények nyomon követésére, illetve a GDPR érvényesülésének folyamatos felügyeletére. Mint látható, intézményi és tagállami szinten a Rendelet nem „ül a babérjain". Mi a helyzet azonban velünk, felhasználókkal, akiknek érdekeit, és jogvédelmét elsődlegesen hivatott ellátni a GDPR? Mindenki tegye szívére a kezét, de azon kívül, hogy egy-egy új oldalra belépve több pipát kell elhelyeznünk, a cookie-k használatához egyes oldalakon pedig a sokat mondó „whatever" gombra kell kattintanunk a böngészés folytatásához, alapjaiban nem változott meg az életünk, illetve saját digitális alapjogainkhoz való hozzáállásunk. Ez azonban nem kérdőjelez(het)i meg a GDPR létjogosultságát és jelentőségét, aminek eredményeit nem az első pár év, hanem az elkövetkezendő évek, évtizedek alatt tapasztalhatjuk csak meg.

Irodalomjegyzék

- Jóri, A. (2010). *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*. (Doctoral dissertation, Pécs)
- Lenkovics, B. & Székely, L. (2000). *A személyi jog vázlata*. Eötvös József Könyvkiadó.
- Majtényi, L. (1997) *Adatvédelem, információszabadság*, Alkotmány- és Jogpolitikai Intézet, Budapest
- Mészáros, J. (2017). *Adatvédelem a XXI. században és az internet világában* (Doctoral dissertation, Szeged).
- Prosser, WL (1960) *Privacy* in: California Law Review, Vol. 48, No. 3
- Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vand. L. Rev.*, *52*, 1607.
- Szabó, M. D. (2005). Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. *Információs társadalom*, *2*, 44-54.
- Van Eecke, P., & Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, *26*(5), 535-546.

Hivatkozott jogszabályok, Uniós aktusok, nemzetközi dokumentumok

- Magyarország Alaptörvénye
- 1959.évi IV. törvény a Polgári törvénykönyvről
- 2013.évi V. törvény a polgári törvénykönyvről
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
- 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
- Az Európai Unió Alapjogi Chartája
- 2012/C 326/01 számú, az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata
- Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet

védelméről

- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
- Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről , valamint az ilyen adatok szabad áramlásáról
- OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról
- Európa Tanács Adatvédelmi Egyezménye
- A Bizottság 2016/1250 VÉGREHAJTÁSI HATÁROZATA (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről.

Hivatkozott bírósági határozatok, ítéletek:

- 8/1990. (VI.23.) AB határozat
- 20/1990. (X. 4.) AB határozat
- 15/1991. (IV. 13.) AB határozat
- A Bíróság 2008. december 16-án kihirdetett C-73/07.sz. ítélete
- A Bíróság 2010. június 29-én kihirdetett C-28/08.sz. ítélete
- A Bíróság 2011.november 06-án kihirdetett C-101/01 ítélete
- A Bíróság 2015. október 06-án kihirdetett C-362/14.sz. ügyben hozott ítélete
- A Bíróság 2016. október 19-én kihirdetett C-582/14.sz. ítélete