

AZ EURÓPAI UNIÓ BŰNÜGYI ADATVÉDELMI IRÁNYELVÉRŐL

A jog társadalmi viszonyok, érdekek, értékek védelmére, szabályozására szolgáló eszköze a mindenkori kormányzatnak. Történeti távlatokat tekintve a védendő, szabályozandó társadalmi viszonyok köre a gazdasági – politikai változással, a technikai-technológiai fejlődéssel folyamatosan változtak, változnak, bár jellemzően inkább bővülnek. Irk Ferenc a büntetőjog által védeni kívánt érdekek történeti fejlődését az alábbiakban összegezte: az első generációs érdekek közé tartozott az élet, testi épség megóvása, a mozgásszabadság, a nemiség, a tulajdon, az államélet biztonsága, a becsület tiszteletben tartása, második generációs érdekek a gazdasági élet, a természet, a közlekedés biztonsága, mint társadalmi érték, harmadik generációs érdekek az önrendelkezési jog, az adatvédelem.¹

Az adatvédelem kapcsán figyelemre méltó Ulrich Sieber és Cole Durham együttes véleménye, miszerint immateriális adatok esetében a tulajdon, mint jog-összesség többféle oszlik és e jogösszesség egyes elemei nem ritkán szembe állnak egymással, sőt versenyeznek egymással, ezért a szereplők jogköreinek tisztázása rendkívül fontos:

- a) az információt létrehozója, összeállítója,
- b) az információ jogszerű birtokosa, valamint
- c) az adatalany között,
- d) az információ szabad áramlásában érdekelt társadalmi érdekek.²

Figyelembe kell venni, hogy az a) b) c) pontokban felsoroltak között azonosságok is adódhatnak, ami versengésüket kizárhatja. Az adatvédelem, mint társadalmi érdek, érték – szabályozása generaliter - a technikai – technológiai változások, és Közép-Kelet Európában a politikai átalakulás is indukálta az adatvédelem kiterjedt védelmét.

Az adatvédelem fejlődése napjainkra több korszakot ível át. Szőke Gergely 1970-es évektől nagyjából évtizedekben mérhető három nagy korszakot különböztet meg.³ Magunk a második korszaktól, az 1980-as évektől tekintjük át az adatvédelem fejlődését. Ennek indoka az, hogy ebben a korszakban születtek az első – akkor még egyelőre csak – a nyugati világot érintő jogszabályok, nemzetközi jogi dokumentumok, például az OECD 1980-ban, illetőleg az Európa Tanács 1981-ben megalkotott normái nyitották meg az azóta is tartó jogalkotási hullámot.

A következő korszak jelentős az adatvédelem szempontjából. Ki kell emelnünk az 1990-es évek magyar Alkotmánybíróságnak aktivitását ezen a területen, számtalan máig ható alkotmánybírósági döntés látott napvilágot az 1990-es évek első felében. Az Európai Unió is reagált arra a rendkívül gyors technikai – technológiai fejlődésre, amely

¹ Magyar kriminálpolitikai és rendvédelmi koncepció. (Készítői között és szerkesztője: Irk Ferenc) Kriminológiai Közlemények 57. Budapest, 1999.

² Cole Durham: The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm. International Review of Penal Law. 1993. 1-2. 64. évf. p(s). 86-93. o. Vö. Sieber: The International Emergence of Criminal Information Law. Köln-Berlin-Bonn-München. 1992. p(s). 37-39. o.

³ Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. Infokommunikáció és Jog. 2013/3. 107-112. o.

nagytömegű adat, köztük személyes adatok kezelésére (gyűjtésére, tárolására, rendszerezésére, továbbítására) vált alkalmassá.⁴ Erre figyelemmel került kiadásra az Európai Parlament és a Tanács 95/46/EK Irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

Az Európai Unió az adatvédelemhez kapcsolódó több jogforrást tett közzé, idetartozik 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, majd 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 („Elektronikus hírközlési adatvédelmi irányelv”), továbbá az Európai Közösség Bizottság 2004/915/EK Határozata (2004. december 27.) a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről.

A 2010-es évekre az Európai Unió joganyag korszerűsítésre megérett. A két évtizedes joganyag korszerűsítésre várt, illetve az Európai Unió eddigi történetéhez képest példátlan bővülést élt át, és az adatvédelem területen észlelhető széttagoltság a jogalkalmazást nehezítette. A Nizzában 2000-ben elfogadott Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

A magyar Alaptörvény szinte szó szerint megismétli ezt a deklarációt: „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.” (Alaptörvény VI. cikk 3) bekezdése).

Hosszas előkészítő munkát, szakmai – tudományos vitát, a civil társadalom megkérdészt követően az Európai Parlament és a Tanács 2016. április 27-én adatvédelmi csomagot fogadott el, amelynek két elem van:

- az Adatvédelem Általános Keretét Meghatározó rendelet (2016/679/EU rendelet – GDPR) és
- a Bűnüldözési Célből kezelt személyes adatok védelmére vonatkozó irányelv (2016/680/EU irányelv – Bűnügyi Adatvédelmi Irányelv).

Még mielőtt a Bűnügyi Adatvédelmi Irányelvet áttekintjük, tisztázzuk az Európai Unió – egyszerűnek nem igazán nevezhető - jogforrásait: Az elsődleges jog alkotói a tagállamok, a másodlagos jog alkotói a jogalkotásra felhatalmazott közösségi intézmények, illetve szervek. Az EU elsődleges jogforrásait kormányközi döntéssel fogadják el, és azokat a tagállamok a maguk alkotmányos eljárásainak megfelelően ratifikálják. Ennek megfelelően az elsődleges jogforrások közé sorolandók: az alapító szerződések (EK-, Euratom-, Európai Unió-alapszerződések). Továbbá: az alapító szerződések egyes rendelkezéseit módosító szerződések (például a Maastrichti Szerződés, az Egységes Európai Okmány, az Amszterdami Szerződés, Nizzai Szerződés), a csatlakozási szerződések, valamint az egyes tagállamok által kötött nemzetközi egyezmények. A másodlagos (származtatott) jogszabályok az alapszerződéseken alapulnak és a szerződésekben lefektetett alapelvek megvalósulását szolgálják. Alapvetően kétféle származtatott jogszabály létezik. Az úgynevezett standard jogszabályok, amelyekről az alapszerződésben

⁴ Nagy Zoltán András: Az informatika és a büntetőjog. Magyar Jog 1991/1. 21-26.o

rendelkeznek: a rendeletek, irányelvek, döntések (kötelező érvényű jogszabályok), állásfoglalások és ajánlások (nem kötelező érvényű jogszabályok). Ami legfontosabb és a lény, a Rendeletet a magyar bíróságnak közvetlenül kell alkalmazni, figyelmen kívül hagyva az addigi magyar jogi szabályozást. A magyar jogi szabályozás akkor kerülhet elő, ha olyan kérdés eldöntéséről van szó, amelyet a Rendelet nem szabályoz. Az Irányelv (Direktíva) tartalma kötelező a tagállamok számára, ám azt, hogy milyen jogforrási szintre emeli be a tagállam, az Unió ezt az országaira bízta.

Az Irányelv megalkotásának indoka az, hogy a bűnüldözés során a tagállamok hatóságainak – a nemzetközi bűnözés és terrorizmus elleni küzdelem részeként – egyre gyakrabban kell személyes adatokat feldolgozniuk és továbbítaniuk. Ebben az összefüggésben az érintett hatóságok közötti együttműködés javításához elengedhetetlenül fontos, hogy az adatvédelemre Uniós szinten világos és koherens szabályozás vonatkozzon. A bűnügyi tárgyú adatkezelésre vonatkozó Európai Uniós szintű szabályok megállapítása megkönnyíti az Unió tagállamai különböző pontjain működő rendőri és büntető igazságszolgáltatási szervek gyorsabb és hatékonyabb együttműködését.

Az Irányelv a bevezetőben kinyilvánítja, hogy a gyors technológiai fejlődésből és a globalizációból adódóan a személyes adatok védelme új kihívásokkal került szembe. A személyes adatok gyűjtésének és megosztásának mértéke jelentősen megnőtt. A technika - technológia a személyes adatok minden eddiginél nagyobb mértékű kezelését teszi lehetővé olyan tevékenységek végzése érdekében is, mint a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy a büntetőjogi szankciók végrehajtása (Irányelv 3. pontja).

Az Irányelv hatálya a korábbi Kerethatározathoz⁵ képest kiterjesztő, ugyanis a bűnüldözési célú (beleértve a terrorizmus, a szervezett és a számítástechnikai bűnözés elleni küzdelmet is) adatkezelés mellett a közbiztonságot fenyegető cselekmények elleni védelemre és azok megelőzésére, valamint a nem állami, de bűnüldözési célból adatokat kezelő gazdasági társaságokra, szervezetekre (pl. a privát börtönökre) is kiterjed.

Nagyon fontos változás a személyes adatok újszerű megközelítése. Az Irányelv a genetikai adat, mint az adatalannal összefüggésbe hozható adatot is meghatározta: „A genetikai adatot olyan, a természetes személy örökölt vagy szerzett genetikai jellemzőivel összefüggő személyes adatként célszerű meghatározni, amely az adott természetes személy fiziológiájára vagy egészségi állapotára vonatkozóan egyedi információt hordoz, és amely az adott természetes személy biológiai mintája elemzésének, így kromoszómaelemzésnek, illetve a dezoxiribonukleinsav (DNS) vagy a ribonukleinsav (RNS) vizsgálatának, vagy az ezekből kinyerhető információkkal egyenértékű információk kinyerését lehetővé tevő bármilyen más elem vizsgálatának az eredménye. A genetikai információk összetettségére és érzékenységére figyelemmel jelentős a kockázata annak, hogy az adatkezelő visszaél az ilyen információkkal, és különböző célokra újra felhasználja azokat. A genetikai jellemzők alapján történő bármilyen megkülönböztetés tilos.” (23. pont)

A büntető igazságszolgáltatásban dolgozó számára figyelmeztető a bűncselekmény fogalmának értelmezése. A bűncselekmény fogalma ugyanis „az Európai Unió bírósága általi értelmezésnek megfelelő, önálló jogi fogalom.” (Irányelv 13. pontja) Tehát nem a nemzeti jogban megfogalmazott bűncselekmény fogalom az irányadó. A kollíziót az Irányelv és a nemzeti jog bűncselekmény fogalma között a GDPR azzal oldja fel, ami a

⁵ A Tanács 2008/977/IB Kerethatározata (2008. November 27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről

Rendeletben jogsértésként van meghatározva és az EU Bírósága elfogadja – az lesz az adatvédelmet sértő bűncselekmény és nem a 2012 évi C. törvény a Büntet Törvénykönyvről idevonatkozó fogalmai (219-220. %).

Az Irányelv néhány általános célkitűzése:

- Természetes személyeket állampolgárság és lakhelytől függetlenül megilletik az irányelv védelmi mechanizmusai (Irányelv 17. pontja).
- Természetes személyek adatainak védelme nem függ attól, hogy technikai eszközzel vagy manuálisan kezelik adataikat. Olyan iratok, amelyek *nem rendszerezettek* nem tartoznak az irányelv hatálya alá (Irányelv 18. pontja.). (Magyarozatként: rendszerezett az irat, ha irategységet (aktát) képez az adott ügyben.)
- A hazai törvényalkotás felé fontos figyelmeztetés. Az Irányelv is megköveteli az Európai Bíróság (más néven Az Európai Közösségek Bírósága vagy Az Európai Unió Bírósága), továbbá az Emberi Jogok Bírósága által is megfogalmazott követelményeket a jogalkotással szemben, így az adatvédelemmel összefüggésben rendelkezni kell a jogszabály céljáról, a kezelendő személyes adatokról, az adatkezelés céljairól, a személyes adatok integritásának és bizalmas jellegének megővéséről, valamint a személyes adatok megsemmisítésére irányuló eljárásokról (Irányelv 33. pont).
- Az Irányelv követelményt támaszt a jogalkalmazók irányába, miszerint: a személyes adatok kezelését jogszerűen és tisztességesen kell végezni; gyűjtése csak meghatározott, egyértelmű és jogszerű célból, kezelése pedig kizárólag ezekkel a célokkal összeegyeztethető módon történjen; az adatkezelés céljai szempontjából megfelelőek és relevánsak, valamint nem túlzott mértékűek kell, hogy legyenek; pontosak és amennyiben szükséges naprakészek legyenek; tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; megfelelően biztosítva legyenek, az adatok jogosulatlan vagy jogellenes kezelésével szembeni védelmet is ideértve. (Irányelv 29 – 30. pontjai).
- Szintén a jogalkalmazók felé fordul az Irányelv, amikor kimondja, hogy az érintett rendelkezésére kell bocsátani legalább a következő információkat: az adatkezelő kilétét, az adatkezelési művelet tényét, az adatkezelés céljait, tájékoztatást a panasz benyújtásának jogáról, valamint az ahhoz való jogról, hogy az érintett az adatokhoz való hozzáférést, az adatok helyesbítését, törlését, illetve az adatkezelés korlátozását kérje az adatkezelőtől.” (Irányelv 42. pont első fordulata). Ezt a tájékoztatást az illetékes hatóság honlapján is közzé lehet tenni. Továbbá, egyedi esetekben és annak érdekében, hogy az érintett gyakorolni tudja a jogait, az érintettet tájékoztatni kell az adatkezelés jogalapjáról és arról, hogy mennyi ideig fogják az adatokat tárolni, ha az adatkezelés konkrét körülményeit figyelembe véve ezekre a kiegészítő információkra szükség van az érintett vonatkozásában a tisztességes adatkezelés garانتálásához. (Irányelv 42. pont második fordulata)
- Az Irányelv előírja azt is, hogy az adatkezelés során egyértelmű *különbséget kell* tenni olyan személyek, akik tekintetében
 - alapos okkal feltételezhető, hogy bűncselekményt követtek el vagy készülnek elkövetni;
 - bűncselekmény elkövetéséért elítélt személyek;

- bűncselekmény áldozatai, illetve olyan személyek, akikről bizonyos tények alapján okkal
- feltételezhető, hogy bűncselekmény áldozatai lehetnek;
- a bűncselekmény kapcsán érintett egyéb felek, például lehetséges tanúk. (Irányelv 7. Cikk)
- Az érintett (jogalanya) jogait határozza meg az Irányelv akkor, amikor deklarálja a felügyeleti hatósághoz történő panasztétel jogát és a hatóság elérhetőségét (Irányelv 52 - 55. cikkei).
- Az adatalany személyes adataikhoz való hozzáférés, valamint azok helyesbítése vagy törlése kérelmezésének jogát, valamint a személyes adataik kezelése korlátozásának jogát. Az adatalannak a hatóságnál kezelt személyes adataihoz főszabályként hozzáférés jogosultsága van, ám ez korlátozható. A hozzáférés korlátozásának esetköreit nézzük szó szerint az Irányelvből:
„A tagállamok számára lehetővé kell tenni, hogy jogalkotási intézkedéseket fogadjanak el az érintettek tájékoztatásának késleltetésére, korlátozására vagy mellőzésére, illetve a személyes adataikhoz való hozzáférésük teljes vagy részleges korlátozására vonatkozóan, amennyiben, illetve mindaddig, amíg az említett intézkedés – kellő tekintettel az érintett természetes személy alapvető jogaira és jogos érdekeire – egy demokratikus társadalomban szükségesnek és arányosnak minősül a következők érdekében: ne gördüljenek akadályok a hivatalos vagy jogi vizsgálatok, nyomozások vagy eljárások elé; annak elkerülése, hogy a bűncselekmények megelőzése, felderítése, nyomozása, a vádeljárás lefolytatása vagy a büntetőjogi szankciók végrehajtása veszélybe kerüljön; a közbiztonság vagy nemzetbiztonság védelme; valamint mások jogainak és szabadságainak védelme. Az adatkezelőnek minden egyes eset konkrét és egyedi vizsgálatokor fel kell mérnie, hogy a hozzáférési jog részleges vagy teljes korlátozása szükséges-e.” (Irányelv 44. pont)

Az adatkezeléssel összefüggő biztonsági követelmények⁶, amelyek bűncselekmény elkövetéséhez is vezethetnek:

- a jogosulatlan személyek számára a hozzáférés megtagadása az adatkezeléshez használt adatkezelő berendezésekhez;
- az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozása;
- a személyes adatok jogosulatlan bevitelének, valamint a tárolt személyes adatok jogosulatlan megtekintésének, módosításának vagy törlésének megakadályozása. (Irányelv 29. cikk)

Az adatok külföldre továbbításának problémája harmadik országnak történő kiadás esetében az irányelv szigorú rendelkezéseit be kell tartani (Irányelv 39. Cikk)

Nem kevés kockázatot jelent a tagállamok állampolgárainak személyes, sőt különleges adatainak továbbítása. Mind az EU tagállami, mind az adatalany elveszti kontrollját a személyes (különleges) adatai felett és adatai egy másik jogrendszert, belső szabályokat használó országba kerül át. Veszélyt jelent, ha az adott országban az adatvédelemre vonatkozó rendelkezések kevésbé szigorúak. Nem kell messzire sem

⁶ Gyarmati Réka: Az informatikai biztonság szükségessége In: Kiss Dávid, Orbók Ákos (szerk.) A haza szolgálatában konferencia, rezümékötet. Nemzeti Közszolgálati Egyetem, Budapest, 2014. 156-158. o.

mennünk, gondoljunk Magyarországnak nem Uniós szomszédaira, vagy a dél-balkáni országokra stb. Nem is szólva a Világ más tájain fekvő országokra. Mivel összekapcsolt számítástechnikai rendszerekről van szó, az adatszivárgás vagy más adatvédelmi incidensnek hatást gyakorolhat (kárt okozhatnak) más ezen adatokat kezelő informatikai rendszerekben. Az adatvédelmi incidenst azonnal, de legkésőbb 72 órán belül jelteni kell a felügyeleti hatóságnak.(Irányelv 61-62. pontja). Az adatkezelésért felelős személyek elszámoltathatóak lesznek munkájukért. Az Irányelv rendelkezéseit megszegőivel szemben, akár büntetőjogi, akár polgári jogi szankciót lehet kiszabni. (Irányelv 89. pontja és 4. cikk (4) bekezdése) Adatvédelmi tisztviselőt kell kinevezniük, aki a szervezeten belül felelős a személyes adatok védelméért (Irányelv – 63. pont).

Egyéb fontos(nak) tartott rendelkezés:

- Kölsönös segítségnyújtási kötelezettség a tagállamok számára (Irányelv 50. cikk).
- Az Irányelv rendelkezéseinek be nem tartása szankciót von maga után az Európai Unió részéről (Irányelv 57. cikk).

A GDPR-ral és a Bűnügyi Adatvédelmi Irányelvvel kapcsolatos jogalkotási feladatok várnak a Magyar Országgyűlésre. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény átfogó módosítására fog sor kerülni. A törvényből ki kerülnek azok a rendelkezések, amelyeket a GDPR szabályoz, maradnak olyan rendelkezések, amelyeket a GDPR nem szabályoz, illetőleg a törvénybe bekerülnek a Bűnügyi Adatvédelmi Irányelvben meghatározott rendelkezések, amelyek nem részei még a magyar jognak.