EÖTVÖS LORÁND TUDOMÁNY EGYETEM
ÁLLAM- ÉS JOGTUDOMÁNYI KAR
Jogi Továbbképző Intézet
Adatbiztonsági és adatvédelmi szakjogász képzés

DR. CSABA JÓZSEF:

A SZEMÉLYES ADATOK BÜNTETŐJOGI VÉDELME

Incidenskezelés a Büntetőjog által szankcionált támadások estén

szakdolgozat

Konzulens:
DR. ESZTERI DÁNIEL

Budapest, 2018

1 BEVEZETÉS

1.1 Az értekezés tárgya:

A szakdolgozati témaválasztásnak több oka is van. Hosszú éveket töltöttem a bűn üldözésével hivatásos rendőrtisztként, majd – többek között – bűnmegelőzéssel, jogi megfelelési (Compliance) igazgatóként egy kereskedelmi bankban. Nagyon hamar kialakult bennem a kérdés: vajon mi az oka annak a szemérmességnek, ami az áldozatokat – legyenek azok természetes- vagy jogi személyek – visszatartja a büntetőeljárás kezdeményezésétől?
Az emberi szabadság- vagy a nemi erkölcs elleni bűncselekmények esetében teljes mértékben érthető, és értelmezhető az áldozat ódzkodása. A korrupciós bűncselekmények esetén meg – az anyagi jogi értelemben vett – passzív alany nem is tekinthető áldozatnak, így az ő érdekében is áll a hallgatás. Még – bizonyos értelemben – arra is lehet magyarázat, ha egy pénzintézet belső vizsgálata által feltárt *Bennfentes kereskedelem (Btk. 410.§)* bűntett megalapozott gyanúja esetén sem kíván a munkáltatói jogokat gyakorló bűntető feljelentést tenni.
De mi az oka a vagyon elleni- vagy az adatvagyont az adatbiztonságot veszélyeztető bűncselekmények – lehetséges – titokban tartásának?

Álláspontom szerint, az adatvédelem, az információ-biztonság olyan területek, melyek megkülönböztetett figyelmet érdemelnek a XXI. századi, modern nagyvállalatok operatív irányításában. Tapasztalataim azonban azt mutatják, hogy a vállalatok nagy többsége még nem tudja helyén kezelni ezt a kockázatot. Jellemzően megelégednek azzal, hogy az adatvédelemmel kapcsolatos kockázatkezelés során kijelölik az informatikai biztonságért felelős területet, a szükséges technikai feltételek megteremtésére. Az az általános vélekedés, hogy egy jól felépített informatikai környezet kellő hatékonysággal képes megvédeni a kezelt – és egyben óriási értéket képviselő – adatvagyont. Sok esetben – teljeséggel – hiányzik, vagy csak részben felépített az a szervezet, amelyik képes folytonos – a legfrissebb tendenciákat is nyomon követő – elemzéseket elvégezni, valamint – az eredmények birtokában – megfelelő szervezési intézkedéseket foganatosítani.

Az Európai Unióban 2012-ben megkezdett, a személyes adatok védelmét érintő jogalkotási folyamat eredményeként a Tanács és az Európai Parlament – mint társ-jogalkotók – 2016-ban *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 szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet* (a továbbiakban: Rendelet) elfogadásáról döntöttek.

Tekintve, hogy egy olyan kereskedelmi bank Compliance területét vezettem, amelyik rendkívüli figyelmet fordított az ügyfelei személyes adatainak megfelelő kezelésére, ahol – a fentiekben leírtaktól eltérően – nem csak informatikai megoldásokkal igyekeztek az adatvédelmi kockázatokat csökkenteni, így már a jogalkotási folyamat kezdetétől nyomon tudtam követni a joganyag előkészítési folyamatát. A bank anyavállalata ráadásul egy brüsszeli székhelyű kereskedelmi bank, így hónapról, hónapra volt lehetőségem eszmét cserélni a folyamat során felmerülő diskurzusokról.

Összegezve a fent leírt tapasztalatokat egyre inkább megfogalmazódott bennem a gondolat, hogy a személyes adatok feletti őrködés egy – nagyon fontos – eleme hiányzik a közgondolkodásból, de – talán – még a vonatkozó jogszabályi környezetből is.

Ha a GDPR megalkotásakor az volt a jogalkotói szándék, hogy az az Európai Unió területén kezelt személyes adatvagyon – mint *virtuális vagyoni érték* – minél hatékonyabban hasznosuljon az Unió gazdaságában, de az adatok – emellett – hatékonyabb védelemben is részesüljenek az illegális támadásokkal szemben, akkor az adatvédelmi incidensek kezelésére – talán – több figyelmet is lehetett volna fordítani. Ha már néhány tagállam – köztük Magyarország – ellentétes véleménye ellenére is rendeletben szabályozta az egységes adatkezelési, adatvédelmi elvárásokat – hangsúlyozva az *egységes piac, egységes gyakorlat elvét* – akkor zászlajára tűzhette volna a Tanács és a Parlament az *„egységes büntető jogi fellépés”* igényét is.

Dolgozatomban igyekszem majd rávilágítani arra, hogy mit gondolok szükségesnek megvalósítani a jövőben, hogy a fent leírt – az intellektuális bűncselekményekre szakosodó alvilág szemében is felmérhetetlen értéket képviselő – adatvagyon valóban úgy teremtsen hozzáadott értéket a határokon átnyúló gazdaság számára, hogy az

adatkezelők az Unió polgárainak privát szféráját (privacy) megfelelő biztonságban tudják majd tartani.

1.2 A dolgozat tagolása

- Az információs társadalom fogalom kialakulása, jelentése
- Az EU információs társadalom célkitűzései
- A számítógépes fenyegetések értékelése
- A privacy fogalomkör az információs társadalomban
- Az információs társadalom szülte új devianciák
- Az „e bűncselekmények”
- A GDPR adatvédelmi incidens fogalomrendszere
- Az incidenskezelés büntetőjogi aspektusai
- Az „új” Btk. vonatkozó törvényi tényállásai
- A hatékony adatvédelmi kockázatkezelés elemei

2 Az információs társadalom kialakulása, fejlődése a kezdetektől napjainkig

2.1 A fejlődés folyamata

Az információs társadalom kutatásával foglalkozó szociológusok, történészek, kriminológusok jellemzően három (ritkábban négy) megközelítési módszert választanak.

Pintér Róbert szerint[1] négyféleképpen definiálhatjuk az információs társadalmat: *Technológiai értelemben* az információval és a tudással végzett műveletek és az ezekhez kapcsolódó infokommunikációs eszközök állnak az információs társadalom középpontjában. *Társadalmi értelemben* a hálózati társadalom és hálózati gazdaság kialakulása, a közösségiség, a folyamatos adaptáció, az újfajta egyenlőtlenségek és a globalizáció jellemzik. A *fejlesztési narratíva értelmében* az információs társadalom

[1] PINTÉR, R., Divatos hívószavak, nagy elméletek, fejlesztési szupernarratívák és metanarratívák – Az információs társadalom jelentésvilága. PINTÉR Róbert*; Budapest, 2007*
http://docplayer.hu/3677572-Divatos-hivoszavak-nagy-elmeletek-fejlesztesi-szupernarrativak-es-metanarrativak.html

utal egy korszak- és paradigmaváltásra (ipari társadalom utáni korszak), illetve egy gondolkodásmódra (amely leírható mint eszme vagy fejlesztési szupernarratíva). Végül az információs társadalom a *tudományos vizsgálat tárgyaként* is megjelenik *(information society studies).*

Álláspontom szerint nincs lényegi különbség a technológiai és a fejlesztési megközelítés között. A társadalmi aspektusok viszont olyan lényeges elemek, melyek megértése elengedhetetlen, ha meg akarjuk érteni, hogy válik egyre inkább célpontjává az információs társadalom és a közösséget alkotó egyén (felhasználó, vagy adatalany) az intellektuális bűncselekmények áldozatává.

2.1.1 Az információs társadalom fejlődésének technológiai alapja

Az információs társadalom kialakulásának és fejlődésének egyik legmeghatározóbb jellemzője a – mindent és mindenkit körülvevő - informatikai és telekommunikációs eszközök számának, sokféleségének, komplexitásának növekedése, valamint ezek folyamatos és szinte követhetetlen tempójú változása.

A XX. század vége újra egy – az ipari forradalomhoz hasonlítható jelentőségű – technológiai változást hozott az emberiség történelmébe. Megjelent, és az átlag felhasználók életének részévé vált a személyi számítógép a PC. Az eltelt alig harminc év alatt az informatikai fejlődés – korábban soha nem látott sebességgel – változtatta meg a gazdasági élet szereplőinek és a társadalom egyedeinek világról és a fejlődés lehetséges irányairól alkotott képét.

2.1.2 A személyi számítógép

A folyamat kiinduló pontja, első szintje tehát a gazdasági, tudományos és a társadalom egésze számára hozzáférhető, az adatok automatizált feldolgozását, továbbítását, tárolását lehetővé tevő számítógép megjelenése.[2]

A számítógép nem csak többszörösére gyorsította az adatok feldolgozását, de a kreativitás ösztönzésével új, magas hozzáadott értékű szolgáltatások és termékek

[2] Szathmáry Zoltán: Alkotmányos büntetőjogi dilemmák az információs társadalomban *Doktori értekezés (25. old) Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskolája „Informatikai és Kommunikációs Jog" Program; Budapest, 2012*

előállítását lehetővé tevő kapacitáshoz juttatta a felhasználókat. Az új erőforrás megjelenésétől kezdve többoldalú védelmet igényelt, másrészt – természetéből fakadóan – új jogi tárgyakat, új, védendő társadalmi érdekeket teremtett.

2.1.3 A számítógépek összekapcsolása, a világháló

Döntő szakasza volt a fejlődésnek, hogy a katonai és tudományos élet területéről kitörve az egyre kisebb méretű, egyre könnyebben kezelhető ám több perifériát csatlakoztatni képes és olcsóbb számítástechnika egyre több és több ember számára vált hozzáférhetővé. 1981-ben az IBM piacra dobta a már nevében is személyeknek szánt PC-t, azaz a *personal computer* -t.[3]

1992-ben megalapították a Virginia állam béli Internet Society (ISOC) nonprofit szervezetet. A szervezet azért felel, hogy összehangolja, és felügyelje az – exponenciális ütemben bővülő – számítógépes hálózatok rendszerét. Létrejött az Internet világháló a Word Wide Web (WWW).

Mivel az internet egymástól különböző hálózatokat köt össze, a felhasználó bátran választhat bármilyen eszközt munkája elvégzéséhez, az adatokat a hálózaton keresztül egységesen tudja kezelni. Ma már elmondható, hogy az internet a világ elektronikus postájává lépett elő.

A legfontosabb hozadéka azonban az, hogy a – korábban kizárólag – egyirányú, üzenetközvetítő médiumokkal szemben a felhasználó nemcsak passzív befogadó, hanem maga is információforrás, aki maga választhatja meg, hogy milyen információra kíváncsi, milyen más információforrásokat követ, vagy éppen milyen új információkat tesz közzé.

Egyre újabb és újabb infokommunikációs eszközök váltak minden ember számára elérhetővé (pl.: laptop, netbook, palmtop, PDA, okos telefonok, tabletek, stb.). A sokrétű személyi hírközlési eszközök integrálták a mobil távközlés, a kép- és mozgóképrögzítés, a hang- és video alapú szórakoztatás, a navigáció funkcióit, a különböző szolgáltatásokhoz tartozó személyazonosító kártyákat, kódokat, az elektronikus aláírást, és fizetési módokat.

[3] Szathmáry Zoltán: Alkotmányos büntetőjogi dilemmák az információs társadalomban *Doktori értekezés (26. old) Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskolája „Informatikai és Kommunikációs Jog" Program; Budapest, 2012.*

2.1.4 A digitalizáció konvergencia hatása a gazdaságban és a társadalom egészében

Koppányi Szabolcs szerint[4] a tapasztalható változás nem azt jelenti, hogy a – korábban elkülönült gazdasági, társadalmi folyamatok – konvergenciájának hatására az eddigi alszektorokból egy új, egységes, mindent átfogó médium alakulna ki, hanem, hogy az információk megjelenési formája válik kompatibilissé, amelynek következtében az információhoz különböző kommunikációs eszközök közvetítésével (internet, telefon, televízió) hozzájutva elmosódnak a határok mind a tömeg- és az egyéni kommunikáció, mind pedig az elosztó és közvetítő médiumok között.

Az új informatikai eszközök és megoldások az eredményezték, hogy a digitalizáció a tartalmak platform-független közvetítésének fejlődésével a korábban elkülönült gazdasági ágazatok, úgymint az informatika, a távközlés és a média közeledését, összeolvadását is elindította.

Ugyanez a folyamat tetten érhető a társadalmi viszonyok átalakulásában is. A távközlésre korábban jellemző bináris (két személy között zajló) kommunikáció kiegészült a különböző – egymással online kommunikáló – csoportok viszonyrendszerével.

A technológiai és társadalmi – fent vázolt – változások értékelése elengedhetetlen, mert meghatározza az informatikai bűncselekmények elkövetésének környezetét nem csak infrastrukturális, hanem kulturális értelemben is.

2.1.5 A technológiai fejlődés társadalmi hatásai.

Az infokommunikációs platformok működtetése, az online kereskedelem, a banki vagy befektetési műveletek elérése döbbenetes tempóban változtatja meg világunkat. A klasszikus iparágak, kereskedelmi folyamatok sem működhetnek már a digitalizált eszközök, és szolgáltatások nélkül. Ha egyáltalán életben képesek maradni a digitális világháló nyújtotta új kereskedelmi, banki, vagy egyéb más gazdasági formációkkal szemben.

A technológiai robbanás szülte gazdasági változások új társadalmi érdekek megjelenését hozták magukkal. A korábbi viszonyrendszerek – óhatatlanul – a technológiai fejlődés

[4] KOPPÁNYI Sz., *Hírközlési jog az európai közösségben és Magyarországon,* Osiris Kiadó Budapest, 2003.

rohamtempójában alakulnak át. A kérdés csak az, hogy az új társadalmi viszonyok, érdekek, és védendő értékek kellő gyorsasággal és hatékonysággal kerülnek e jogalkotói górcső alá? Képes-e az igazságszolgálgatás lekövetni az új társadalmi viszonyok fogalomrendszerét, és megfelelően alkalmazni az új jogszabályokat? Van-e olyan szakértő apparátus aki korrekt módon interpretálni képes azokat a szakkérdéseket, melyek megválaszolása elengedhetetlen egy – a fent vázolt új viszonyokból származó – eldöntendő jogvita, vagy éppen büntető ügy kapcsán?

2.1.6 Amikor a tér és az idő dimenzió már szinte nem értelmezhető

Az ügyfeleiket tömegesen kiszolgálni szándékozó kereskedelmi vállalkozások, pénzügyi szolgáltatók – költséghatékonysági szempontokat figyelembe véve – mind gyakrabban keresik az olcsó – és a jelen közgondolkodás szerint – biztonságosnak tekintett felhő szolgáltatókat.

Az informatikai rendszerek üzemeltetése egyre inkább közműjelleggel és szolgáltatásszerűen történik, ami részben abban nyilvánul meg, hogy a felhasználók személyi számítógépein installált programok mind nagyobb része kerül központi szolgáltatásként futtatva, gyakran a felhasználó adatainak nagy részét is a szolgáltató szerverein tárolva. Ennek az a kockázata, hogy a felhasználók adatai a szolgáltatók birtokába kerülnek, és azokra a felhasználónak pusztán csak igénye van.

A változás oly annyira robbanásszerű, hogy szinte még fel sem tettük a megfelelő kérdéseket – nemhogy megválaszoltuk volna azokat – már változik is körülöttünk a virtuális világ.

A felhő technológia (cloud computing) széleskörű terjedése kapcsán a felmerülő kérdések, melyekre a jogalkotóknak, jogalkalmazóknak választ kell találniuk: kinek van joghatósága; illetékessége; mi az elkövetés helye; büntethető-e a feltárt magatartás?

2.2 A várható tendenciák

Az elmúlt harminc év informatikai technológiai fejlődését vizsgálva Szathmáry Z[5] az alább felsorolt, további változásokat vetíti előre:

- A számítógépek és adatátviteli vonalak teljesítményei oly mértékben növekednek, hogy gyakorlatilag nem jelentenek majd korlátot a megoldandó feladatok méreteire vonatkozóan.
- Teljessé válik az eszközök összekapcsoltsága, nem lesznek elszigetelten működő számítógépek.
- Az információfeldolgozás és adatátvitel lehetőségei megjelennek az embert körülvevő környezet tárgyaiban (pl. háztartási berendezések, járművek), akár az emberi testben, gondoljunk a különféle bionikus protézisekre, készségjavító implantátumokra.
- Az informatikai rendszerek működése egyre több intelligens vonást mutat.
- A rendszerekben a szolgáltatások különböző fajtái kerülnek előtérbe, a felhasználók mind inkább szolgáltatásokat és nem termékeket vásárolnak.
- Az infokommunikációs rendszerek fokozott mértékben támogatják az őket használó emberek együttműködésének különböző formáit.
- Az infokommunikációs rendszerek működésének biztonsága egyre nagyobb kihívást jelent.

A felsorolt változások nem is túl távoliak, így a bekövetkezésük nem egy merész jóslat. Egyre másra jelennek meg a piacon azok az alkalmazások melyek már a szupergyors „BIG DATA" analitikán, vagy az öntanuló rendszereken (self-learning machine) alapulnak.

A fejlődési folyamat eredményeképpen az internet egyre inkább interfész-szerepet tölt majd be a helyüket változtató emberek és az őket körülvevő fizikai világ között, végül olyan egységes és programozható rendszerré válhat, amely megtestesíti a korábbi kibertér *(cyberspace)* víziókat.[6]

A „**kibertér"** kifejezést William Gibson tudományos-fantasztikus (sci-fi) író alkotta meg az – 1982-ben megjelent – "Burning Chrome" című novellájában majd később az 1984-es „Neurománc" című regényében.

[5] Szathmáry Zoltán: Alkotmányos büntetőjogi dilemmák az információs társadalomban *Doktori értekezés (30. old) Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskolája „Informatikai és Kommunikációs Jog" Program; Budapest, 2012*

[6] DÖMÖLKI, B., KÓSA, Zs., KÖMLŐDI, F., KRAUTH, P., & RÁTAI, B., *Égen-földön informatika – Az információs társadalom technológiai távlatai,*

Munk Sándor – nem rég publikált értekezésében – több helyen rávilágít a kibertér alkotta potenciális viszonyok megválaszolásra váró kérdéseire. Hol vannak a határok a valós és a virtuális világ között?

A fejlett információtechnológia eredményeként kialakuló hálózatok egy olyan szolgáltatási, virtuális működési környezetté, sőt „életkörnyezetté" váltak, amelyek mindenki számára érzékelhető virtuális térként, világként megélhető környezetet alkotnak. Ebben a „térben" szereplők tevékenykednek, folyamatok zajlanak, események történnek, amelyek pozitív hatással, vagy negatív (káros, vagy akár pusztító erejű) következményekkel vannak a „hagyományos" világ szereplőinek életére, tevékenységére.[7]

Munk – katonai biztonsági elemzőként – a kibertér veszélyei közül a biztonsági kérdésekkel foglalkozik tanulmányában.

Ennél a körvonalazott új világ kicsit komplexebb. Talán a legfontosabb kérdés, hogy vajon a kibertér pusztán virtuális, vagy vegyes jellegű (vagyis léteznek fizikailag létező összetevői is). A virtuális környezet és a virtuális környezetben található virtuális tárgyak feletti rendelkezési jogosultságok (átruházás, megszüntetés, jogutódlás), virtuális tárgyak eltulajdonításáért való felelősség egyúttal számos új szabályozási kérdést vetnek fel.

2.3 Az új védendő értékek

Az információs társadalom fejlődésének – a fentiekben vázolt – elemzése az új társadalmi érdekek és azokon keresztül a büntetőjog által védett jogi és elkövetési tárgyak meghatározását célozta. A technológiai/ társadalmi megközelítés mentén az szögezhető le, hogy a társadalom szinte valamennyi alrendszerének – legyen az a politika, jog, gazdasági élet vagy magánélet – informatizálása zajlik. Az alrendszerek mindegyikében – az ott korábban kialakult – társadalmi viszonyokra kihatással van. Az érintett, - vagyoni, szellemi, gazdasági – értéket képviselő társadalmi viszonyok büntetőjogi leképeződései a védendő jogi tárgyak.

Ahogy Szathmáry kifejti:

- Egyfelől kiemelt társadalmi érdekként jelent meg magának a kommunikációs *infrastruktúra* biztonsága, megfelelő védelme, hiszen az a rajta keresztül

[7] Munk Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései, 2018 Budapest*

folytatott interakciók, virtuális aktusok mennyisége és fajtája miatt – függetlenül a tartalmukhoz kapcsolódó érdekszféráktól – meghatározó a társadalom legtöbb tagja, entitása (az állami szervek, gazdasági szereplők, magánszemélyek) számára.[8]

- Másrészt a jogi tárgyak tekintetében elmondható, hogy az elemzett technológia olyannyira része a mindennapok életvitelének, az állami és gazdasági életnek, hogy ugyancsak kiemelt társadalmi érdek a fenti infrastruktúrához való *hozzáférés*, és az azon folytatott interakciók *biztonsága, hitelessége, bizalmassága*.[9]

Valószínűleg pusztán tudományos szempontokból van jelentősége a különbség tételnek. Számomra – a kriminogén jelenségeket gyakorlatiasabb szemmel vizsgáló elemzőnek – ez egy és oszthatatlan. Maga a kiépített – és rohanó tempóban továbbfejlődő – számítástechnikai infrastruktúra és annak zavartalan, biztonságos és hiteles működése a védendő jogi érdek.

2.4 A globalizáció adta kihívások

Mint ahogy majd a későbbiekben igyekszem bemutatni, az Európai Unió döntéshozói is ideje korán felismerték az információs társadalom robbanásszerű kialakulásában rejlő kockázatokat, mégis – a tagállamok, és az állampolgárok számára némileg zavaró módon – hiányzik az egységességet biztosító koherens jogalkotási folyamat.
Az jól tetten érhető, hogy az Unió – noha gyakran szöges ellentétben álló politikai érdekek figyelembevétele mellett kénytelen szabályozási folyamatait mederben tartani – igyekszik adekvát válaszokat találni az információs társadalom által vezérelt globalizációból fakadó veszélyekre.

Vizsgálva az elmúlt évek EU –n belül zajló politikai csatározásait, szabályozási és döntés-előkészítési folyamatait az a kép kezd kirajzolódni, hogy nagyobb a politikai akarat az Unión belül struktúrákba rendezett adatvagyon hasznosítása mellett, mint a személyes adatok – egységes és megfelelően integrált – megvédése érdekében.

[8] Szathmáry Zoltán: Alkotmányos büntetőjogi dilemmák az információs társadalomban *Doktori értekezés (31.old) Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskolája „Informatikai és Kommunikációs Jog" Program, Budapest, 2012.*

[9] Szathmáry Zoltán: ugyanott

Az Általános Adatvédelmi Rendelet (General Data Protection) megalkotási folyamatában mind a tagállamok, mind a képviseletükben eljáró politikai csoportok más és más szándékkal ültek le a tárgyaló asztalhoz. Az szinte már megszokott, hogy más a politikai érdekrendszere a fejlett nyugati államoknak, és – az őket utolérni szándékozó – közép európai új tagoknak. Az is egyre inkább kirajzolódik, hogy a baloldali tömörülés – gyakran szignifikánsan – mást gondol az egyes politikai programokról és a mögöttes szabályozandó társadalmi viszonyokról. A GDPR megalkotása során azonban még tagoltabb, még szerteágazóbb politikai érdekek feszültek egymással szembe.
A végeredmény az EU Rendelet talán épp ezért lett olyan amorf, kissé túlburjánzó és meglehetősen szokatlan (ld: 173 preambulum bekezdés, 31 oldalon keresztül) jogszabály.
Elemezve a Rendelet preambulumában megfogalmazott elveket látható a jogalkotói kettős szándék:

- megvédeni az Unió állampolgárainak személyes adatait;
- biztosítani a személyes adatok Unión belüli szabad, akadálymentes áramlását.

Noha hosszasan tagolja a preambulum az állampolgárok privát szférájához fűződő állampolgári jog súlyát és jelentőségét, de egyben hangsúlyosan megjelenik az Unió – ezzel némileg szembenálló – össz-gazdasági érdeke is.
Álláspontom szerint jól példázza ezt a kettősséget a (13) preambulum bekezdés:
„A természetes személyek egységes, uniós-szintű védelmének biztosítása, valamint a személyes adatok belső piacon való szabad áramlását akadályozó eltérések megelőzése érdekében rendelettel kell biztosítani a jogbiztonságot és az áttekinthetőséget valamennyi tagállam gazdasági szereplői részére… A belső piac megfelelő működése érdekében a személyes adatok Unión belüli szabad áramlását a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból nem szabad korlátozni vagy megtiltani.”

Igen, Európa korábbi gazdasági vezető erejét – némileg – elveszítve mára elsősorban, mint piac, mint a legnagyobb fogyasztó jelentkezik a világgazdaságban. Ha a döntéshozók változtatni akarnak a közelmúlt kedvezőtlen folyamatain, akkor nem hagyhatják, hogy a technológiai értelemben versenyképesebb USA, vagy a távol keleti országok akadálymentesen profitáljanak az európai piac adatvagyonából úgy, hogy közben erre az Unió nem igazán képes.

Természetesen vannak – sőt talán régebb óta vannak – EU kezdeményezések, politikai programok napirendend azért, hogy a kibertér társadalmát majd koherens módon védjék a tagállamok. Komoly fejlődés látható abban az irányban, hogy a tagállami büntetőjogi szankciók hasonló módon értelmezzék az informatikai környezetben elkövetett deliktumokat, és azokat a lehető legegységesebb módon szankcionálják.
Az eddigi legfontosabb eredmény éppen Budapesthez köthető. Az Európa Tanács 2001. november 23-án Budapesten fogadta el a Számítástechnikai Bűnözésről szóló Egyezményét. (Convention on cybercrime).
A későbbiekben igyekszem felvázolni az EU eddigi programjainak során elért eredményeket, hangsúlyozva álláspontom, hogy a személyes adatok büntetőjogi védelmének egységes szabályozása várat magára.

3 Az információs társadalomban megjelenő kriminogén tendenciák és a kapcsolódó nemzetközi bűntető jogforrások

3.1 A kezdeti regionális törekvések

Ahogy a korábbiakban igyekeztem hangsúlyozni, az információs társadalom kialakulására és fejlődésére – már a kezdetektől – jellemző volt, hogy csak minimális mértékben kötődik a nemzetállami határok létéhez. Talán csak az egy nemzethez, egy kultúrához tartozók alkotnak – valamilyen politikai, vagy társadalmi érdek megjelenése mentén – zártabb csoportokat. Ezektől az alkalmi közösségektől és bennük folyó – bizonyos témák mentén alakuló – digitális kommunikációtól eltekintve leszögezhetjük, hogy a világháló kialakulása – soha a történelem során még nem látott módon – változtatta meg világképünket, gazdasági társadalmi viszonyainkat.
A globalizációból fakadóan a számítógépes bűnözés könnyen vált – és válik egyre inkább – nemzetközivé. A vagyoni, erkölcsi és reputációs kárt okozó bűncselekmények elkövetésének közege valamint eszköze az országokat összekapcsoló nemzetközi hálózat, mely körülmény természetes következménye és egyben oka, hogy az ellene való harc is csak nemzetközi fellépéssel kecsegtethet sikerrel.

Az első figyelemreméltó kezdeményezés az OECD (Gazdasági Együttműködési és Fejlesztési Szervezet) által életre keltett ad hoc bizottság felállítása volt, amely 1983. és

1985. között az európai államok kiber térben elkövetett bűncselekményekkel kapcsolatban kialakult joggyakorlat kapcsán végzett felméréseit alapul véve, összegezve közzétette a büntetőjogi reformokat sürgető jelentését. A *Computer-Related Crime: Analysis of Legal Policy* (Számítógépes bűncselekmények: jogpolitikai elemzés) 1986-ban jelent meg.
Nem sokkal ezt követően az Európa Tanács – szakértő bizottságának jelentését alapul véve – 1989-ben kibocsátott egy ajánlást[10] a tagországok számára, mely egy minimális, illetve egy fakultatív listát tartalmazott a számítógépes környezetben elkövethető és szankcionálandó cselekményekről. Az ajánlás kihirdetett egy „minimum" és egy „fakultatív listát. A minimum listán szereplő deliktumok feltétlen büntetőjogi szankcionálását javasolja, míg a fakultatív listán szereplő cselekményekkel kapcsolatban a bűntető törvénybe történő illesztését megfontolásra ajánlja.

Az Egyesült Nemzetek Szervezete 1994-ben adta ki az első – tárgykörre vonatkozó – tanulmányát. A kézikönyv[11] hangsúlyozza, hogy a regionális szinten megtett lokális kezdeményezések nem elegendőek az informatikai bűnözés megállításához. A kiber-bűncselekmények hatóköre a nemzetközi telekommunikációs rendszerek egészét átfogja.

A világgazdaság főszereplői a G8 csoport tagjai 1995 – ben felállítottak egy olyan állandó jelleggel működő hálózatot a tagállamok között, amelynek célja a hatékony határokon átnyúló nyomozás elősegítése, s amelynek igénye – mint később látni fogjuk – a Cyber-crime Egyezményben is felmerül.

Az Európa Tanács a számítógépes bűncselekmények terjedésének hathatós visszaszorítása érdekében 1999. január 1-ei hatállyal egy négy évre szóló akciótervet fogadott el. A fókuszba – kiemelt hangsúllyal most először – az Internet biztonságos használata került.

Az ENSZ rendezésében, 2000 áprilisában megtartott Bécsi kongresszus záró dokumentuma hangsúlyozza az informatikai bűncselekmények – minden más

[10] Miniszteri Bizottság R (89) 9. számú Ajánlás a számítógépekkel kapcsolatos bűncselekményekről
[11] UN Manual on the Prevention and Control of Computer-Related Crime (ENSZ-tanulmány a számítógépes bűnözés megelőzéséről és szabályozásáról)

deliktumtól – elkülönített cselekménytípusként való kezelésének a fontosságát, szorgalmazza a fejlődő országok támogatását, illetve a nemzetközi, a nemzeti és a magánszektor által tett intézkedések, lépések elemzését, valamint jövőbeni összehangolásának igényét.

3.2 A kiber-bűnözés egyezmény (Convention on cybercrime)

Az egyezmény előkészítésének folyamatában az EU bizottság – a korábbi nemzetközi együttműködés eredményeire, ösztönző hatásaira tekintettel - határozatában felvázolta a szükséges feladatokat. Az 1997–ben megtartott prágai konferencián az igazságügyi miniszterek által elfogadott határozatban a Miniszteri Bizottság számára az a javaslat fogalmazódott meg, hogy támogassa a Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottság (CDPC) számítástechnikai bűnözéssel kapcsolatos tevékenységét. Ez a bizottság már akkor szorgalmazta a nemzeti büntető jogalkotás harmonizációját és a számítástechnikai bűncselekményekkel szembeni hatékony nyomozati eszközök bevezetését és koordinációját.

A 2000. június 8-9-i, XXIII. Konferencián elfogadott határozat hangsúlyozta a számítástechnikai bűnözés elleni harc sajátos követelményeit figyelembe vevő, gyors és hatékony nemzetközi együttműködés eszközrendszerének, annak mielőbbi megteremtésének szükségességét.

Egyezmény végleges tervezetét több tanulmány is megelőzte. Az egyik az ún. Sieber-féle jelentés. Ulrich Sieber – a Würzburgi Egyetem professzora – három fő követelményt támaszt a jogi szabályozással szemben egy – 1998-as, az Európai Bizottság számára készített – tanulmányában.[12]

1. *Nemzetköziség*: hiszen az információ szabad áramlásának nemzeti szabályozása és megszorítása hatástalan lenne nemzetközi együttműködés nélkül;
2. *Mindenre kiterjedő, átfogó szabályozás*: a felmerülő kérdések nem csak jogi eszközökkel történő orvoslása – mint a technológia, az oktatás és a gazdaság önszabályozása – gyakran sokkal hatásosabbak lehetnek, mint pusztán a büntetőjogi rendelkezések szigorítása;

[12] Prof. Ulrich Sieber: *Legal Aspects of Computer-Related Crime in the Information Society*, 1998. (A számítógépes bűncselekmények jogi aspektusai az információs társadalomban)

3. *A bevezetett megoldások specifikus jellege*: az információ egy olyan új, jól elhatárolható érték, melynek védelme megvalósíthatatlan a fizikai tárgyak védelmének analógiájára.

A leírt előzményeket követően, az Európa Tanács 2001-ben fogadta el a Számítástechnikai Bűnözésről Szóló Egyezményét (*Convention on Cyber-crime,* a későbbiekben: Cyber-crime Egyezményt). A „Budapesti Egyezmény néven emlegetett" dokumentumot 2001. november 23-án írta alá Budapesten mintegy harminc ország. Ez a nemzetközi paktum több lényeges szempontból meghaladja az elődjeit, mivel konkrét definíciókat ad a számítástechnikai rendszer egységeire vonatkozóan, az anyagi jogi, eljárásjogi és a nemzetközi jogi összefüggéseket együtt tárgyalja, ennek megfelelően magába építi az anyagi jogi kérdésekkel foglalkozó (89) 9. ET ajánlást, és az eljárásjogi kérdéseket tárgyaló (95) 13. ET ajánlást is. További – a napjainkig tartó hatással bíró – újdonsága az Egyezménynek, hogy abban a számítástechnikai rendszer és adatok elleni bűncselekmények (jogtalan belépés, jogtalan kifürkészés, adatok és rendszer elleni cselekmények, visszaélés számítástechnikai eszközzel, számítástechnikai csalás és hamisítás) mellett megjelentek a hálózatokon elkövethető „tartalom-bűncselekmények" is, úgymint a digitális gyermekpornográfia és a különböző szerzői jogi bűncselekmények. Igyekezett választ adni az olyan elterjedten jelentkező kérdésekre is, mint a jogellenes fájlcserélő rendszerek alkalmazása, a kéretlen kereskedelmi levelek (spam) küldözgetése, vagy az adathalászat (data phishing).[13]

Az Egyezmény elsődleges célja volt a – bűnügyi együttműködés eredményességéhez elengedhetetlenül szükséges – közös jogi alap megteremtése, hiszen az 1959-es strasbourgi, kölcsönös bűnügyi jogsegélyről szóló egyezmény szerint a jogsegély kérésének és nyújtásának az a feltétele, hogy az adott cselekmény az érintett országokban büntethető legyen.

3.3 Az Európai Unió számítógépes bűnözés elleni jogforrásai

Az Európai Unió működési feltételeit lefektető Lisszaboni Szerződés előtt az Unió jogalkotása szempontjából – a Maastrichti Szerződés által létrehozott és az Amszterdami Szerződés által módosított – harmadik pillérébe tartozott a tagállamok

[13] NAGY Z., A számítógépes környezetben elkövetett bűncselekmények kriminológiai aspektusairól. Gál I. & Nagy Z. : *Informatika és büntetőjog,* Pécs, 2006.

közötti bűnügyi együttműködés irányítása. A Bizottság több közleményben is hangsúlyozta a nemzeti határokon átnyúló fellépés szükségességét, kiemelve azt a körülményt, amely szerint az információs rendszerek elleni támadás komolyan veszélyezteti a biztonságos információs társadalom, valamint a jogszerű működésen alapuló térség megvalósítását, valamint, hogy az ellen az Európai Unió szintjén kell fellépni.

A Tanács a fentiekre figyelemmel rövid időn belül, 2005. február 24. napján megalkotta a még jelenleg is hatályos 2005/222/IB számú kerethatározatot, amely ha nem is szó szerint, de lényegét tekintve közel azonos megfogalmazással átvette a Cyber-crime Egyezmény számítástechnikai bűncselekményekre vonatkozó tényállásait. Mivel a kerethatározat uniós jogforrás, ezért – még ha nem is közvetlenül hatályos – kötelező az unió valamennyi tagállamára nézve, így máris hathatósabb lépés az informatikai bűncselekmények elleni nemzetközi együttműködésben, mint – a kiinduló dokumentumnak tekinthető – Cyber-crime Egyezmény.

A kerethatározat mellett ezekben az években sorra születtek az Unió egyéb más – a kiber biztonságot megteremteni szándékozó – egyéb jogforrásai.

A teljesség igénye nélkül:

- a 2001/413/IB. számú kerethatározat a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről;
- a 2002/58/EK elektronikus hírközlési adatvédelmi irányelv;
- a kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről szóló közlemény (COM{2006} 688); valamint – a talán legfontosabb –
- a 460/2004/EK rendelet az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (ENISA).

3.4 Az EU Kiber-védelmi stratégiája napjainkban

Egy 2015–ben készített felmérés szerint[14]: az EU lakosságának átlagosan 63 százaléka használta mindennapi szinten otthonában az internetet és 47 százaléka legalább egyszer észlelt már rendszerében káros szoftvert. Ennek ellenére az uniós lakosságnak átlagosan csak 31százaléka használt on-line felületeken különböző jelszavakat, 27 százaléka

[14] Special Eurobarometer 423
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

cseréli jelszavait rendszeresen és 61 százaléka telepített antivírus programot készülékére.
A tagállamok vállalati szektorára vonatkozó elemzés szerint 2015-ben az EU vállalatainak átlagosan csak 32 százaléka rendelkezett infokommunikációs biztonsági stratégiával.

A fenti veszélyforrásokat hathatósan elemző európai döntéshozók éppen ebben az időben készítették elő az Általános Adatvédelmi Rendelet tartalmi elemeit. Nyilván számos érv szólt amellett, hogy az Unió határain belül a személyes adatok áramlását „akadály- mentesítsék", és vélhetően ezt – a jelentős gazdasági előnyökkel kecsegtető és kötelező erejű – jogforrást nem akarták úgy megalkotni, hogy ne ez maradjon a figyelem középpontjában. Nagy valószínűséggel megállapítható, ez volt az oka, hogy az infokommunikációs hálózatok egységes védelmének kialakítása, a kiberbűnözés visszaszorítása egy másik – tagállami kötőerejét tekintve kisebb súlyú – uniós dokumentumban lett szabályozva. Az Unió Bizottsága 2013 februárjában elfogadta az Európai Unió kiberbiztonsági stratégiáját,[15] valamint létrehozta az EUROPOL szervezetén belül a Kiberbiztonsági központot (EUROPEAN CYBERCRIME CENTRE - EC3)[16].
Végül 2016 júliusában – a GDPR elfogadását követően – megszületett a hálózat- és információbiztonsági irányelv.[17]

Az irányelv az első átfogó uniós szabályozás, amely közösségi és nemzeti szinteken egyaránt meghatározza a kibervédelem kialakítandó intézményi rendszerét. A jogszabály azért is kiemelkedő fontosságú, mert bár – Bulgária, Görögország és Svédország kivételével – minden tagállam rendelkezik kibervédelmi stratégiával és adatbiztonsági-incidenskezelő szervezetekkel, ezek cél- és eszköz rendszere valamint azok hatékonysága korántsem egységes, ami közvetve az unió infokommunikációs hálózatait is veszélyezteti.

[15] http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu
[16] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[17] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE: a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Az irányelv többek között

- tagállami szinten előírja minimum egy – meghatározott feladatkörű – számítógép-biztonsági incidenskezelő csoport (Computer Security Incident Response Team, CSIRT) felállítását;
- szigorú biztonsági előírásokat és incidens-bejelentési kötelezettséget ír elő a társadalom és a gazdaság számára létfontosságú infrastruktúrák, illetve a digitális szolgáltatásokat nyújtó vállalatok számára; (*érdekes a párhuzam elemzése – melyre a dolgozat későbbi részében kitérek – a GDPR adatvédelmi incidenskezelési előírásaival*)
- közösségi szintű szervezetet hoz létre a tagállamok kompetens hatóságai és CSIRT - szervei közötti együttműködésre.

4 A védendő alkotmányos érdekek

4.1 Az információs társadalmat támadó bűncselekmények és a személyes adatok védelmét biztosító jogszabályok – védendő érdekek szerinti – közös halmaza

Ahogy azt az információs társadalom kialakulásáról és fejlődéséről írtakban igyekeztem bemutatni, ezen új társadalmi lét, a közösségek új megjelenési formája olyan új – eddig elképzelhetetlen – deliktumok sokaságát szülte, melyeknek csak töredéke az, amiről ebben az értekezésben írni szándékozom.
A dolgozat célja rávilágítani az igényre mely a személyes adatok büntetőjogi védelmének hatékonyabb érvényesülését, a privát szférát támadó bűnelkövetők egységes és hatékony szankcióval való fenyegetését várják el a jogalkotóktól.

A fentiekben részletesen írtam – a későbbiekben majd elemzésre kerülő – deliktumok kialakulását meghatározó történelmi, technológiai, társadalmi viszonyokról. Felvázoltam a – jelenség globalizált (a világ összes nemzetállamában megjelenő) jellegéből fakadó igényt az egységes szabályozásra. Amit – a jelenleg hatályos jogszabályi helyek elemzése előtt – meg kell tenni, az a védendő alkotmányos társadalmi érdek definiálása. Mi az a közös halmaz, melyet az adatvédelmi szabályok

(Info tv; GDPR) és a Btk. különös részi rendelkezései igyekeznek oltalmuk alá helyezni?

4.2 A „Right to privacy" evolúció egyik eredménye: az „információs önrendelkezési jog"

A magánélet védelmének a huszadik század végétől kezdve az egyik leghatékonyabb jogi eszköze a személyes adatok védelméhez való jog garantálása. Az adatvédelem igen fiatal jogi szakterület, az európai jogrendszerekben csak az elmúlt évtizedekben jelent meg. A háborítatlan magánélethez való, ennél mindenképpen tágabb jog általános elismerése a tizenkilencedik század végén az amerikai jogrendszer fejlődésének eredménye volt.[18]

Mint az angol-szász jogrend kitermelte jogi tárgy, igen nehéz más – nem angol nyelven törvénykező – államok jogi környezetébe a fogalomrendszert átültetni. Mégis az alábbiakban a privacy tartalmának a meghatározását kísérlem meg magyarul annak érdekében, hogy megfelelően definiálni lehessen a védelem tárgyát. Ennek részeként azt igyekszem majd bemutatni, hogy a privacy védelmének a magyar jogrendszerben is rendkívül összetett eszközrendszere van.

A privát szféra (privacy) védelmével kapcsolatos gondolkodás hagyományosan az ember – mint társadalomalkotó egyed – két jellemző életszférája közötti különbségtételből, nevezetesen a „magánlét" és az azon kívül álló világ elválasztásából indul ki.

A továbbiakban kísérletet teszek arra, hogy bemutassam a „privacy" a magyar jogban több mindent is lefed. Nem csak az adatvédelmi jog tárgya, hanem sok más egyéb jogágban – más és más jelentéstartalommal – tetten érhető. Az elemzés során a fogalomkört úgy darabolom részeire, hogy az egyes részekhez nevesített alkotmányos jogok beidézésével rendelek valamilyen tartalmat. Végül a definíció meghatározásának részeként tisztázni kívánom a tárgyalt fogalom viszonyát a személyes adatok védelméhez való joghoz, amivel a privacy-t igen gyakran azonosítják.

[18] Szabó Máté Dániel : *Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival* (Információs társadalom, 2005)

Álláspontom szerint a privacy nem más, mint az egyén joga ahhoz, hogy önmagáról, a saját személyéhez fűződő jogokról döntsön.
A magyar jogirodalomban, alkotmánybírósági gyakorlatban és a jogrendszer más területein is ismert jogról van tehát szó, az önrendelkezés szabadságáról, arról, hogy mindenki maga döntheti el, mi lesz a saját sorsa, mit tesz magával, ki és mit tehet vele, a testével és a rá vonatkozó adatokkal, ismeretekkel.
Az emberi lét, és az azzal kapcsolatos közgondolkodás történelmi fejlődésének köszönhetően a fizikai léttel kapcsolatos jogfogalmak már a Római jogban (vagy még korábban) tetten érhetőek. Az emberre vonatkozó, a létét leíró adatok, információk személyhez kötöttsége már sokkal mélyebb gondolkodást igényel.
Az, hogy az Ember nem árucikk (ugyan az ókorban csak a szabad polgárok joga volt) nagyon hamar jelen volt a közgondolkodásban. Az viszont, hogy az egyénről szóló ismeretek – azok mások számára hozzáférhetővé tétele – ugyancsak az egyén joga (és az sem szabad árucikk), még napjainkban is csak a társadalom – viszonylag – kis része értékeli helyesen. A személyiséggel rendelkező embernek fizikai és ismeretekben létező elemekből álló magánszférára van szüksége, ami felett maga rendelkezik.

Az előzőekből – álláspontom szerint – már levezethető, hogy az egyén fizikai léte mellett egyre hangsúlyosabbá válik az ismeretekben való léte is, és ezzel párhuzamosan a fizikai léte feletti önrendelkezési joga és információs önrendelkezési joga egybeolvad, ám ez utóbbi egyre hangsúlyosabbá válik. Az önrendelkezési jog részben az egyén arra vonatkozó döntési jogát jelenti, hogy hol húzza meg a határt önmaga és a külvilág között, azaz meddig engedi be a külvilágot a személyes szférájába.
Az egyén önrendelkezési joga, pontosabban annak mindkét általunk említett oldala, a fizikai és az információs önrendelkezési jog egyaránt számos nevesített alapvető jogban megjelenik. Ebben a körben – többek között – az élethez való jogot, a kínzás és a megalázó, embertelen bánásmód tilalmát, a személyes szabadság- és biztonság jogát, a mozgás szabadságát lehet felsorakoztatni.

A dolgozat témájának szempontjából az egyén információs önrendelkezéshez való joga, bír relevanciával, amellyel kapcsolatban azt állapíthatjuk meg, hogy az egyénnek a személyes adatai védelméhez fűződő jogánál sokkal többet foglal magában. Álláspontom szerint az információs önrendelkezés fűződő jog biztosítja az egyén számára, hogy ellenőrzést gyakoroljon mindenféle információátvitel, adatkezelés felett,

ami a jog alanya – vagyis az egyén – és a külvilág között történik, mind pozitív, mind pedig negatív értelemben. Ezek együttesen teszik ki az információs önrendelkezési jog valamennyi elemét.

A fentieket összegezve megállapítható, hogy a privacy (a privát szférához való jog) elemei közül a személyes adatok védelméhez fűződő jog, ami a számítógépes bűncselekmények jogi tárgya lehet. Értelemszerűen ezen lehetséges deliktumok közül is csak ott értelmezhető, ahol a bűncselekmény a személyes adatokat támadja, azokkal kíván visszaélni.

5 A hatályos magyar büntető anyagi jogi szabályozás

5.1 Az informatikai bűncselekmények rendszere

Alapul véve a korábbiakban elemzett technológiai, társadalmi viszonyokat: informatikai bűncselekményeknek nevezhetjük azon bűncselekményeket, amelyek elkövetésével – jellemzően – valamely adatot, vagy az adatkezelés, adatfeldolgozás folyamatát és az ezekhez fűződő társadalmi érdeket sért vagy veszélyeztet az elkövető.
A bűncselekmények jogi tárgyai alapján az informatikai bűncselekmények tovább csoportosíthatók, mivel a különböző védett társadalmi viszonyok különböző jogi, szűkebben különböző büntetőjogi szabályozást igényelnek. Ezért az informatikai bűncselekményekhez sorolhatjuk az

- adatvédelmi;
- a szerzői jogok (vagy azokhoz kapcsolódó egyéb jogok) megsértésének bűncselekményeit;
- a tiltott pornográf felvétellel visszaélést;
- és a számítástechnikai bűncselekményeket;
- Számítógéppel érintett bűncselekmények (computer-related crimes)

Jelen dolgozat keretében – értelem szerűen – a személyes adatok kezelésével kapcsolatban elkövethető, az adatok jogellenes megsemmisítésére, megváltoztatására

irányuló, valamint azok jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.[19]

5.2 Az adatvédelmi bűncselekmények

Ahogy az a fentiekben már több alkalommal igyekeztem hangsúlyozni, az egyre inkább – jellemzően – számítógéppel történő adatkezelés és adatfeldolgozás miatt az EU Általános Adatvédelmi Rendelete, valamint információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben leírtak szerinti, számítástechnikai feldolgozásra alkalmas formában megjelenő adat és az ahhoz kapcsolódó személyiségi jogok védelmében a büntetőjogi tényállások jelentik az egyik legkomolyabb szabályozási elemet az adatvédelem összetett rendszerében.

A magánszféra védelme informatikai jogi szempontból a személyes adatok védelmét jelenti, a cél azonban a személyes adat által leírt, tárgyiasult emberi személyiség szabadságának, méltóságának, pontosabban a magánszférának (privacy) védelme, nem pedig magának az adatnak a védelme. Fokozza a személyiség alávetettségét, hogy az informatikai eszközök segítségével könnyen, gyorsan előállítható olyan személyiségprofil, mellyel feltérképezhető az egyén teljes magánélete, így családi állapota, jelene, múltja, következtetni lehet terveire, jövőjére, sértve ezzel szabad akaratát, méltóságát, komoly visszaélésekre adva ezzel alapot.[20]

5.2.1 Személyes adattal visszaélés

Btk. 219. § (1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában[21] meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja,

vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

[19] Ld: GDPR 4. cikk Fogalommeghatározások, 12. pont *„adatvédelmi incidens”*

[20] GALÁNTAI Z., E-privacy olvasókönyv. Forrás: http://mek.oszk.hu/04100/04134/04134.pdf

[21] Btk. 219§ (1) bekezdés nyitó szövegrésze a 2017: CXLIV. törvény 60. § a) pontja szerint módosított szöveg

A bűncselekmény jogi tárgya: az érintett személyes adatai megismeréséhez és biztonságos kezeléséhez, őrzéséhez fűződő (privacy) jog.

A deliktum elkövetési tárgya: a személyes adat.

> A friss törvényi módosítás nyomán az új háttérjogszabály az EU Általános Adatvédelmi Rendelete. A személyes adat a Rendelet definíciójából fakadóan: *azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ;*
> Az azonosítható természetes személy fogalomkörét maga a Rendelet „nyitott módon" példálózó jelleggel fogalmazza meg: *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.*

Az alapeseti elkövetési magatartások:
a; a jogosulatlan, vagy a céltól eltérő adatkezelés;

> Az adatkezelés nem új keletű jogi fogalom már a korábbi adatvédelmi jogszabályok is definíciószerűen meghatározták, és így tesz a GDPR is.
>
> A Rendelet 4. cikk 2. pontja szerint „adatkezelés": a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.
> A jogosulatlan, vagy a céltól eltérő – jogellenes – adatkezelés értelmezéséhez figyelembe kell venni a Rendelet 6. cikkében felsorolt – az adatkezelés jogszerűségét meghatározó – jogalapokat. Amennyiben az adatkezelés jogalapja hiányzik az elkövetési magatartás alakszerű.

b; az adatok biztonságát szolgáló intézkedés elmulasztása.

> A Rendelet 5. cikk (A személyes adatok kezelésére vonatkozó elvek) (1) bek. f) pontja meghatározza az adatkezelés biztonságára vonatkozó elvárásokat: *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 („integritás és bizalmas jelleg”).*
> Az elvárt – kockázatarányos – technikai vagy szervezési intézkedések nem megfelelő alkalmazása, vagy negligálása alakszerű elkövetési magatartás.

<u>*Célhoz kötöttség, szándékosság*</u>: megvalósul a személyes adattal visszaélés, ha azt *haszonszerzési célból vagy jelentős érdeksérelmet okozva* követik el. Ezek hiányában – így a gondatlan elkövetési magatartás sem – a cselekmény nem büntetendő.

<u>*Minősített, kiegészítő tényállások:*</u>

(2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével az érintett hozzáféréshez való jogának gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

<u>*Elkövetési magatartás:*</u> a tájékoztatási kötelezettség szándékos negligálása, vagy az érintett hozzáférési jogának megtagadása.

<u>*Célhoz kötöttség, szándékosság*</u>: a (2) bekezdés szerinti magatartás büntetendő akkor is, ha az elkövetőnek ezzel nincs konkrét célja, de az érdekeltnek, vagy bárki másnak jelentős érdeksérelmet okoz. (Az érdeksérelem mértéke – mind más hasonló tényállások vonatkozásában is – bírói mérlegelés tárgya.)

Súlyosbító körülmények: A jogalkotói szándékból kitűnik, hogy a magyar büntetőjogi hagyományoknak megfelelően az elkövető súlyosabb büntetésre számíthat, ha a cselekményét erősebben védett szenzitív adatokra követi el.

> A különleges személyes adatok kezelése tekintetében a Rendelet új szabályozást alkalmaz. A 9. cikkben – főszabályként – megtiltja azok kezelését, aztán felsorolja a kivételeket.
> A rendelet értelmében különleges adatok: *a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.*
> A Nemzeti Adatvédelmi Hatóság (NAIH) Adatvédelmi Értelmező Szótára a bűnügyi adatra ezt a meghatározást adja: *bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.*

(3) A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra vagy bűnügyi személyes adatra követik el.

Bűntetté minősítő körülmény: Ha a bűncselekmény alanya közmegbízatásával összefüggésben birtokába került személyes adatokkal él vissza, azt a hatályos Btk. – a már kialakult gyakorlatnak megfelelően – súlyosabb büntetéssel fenyegeti.

(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.

A személyes adattal visszaélés bűncselekményének elemzésénél fontosnak tartom kiemelni, hogy a jogalkotó rendszertani megfontolásokból – a XXI. fejezetben – *az emberi méltóság és egyes alapvető jogok elleni bűncselekmények* között helyezte el. A

döntés összecseng mindazzal, amit fentebb boncolgattam, miszerint az – alkotmányos garanciák által is védett – önrendelkezési jog megsértése egyre inkább büntetőjogi kategóriává válik. A modern jogállamok az ilyen cselekményeket ma már jellemzően szabadságvesztés büntetéssel fenyegetik.

Felmerülhet a kérdés, hogy a következő bűntetetendő deliktum – melynek jogi tárgya, és elkövetési tárgya részben megegyezik a személyes adattal visszaélés kapcsán kifejtettekkel – vajon miért válik rendszertanilag annyira külön a hatályos Btk. – ban?

5.2.2 A tiltott adatszerzés

A hírszerzés – vagy kémkedés – visszanyúlik még az ókori társadalmak kialakulása előtti időkre. A mások titkainak kifürkészése a fennmaradásért folytatott folyamatos harc meghatározó elemévé vált.
Mások titkainak kifürkészése nem csak a személyes adatok jogosulatlan megszerzésére irányulhat. Az egyes társadalmak elkülönülésének kezdetén ezek jórészt katonai titkok voltak. Később a gazdasági fejlődés eredményeként megszülettek azok az előnyt, és értéket képviselő információk, melyek megvédése szellemi kimunkálójuk jelentős érdekévé vált. Az adatkör, melynek megszerzésére a kémkedési magatartás irányul így nem csak személyes adat lehet.

A hatályos Btk. a fenti szempontok helyes mérlegelésével a 422. § alatt szabályozott bűncselekményt – a fentiek fényében érthető okokból – a XLIII. fejezetben, nem az önrendelkezési jogok megsértései között helyezi el.
A rendszertani elhelyezés mindenképp figyelemre méltó. A védett jogi- és elkövetési tárgyak – többes jellegükből fakadóan – a Büntető Törvénykönyv más és más fejezetiben leírt bűncselekményekhez illeszthetők. A jogalkotó – figyelemmel az információs társadalom meghatározó szerepére – a legújabb szabályozásban az információs rendszer elleni deliktumokkal egy fejezetben definiálta a jogellenes adatszerzés elkövetési magatartásait.

Btk. XLIII fejezet: *Tiltott Adatszerzés és Az Információs Rendszer Elleni Bűncselekmények*

422 § Tiltott adatszerzés

(1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,

b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával titokban megfigyeli vagy rögzíti,

c) más postai küldeményét vagy egyéb zárt küldeményét titokban felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,

d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti,

e) információs rendszerben kezelt adatokat titokban kifürkész, és az észlelteket technikai eszközzel rögzíti,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(1a) Az (1) bekezdés szerint büntetendő, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiséget vagy területet, – a közösségi közlekedési eszköz kivételével – járművet, továbbá más használatában levő tárgyat titokban átkutat,

b) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiségben vagy területen, továbbá – a közösségi közlekedési eszköz kivételével – járművön történteket titokban technikai eszköz alkalmazásával megfigyeli vagy rögzíti.

A törvényi tényállás elemzését – talán – a személyes adattal való visszaélés vétségével történő összehasonlítással érdemes kezdeni. Azért is választom ezt kiinduló pontnak, mert a dolgozatom elején – többek között – azt is felvetettem, hogy mi az oka annak a szemérmességnek, ami miatt az adatokat sértő deliktumok felfedezését követően – tapasztalataim szerint nagyon sok esetben – az érintett vállalatok, vagy más társaságok nem akarnak a büntető feljelentés lehetőségével élni. De ha mégis megteszik ezt, gyakran keverik a két bűncselekményt.

Nézzük, melyek a lényegi különbségek!

A *visszaélés személyes adattal* vétség alanya – első olvasatra talán félreértelmezhető módon – csak a Rendeletben definiált *adatkezelő* lehet, aki ebben a minőségében kezel személyes adatot jogalap nélkül, vagy az eredeti – megfelelő jogalappal rendelkező – célhoz képest eltérő jogellenes módon.
A helyes értelmezéshez azonban figyelembe kell venni a törvényi tényállásban szereplő *„Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi…”* megfogalmazást, ami arra utal, hogy bárki elkövetheti a bűncselekményt. Az *„Aki”,* mint általános alany helyes értelmezéséhez figyelembe kell venni azt a körülményt is, hogyha valaki teljesen illegális módon – azaz jogalap nélkül – végez adatgyűjtést, automatikusan adatkezelővé válik. A tevékenysége törvénytelen, és – ha haszonszerzési célból, vagy jelentős érdeksérelmet okozva teszi ezt – büntetendő is.
Ezt az értelmezést támasztja alá a Kúria 1/2012. BJE számú (2012. október 29.) jogegységi határozata is.
A *tiltott adatszerzés* bűntett alanya – egyértelműen – bárki lehet. Nagyon extrém esetben elképzelhető olyan elkövetési magatartás, ahol az elkövető – egyes adatokra vonatkozóan jogos – adatkezelői státusszal rendelkezik, de ezzel nem érdemes foglalkozni. Az már lehet érdekes, hogy a kifürkészett adatok tárolása, továbbítása esetén a bűncselekmény alanya már adatkezelőnek minősül (még ha jogalap nélkül is) és így a visszaélés személyes adattal is vizsgálandó lenne, de – álláspontom szerint – ez esetben a jogellenes adatkezelés büntetlen eszköz cselekményként minősül.

A *tiltott adatszerzés* jogi tárgya szélesebb körű, mint a *személyes adattal visszaélés* esetén az információs önrendelkezéshez fűződő jog. Ez esetben több védendő jogi érdekről lehet még említést tenni: a szellemi alkotások védelme, vagy a tisztességes gazdasági verseny biztosítása.

A 422. § alatti elkövetési tárgyak köre, is meghaladja a pusztán személyes adatra fókuszáló 219 § esetén definiáltakat. A személyes adat mellett, itt találjuk a magántitkot, az üzleti- és gazdasági titkokat is. Ezek a titkok jellemzően a személyes adatok körén kívül eső információk.

A jogszabályi helyek esetén meghatározott célok is lényegesen eltérnek. Amíg a *személyes adattal visszaélés* esetén a haszonszerzés vagy az érdeksérelem okozása

minősíti a magatartást büntetendővé, addig a *tiltott adatszerzés* esetén nem több mint a jogosulatlan megismerése az információnak.

Az *elkövetési magatartások* mindkét bűncselekmény esetén – pontonként jól elkülönítve – precízen meghatározottak, és jól jellemzik a különbséget a két deliktum között.

Érdemes még – néhány gondolat erejéig – az elkövetés lehetséges helyszíneivel foglalkozni.
A közelmúltban több olyan – nagy média vihart szült – büntetőeljárás folyt, ahol az volt az eldöntendő – jogértelmezési – kérdés, hogy vajon a „más lakása vagy egyéb helyisége esetén" lehet-e büntetni azt, aki a titkokat nem egy (vagy több) természetes személy birtokában lévő ingatlanon (esetleg járműben), hanem valamely jogi személy által használt, birtokolt, vagy a közösség számára nyilvános helyen (járművön) követi el. Lényegében, ki minősül „másnak"? A vitának a személyes adatok kezelésével kapcsolatos 2017. évi CXCVII törvény szerinti Btk. módosítások vetettek véget. Azóta a 422. § (1a) bekezdése egyértelműen definiálja, hogy a magánszféra van a jogszabályi hely fókuszában.
Sokan – köztük én magam is – vitatják, hogy miért lehet az büntetlen, aki a munkahelyi irodámat kutatja át, míg a parkolóban hagyott autóm átkutatása már büntetendő. Ha az elérendő cél ugyanaz, ha az elkövetési magatartás ugyanaz, miért a különbségtétel? Álláspontom szerint nem szűnik meg a privátszférám a közösség számára nyitva álló helyeken sem.

A 422. § (2) bekezdésében leírt törvényi tényállás számomra kissé testidegen:
Az (1) bekezdés szerint büntetendő, aki fedett nyomozó, illetve titkos információgyűjtés folytatására vagy leplezett eszközök alkalmazására feljogosított szervvel titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.

Magának a bűntetté nyilvánított elkövetési magatartásnak sem látom visszatartó erejét. Nem hiszem, hogy a szervezett alvilág tagjai, majd azért nem akarják tudni, hogy folyik-e ellenük titkos nyomozás, mert az büntetendő.

A 422. § (4) bekezdésében felsorolt minősített esetek viszont szervesen illeszkednek az Büntető törvényt átfogó jogalkotói szándékba:
A büntetés egy évtől öt évig terjedő szabadságvesztés, ha az (1)–(3) bekezdésben meghatározott tiltott adatszerzést
a) hivatalos eljárás színlelésével,
b) üzletszerűen,
c) bűnszövetségben vagy
d) jelentős érdeksérelmet okozva
követik el.

Amiről még – mindenképp – érdemes néhány gondolatot papírra vetni, az a (3) bekezdésben leírt külön státuszú elkövetési magatartás:
(3) Az (1) bekezdés szerint büntetendő, aki az (1)–(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.

A tényállás egyfajta bűnsegédi magatartás „sui generis" önálló büntetendő deliktumkén történő szabályozása. Az elkövetési magatartás jogosulatlan adatkezelésnek is minősíthető a GDPR alapelveket figyelembe véve. Amennyiben a – felsoroltak közül – a személyes adat az, amelyre a bűncselekményt elkövetik, úgy – formailag – a személyes adattal visszaélés is megállapítható lenne. Ez esetben azonban a célzat különbözősége okán a súlyosabb bűncselekmény magába olvasztja a vétségi formát.

6 Összegzés és következtetések

6.1 A személyes adatokkal kapcsolatos hazai büntetőjogi szabályozás

Visszatekintve a magyar bűntető anyagi jogi szabályozás elmúlt harminc éves fejlődésére, leszögezhető, hogy a hazai jogalkotói szándék az információs társadalom kialakulásának kezdeteitől tetten érhető volt a személyes adatokhoz fűződő önrendelkezési jog – mint védendő alkotmányos érdek – büntetőjogi szabályozásában.

Az Országgyűlés az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményét (a továbbiakban: Egyezmény) a 2004. évi LXXIX. számú törvénnyel kihirdette. Az egyezmény aláírásakor vállaltak megfelelően – többek között – az alábbiakban felsorolt büntetendő magatartásokra új törvényi tényállásokkal egészítette ki a korábban hatályos Bűntető Törvénykönyvet. A későbbiekben pedig a törvény újra kodifikálásakor a vonatkozó tényállási elemeket – az információs társadalom fejlődésével összhangba hozva – a jogszabályi helyeket újra gondolta, rendszerezte, pontosította.

A személyes adatokkal kapcsolatos elkövetési magatartások a Cyber Crime egyezményben foglaltak – a 2004. évi LXXIX. számú törvényben kihirdetettek – szerint:

I. Fejezet (büntető anyagi jog)

I. Cím (számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények)

3. Cikk; <u>Jogosulatlan kifürkészés:</u>

Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai rendszeren belüli, az abból származó, illetőleg a rendszerbe irányuló számítástechnikai adatok nem nyilvános továbbítása során technikai eszközök felhasználásával történő jogosulatlan és szándékos kifürkészése, ideértve az ilyen számítástechnikai adatokat továbbító, a számítástechnikai rendszerből származó elektromágneses sugárzást. A Fél kikötheti, hogy a bűncselekményt tisztességtelen céllal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

4. Cikk; <u>Számítástechnikai adat megsértése:</u>

1. Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése.

2. A Fél fenntarthatja magának a jogot annak kikötésére, hogy az 1. bekezdésben meghatározott cselekmény eredményeként jelentős kár következzen be.

A leírtakból kitűnik, hogy az egyezmény – noha annak egészéből a teljes körűség szándéka kiolvasható – nem ad teljes körű kötelezést az aláíró országok jogalkotóinak a személyes adatokkal kapcsolatos büntetőjogi szabályozás megteremtésére.

Az Általános Adatvédelmi Rendelet megalkotása során – mint ahogy azt a dolgozatomban több alkalommal kifejtettem – egyértelmű volt a szándék az EU állampolgárok személyes adatainak az egységes kezelésére. Ez azonban – a szövegből több helyen kitűnve is – elsősorban az adatok szabad áramlásának a biztosítását célozta. Nem akarom kétségbe vonni az adatok védelmére vonatkozó jogalkotói szándékot, de azt állítom, hogy nem ez volt az elsődleges cél.
A személyes adatok büntetőjogi védelmével kapcsolatban a Rendelet a (149) számú preambulum bekezdésében mindössze a következőket írja:

A tagállamok megállapíthatják az e rendelet megsértése – így ideértve az e rendelet alapján és általa szabott korlátokon belül elfogadott nemzeti szabályok megsértése – esetén alkalmazandó büntetőjogi szankciókra vonatkozó szabályokat. E büntetőjogi szankciók lehetővé tehetik például az e rendelet megsértése révén szerzett vagyoni előny elvonását. Az ilyen tagállami szabályok megsértésére vonatkozó büntetőjogi szankciók, illetve közigazgatási szankciók kiszabása azonban nem eredményezheti a Bíróság értelmezése szerinti ne bis in idem elv megsértését.

A rendelet (152) preambulum bekezdése is – elsősorban – tagállami hatáskörben tartja a büntetőjogi szankcionálás lehetőségét.

Ha e rendelet nem harmonizálja a közigazgatási szankciókat, vagy ha egyéb esetekben ez szükséges – például e rendelet súlyos megsértése esetén –, a tagállamok hatékony, arányos és visszatartó erejű szankciókat előíró rendszert vezetnek be. E szankciók büntetőjogi vagy közigazgatási jellegét a tagállami jog határozza meg.

Ahogy azt a dolgozat során igyekeztem több oldalról is bemutatni az információs társadalom kialakulása két olyan lényeges körülményt hozott az emberiség életében,

ami a korábbi technológiai fejlettségi szinteken elképzelhetetlen volt. Az egyik az információk országhatárokon áthatoló – korábban elképzelhetetlen sebességű – áramlása, míg a másik a személyes adatok felhasználásában rejlő – globális – gazdasági érdek.

Az adatok hozzáférése érdekében globális harc folyik a gazdaság szereplői körében. De az a harc – mint a történelem során sok másik is – magával hozta a tisztességtelen küzdelmeket is. Megjelent – és a technológiai fejlődés roham tempójával párhuzamosan fejlődik – a kiberbűnözés is. A társadalom önvédelmi reflexként megszületett a „privacy" információs önrendelkezési jogként való igénye. Ezt az alapvető emberi jogot minden demokratikus jogalkotónak tiszteletben kell tartania. Ha a technológia fejlődése, az információs társadalom alakulása, és az azzal járó szervezett bűnözés globalizálódik, akkor az ellene folytatott harcot – a büntetőjog eszközeivel is – nemzetközi szinten kell a jövőben folytatni.

6.2 A személyes adatok jogszerű kezelését sértő bűncselekmény, mint adatvédelmi incidens

A GDPR (85). számú preambulum bekezdése – példálózó jelleggel sorolja fel – az adatvédelmi incidens bekövetkezése estén veszélyeztetett értékeket:

> *Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.*

A felsorolt jogsérelmek között nem egy olyan található, melyet csak bűncselekmény okozhat. Azt pedig mindegyikről kijelenthetjük, hogy jelentős kockázattal következhetnek be a személyes adatokra elkövetett bűncselekmények során.

A Rendelet 33. cikke hívja fel az adatkezelőt az észlelt adatvédelmi incidens esetén teendő jelentési kötelezettségére. A (3) bekezdés sorolja fel, hogy az illetékes felügyeleti hatóságot milyen tartalommal kell tájékoztatni az incidens lényeges elemei kapcsán:

> *a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;*
>
> *b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;*
>
> *c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;*
>
> *d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.*

Sem ebben a cikkben, sem másutt a Rendeletben nem találunk kötelezést, vagy utalást arra, hogy bűncselekmény észlelése esetén az adatvédelmi incidens kapcsán akár az adatkezelőnek, akár az illetékes felügyeleti hatóságnak feljelentési kötelezettsége lenne.

Nem szabad megfeledkezni arról, hogy a helyes jogalkotási gyakorlatnak társadalomformáló hatásuk is van. Tapasztaljuk, hogy az egyes adatkezelők azért nem akarnak büntetőeljárást kezdeményezni, mert annak – többek között a digitális médiának köszönhetően is – negatív reputációs hatása van. Ez természetesen érthető. Szemben áll azonban a titokban tartás mellett szóló érdek, és az adatalany önrendelkezési jogának sérülése. Így – ha kellő körültekintés mellet is, de – szükséges olyan jogszabályi környezetet teremteni, amit az információs társadalom széles körben támogat.