Adatvédelmi ismeretek

Bevezetés

A 21. századra eljutottunk a 4. ipari forradalom korszakába, amelyben egyre inkább megtapasztalhatjuk, hogy a számítógépre, az informatikai eszközökre minden területen szükségünk van, úgy az oktatásban, a gazdaságban, a kommunikációban, mint a pénzügyi életben. A bűnözés is áttevődött a fizikai térből a kibertérbe, mivel felismerték azt, hogy a felhasználók szívesen osztanak meg információkat, adatokat magukról, aminek következtében egyre több és egyre kevésbé észlelhető bűncselekményt lehet elkövetni.

A felhasználók által megadott adatok – személyes adatok, érzékeny adatok, különleges adatok stb. – védelme nemcsak magának a felhasználónak az érdeke, hanem az egyre szigorodó adatvédelmi és kiberbiztonsággal foglalkozó jogszabályoknak, nemzeti és nemzetközi szervezeteknek is, betartását, betartatását az államok, szervezetek követik figyelemmel és felügyelik is. A folyamatos kontrollnak köszönhetően a biztonságtudatosság, az adataink védelme mindinkább előtérbe került, és komolyabb szankciókkal, egyes esetekben komolyabb pénzbírsággal sújtották a cégeket, szervezeteket.

A kiberbűncselekmények és a kibertámadások egyik célja épp az adatok (akár a személyes adatok, a közérdekű adatok, egészségügyi adatok stb.) megszerzése, felhasználása, azok egyrészt anyagi, másrészt öncélú, akár bosszúból történő ellopása.

Az adatok életünk minden területén körbevesznek minket: az egészségügyben, a bűnüldözésben, a közlekedésben, az értékelőrendszerek működésében, a reklám- és marketingértékesítés területén.

Az egyre terjedő informatikai eszközök és a rajtuk futó alkalmazások használata során számos adat (fényképek, helyadatok, egészségügyi adatok, biometrikus adatok stb.) keletkezik, amelyeket annak használója generál, és amelyeket a különböző kényelmi szolgáltatások (applikációk) révén nyilvánossá tehet, vagy épp amelyekhez a hozzájárulását adja. Ezen kényelmi szolgáltatások legteljesebb mértékű kihasználásáért a szolgáltató vagy az „áruház” nem kér pénzt, csak hozzáférést az adatokhoz, fényképekhez. Ilyenkor a felhasználók hátradőlnek, és az ingyenesnek vélt szolgáltatást igyekeznek a legteljesebb mértékben kihasználni, és meggondolatlanul és elolvasás nélkül fogadják el az adatvédelmi beállításokat. Pedig nincs semmi sem ingyen. A szolgáltatóknak, a cégeknek az adatainkkal fizetünk.

https://doi.org/10.36250/01004_02

A következőkben az adat fogalmával, a fent is leírt adatfajtákkal, azok védelmével, törvényi és büntetőjogi hátterével fogunk foglalkozni.

Magyarországon több törvény is tartalmazza az adatokkal és az adatvédelemmel kapcsolatos szabályokat. A kiberbűncselekmények szempontjából kiemelt a 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról, a 2009. évi CLV. törvény a minősített adatok védelméről, a 2013. évi L. törvény az állami és önkormányzati szervek információbiztonságáról.

Az adat fogalma

Az adat fogalmát a 2013. évi L. törvény (Ibtv.)[26] értelmező rendelkezése tartalmazza. Ennek alapján az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

A számítástechnikában az adat fogalmára kétféle meghatározás létezik. Az egyik esetben az adat a számítógépes állományok meghatározott része (minden, ami nem program); vagy pedig mindaz, amivel a számítógépek működésük során foglalkoznak (ki- és bemeneti, tárolt, feldogozott, továbbított, megsemmisített adat).[27]

Az adatot mint fogalmat sokszor tévesen azonosítják vagy szinonimaként használják az információ fogalmával.

Az információ meghatározására többféle – tartalmában egymást átfedő – fogalmat használnak:

Az informatikai biztonság kézikönyve alapján:

> „bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg".[28]

[26] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[27] Muha Lajos: Fogalmak és definíciók. In Muha Lajos (szerk.): *Az informatikai biztonság kézikönyve.* Budapest, Verlag Dashöfer Szakkiadó, 2004.

[28] Vö. Muha (2004) i. m.

A *Rendészettudományi szaklexikon* szerint:

> „valamely személyre, ügyre vagy dologra vonatkozó olyan tájékoztatás, felvilágosítás, értesülés, hír, amely a címzettet választásra, döntésre, meghatározott cselekvésre, magatartásra, gondolkodásra készteti. Információ: értesülés, hír, üzenet, tájékoztatás, amely egyben az informatika alapfogalma."[29]

Az Ibtv. akként fogalmaz, hogy

> „információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti."

Az adatvédelem során a két legfontosabb jogszabályról mindenképpen szót ejtünk a fejezetben, a minősített adatokkal kapcsolatos szabályozást ugyanakkor a büntetőjogi alfejezetben csak említjük, hiszen arról részletesen fognak tanulni a bűnügyi szolgálati ismeretek és az adat- és titokvédelmi tantárgyak keretei között.

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete, a GDPR *(General Data Protection Regulation)* (a továbbiakban: Rendelet) az európai általános adatvédelmi rendelet, amely 2018. május 25-étől lépett életbe, és amelynek következtében az Infotv. is több módosításon ment keresztül annak érdekében, hogy a személyes adatok védelme a legteljesebb mértékben érvényre jusson.

A Rendelet célja:

> „A természetes személyek személyes adataik kezelésével összefüggő védelméhez kapcsolódó elvek és szabályok a természetes személyek állampolgárságától és lakóhelyétől függetlenül tiszteletben tartják e természetes személyek alapvető jogait és szabadságait, különösen, ami a személyes adataik védelméhez való jogukat illeti. Ez hozzájárul a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség, valamint a gazdasági unió megteremtéséhez, a gazdasági és társadalmi fejlődéshez, a belső piacon belüli gazdaságok erősödéséhez és konvergenciájához, valamint a természetes személyek jólétéhez."[30]

[29] Boda József (főszerk.): *Rendészettudományi szaklexikon.* Budapest, Ludovika Egyetemi Kiadó, 2019.

[30] Európai Parlament és a Tanács (EU) 2016/679. rendelete. Bevezető, 2. pont.

Az Infotv. 1. §-ában kötelezettségként határozza meg, hogy „a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon".

Az adatvédelem fogalma

Az adatvédelem *(data protection)* a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.[31]

A kiberbűncselekmények sokszor az informatikai rendszerek ellen irányulnak, az azokban tárolt adatok elleni támadásokban nyilvánulnak meg, amelyeket a szaknyelv *incidensnek* nevez. Az adatvédelmi incidens fogalmát az Infotv. szabályozza. Ennek alapján az az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.[32]

Az adatvédelem elvei

A GDPR 2. §-ában a következő alapelveket nevezi meg:

- célhoz kötöttség,
- jogszerűség, tisztességes eljárás, átláthatóság,
- adattakarékosság,
- pontosság,
- helyesbítéshez való jog,
- korlátozott tárolhatóság,
- integritás és bizalmas jelleg,
- elszámoltathatóság.

A *célhoz kötöttség* elve az Infotv.-ben található, és alkotmányossági alapelv is, amely alapján a személyes adat kizárólag meghatározott célból, a jog gyakorlása

[31] Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár* (é. n.).
[32] Infotv. 3. § 26. pont.

és kötelezettség teljesítése érdekében kezelhető. Az adatvédelmi munkacsoport 2013. április 2-ai állásfoglalása szerint a személyes adatok kezelése csak meghatározott, egyértelmű és törvényes célból történhet, illetve az adatok további kezelése nem végezhető e célokkal összeférhetetlen módon.

Az elv kimondja tehát, hogy személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját *egyéb eszközzel észszerű módon nem lehetséges elérni,* vagyis a cél elérése érdekében ténylegesen szükség van az adatok kezelésére. Az adatkezelőnek haladéktalanul törölni kell az érintett személyes adatait, amennyiben az adatkezelés célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához (ennek ágazatban való gyakorlati megvalósulása kérdéses). Az adatkezelés során csak a cél megvalósulásához szükséges mennyiségben és mértékben kezelhetők az adatok.

A személyes adatok gyűjtése, eredeti céljától eltérő, egyéb célból történő kezelése csak akkor megengedett, amennyiben *az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival,* amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését. Ez az elv megvalósul, ha ugyanannak az ellátott személynek a segítésben kitűzött célját próbáljuk elérni, s ehhez más-más formában, de folyamatosan használjuk a személyes adatait.

A *jogszerűség* követelménye értelmében annak érdekében, hogy a személyes adatok kezelése jogszerű legyen, annak az érintett hozzájárulásán kell alapulnia, vagy valamely egyéb jogszerű, jogszabály által megállapított – akár e rendeletben, akár más, az e rendeletben említettek szerinti uniós vagy tagállami jogban foglalt – alappal kell rendelkeznie, ideértve az adatkezelőre vonatkozó jogi kötelezettségeknek való megfelelés szükségességét, az érintett által kötött esetleges szerződés teljesítését, illetve az érintett által kért, a szerződéskötést megelőzően megteendő lépéseket.

A jogszerűség elve mellett az *átláthatóság elve* szerint a természetes személyek számára átláthatónak kell lennie annak, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, hogyan tekintenek bele, vagy milyen egyéb módon kezelik, valamint annak, hogy a személyes adatokat milyen mértékben kezelik, vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint az átláthatóság követelménye, hogy annak világosnak és egyszerű nyelvezettel fogalmazottnak kell lennie.

Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további

tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak *tisztességes és átlátható* kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról.

Az *adattakarékosság* elve szerint a kezelt adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek, és a kezelt adatok körét és a kezelés mértékét pedig a célhoz szükséges minimumra kell korlátozni.

A *pontosság* követelménye szerint 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.

A *helyesbítéshez való jog.* Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Az *integritás és a bizalmasság elve* azt jelenti, hogy a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. A személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. A személyes adatokat úgy kell kezelni, hogy azoknak a megfelelő szintű biztonsága és bizalmas kezelése során megakadályozzák a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

Az *elszámoltathatóság* elvének követelménye szerint az adatkezelő alakítsa ki azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek a rendeletből fakadó kötelezettségek teljesítéséhez szükségesek, másrészt képes legyen a megfelelés bemutatására.

Az adatok fajtái

Amikor adatokról beszélünk, a jobb megértés miatt célszerű megnevezni, hogy milyen típusú adatra gondolunk, hiszen az önmagában tág fogalom.

Az Európai Uniós Adatvédelmi Rendelet alapján személyes adatnak nevezünk minden olyan információt, amely valamely *azonosított vagy azonosítható élő személlyel* kapcsolatos. Mindazon információk, amelyek összegyűjtése

egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek.[33]

A *személyes adat* fogalmát az Infotv. csak egy mondattal határozza meg: az érintettre vonatkozó bármely információ.[34]

A személyes adat fogalmának használatakor szükséges megemlíteni azokat az eseteket, amikor bár maga a személy nincs pontosan megnevezve, mégis a róla gyűjtött adatokból személyére következtetni lehet, hasonlóan a *Ki vagyok én?* elnevezésű társasjátékhoz.

Az azonosításra alkalmatlanná tett, titkosított vagy *álnevesített* személyes adatok, amelyek felhasználhatók egy személy újraazonosítására, személyes adatnak minősülnek, és az általános adatvédelmi rendelet hatálya alá tartoznak.

Az olyan személyes adatok, amelyeket olyan módon *anonimizáltak,* amelynek következtében az érintett nem, vagy többé nem azonosítható, nem tekinthetők többé személyes adatnak. Az adatok valódi anonimizálásához az anonimizálásnak visszafordíthatatlannak kell lennie.

Az általános adatvédelmi rendelet a személyes adatokat *az adatok kezelése során használt technológiától függetlenül* védi – a jogszabály „technológiasemleges", és egyaránt vonatkozik az automatizált és manuális kezelésre, feltéve, hogy az adatokat kritériumok szerint rendszerezik (például betűrendben). Nem számít az sem, hogy az adatokat milyen módon tárolják: IT-rendszerben, videokamerás megfigyelőrendszerben vagy papíron; ezen esetek mindegyikére vonatkoznak az általános adatvédelmi rendelet személyes adatok védelmére vonatkozó követelményei.

Személyes adatoknak minősülnek:

- vezetéknév, családnév,
- lakcím,
- e-mail-cím, amely például annak használójára visszavezethető,
- személyazonosító igazolvány száma,
- helymeghatározásra vonatkozó adatok (GPS-adatok, közösségi oldalakon a tartózkodási hely megjelölése, a különböző alkalmazásokból gyűjtött helyadatok stb.),
- IP-cím,
- süti-azonosító (cookie),
- a telefon hirdetési azonosítója,

[33] GDPR ide vonatkozó számos rendelkezése.

[34] Infotv. Értelmező rendelkezések 3. § 2. pontja.

– a személy egyedi azonosítását lehetővé tevő, kórház vagy orvos által tárolt adatok.
– A *különleges adat* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
– *A genetikai adat* egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.
– *Biometrikus adat* az, ami egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.
– *Az egészségügyi adat* egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.
– *Bűnügyi személyes adatnak* minősül 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.

Az Európai Adatvédelmi Rendelet alapján a fent felsorolt típusokon kívül *különleges adatnak* minősül még:
– faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre utaló személyes adatok;
– szakszervezeti tagság;
– a nemi életre vagy a nemi irányultságra vonatkozó személyes adatok.

A személyes adat mellett sokszor lehet hallani a különböző adatigénylések kapcsán a közérdekű adat fogalmát. Közérdekű adatnak minősül az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó, vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Az utolsóként meghatározott adatfajta a közérdekből nyilvános adat, ami a közérdekű adat fogalma alá nem tartozó minden olyan adatot jelenti, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Az adatvédelem büntetőjogi háttere

Ahogy felületesen is, de érintettük, az Infotv., illetve az Európai Adatvédelmi Rendelet szabályainak megszegése esetén az azt sértő vállalkozások, szervezetek, weboldal-üzemeltetők ellen a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) bírságot szabhat ki. Ugyanakkor a pénzbírság nem mindig elegendő és lehetséges az adatok nem megfelelő felhasználásával, esetleg az azokkal való jogellenes visszaéléssel szemben. Lássuk a legfontosabb tényállásokat és azok vázlatos elemzését!

A személyes adattal visszaélés bűncselekménye

„Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában 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 […].”[35]

[35] Btk. 219. §.

Az elkövetési (tevékenységi) tárgy a személyes adat, valamint a különleges adat.

A bűncselekmény sértettje az a természetes személy, akire az adatok vonatkoznak.

Az elkövetési (tevékenységi) magatartásai:

Adatkezelés, vagyis az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége (például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, lekérdezése stb.) A büntetőjogi szabályozásnál ugyanazok az elvek érvényesülnek, amelyeket már fentebb is ismertettünk. Személyes adatot kezelni csak meghatározott célból, jog gyakorlása, illetve kötelezettség teljesítése érdekében lehet, míg a különleges adat esetén (fogalmát lásd fentebb) szükséges, hogy annak kezeléséhez az érintett hozzájáruljon. Fontos megjegyezni, hogy írásbeli hozzájárulás nélkül a faji eredetre, a nemzetiséghez való tartozásra, politikai véleményre, pártállásra, szexuális beállítottságra, vallásos vagy egyéb világnézeti meggyőződésre, érdekképviseleti tagságra vonatkozó személyes adat kezelése akkor lehetséges, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához szükséges, vagy ha azt az Alaptörvényben biztosított alapvető jog érvényesítése, bűncselekmény megelőzése, üldözése érdekében vagy nemzetbiztonsági, illetve honvédelmi érdekből törvény elrendeli.

A bűncselekmény tettese (aktív alanya) bárki lehet, aki személyes adatot kezel, feldolgoz, akinek törvényben írt kötelessége a személyes adatok biztonságáról történő gondoskodás. Ennek során köteles megtenni azokat a technikai és szervezési lépéseket, intézkedéseket, figyelemmel lennie azokra a szabályokra, amelyeket az Információs és önrendelkezési jogról szóló törvényben, valamint az adat- és titokvédelmi törvényben rögzítettek, így különösen az adat tárolására, hozzáférésére, megosztására, nyilvánosságra hozására, törlésére, úgyszintén az adat megváltoztatására, véletlen megsemmisülésére vagy sérülésére, a hozzáférhetetlenné tétele megakadályozására.

Az adatról az érintett kérelmére az adatkezelő köteles tájékoztatást adni. A kérelem vonatkozik a kezelt adatokra, a megbízott adatfeldolgozó által feldolgozott adatokra, azok forrására, az adatkezelés céljára, jogalapjára, időtartamára, az adatfeldolgozó nevére, címére, az adatkezeléssel összefüggő tevékenységre, az adattovábbítás jogalapjára és címzettjére.

Egyes esetekben az adatkezelő törvényi felhatalmazás alapján megtagadhatja a tájékoztatást. Ilyen eset az állam külső vagy belső biztonságának megőrzése, bűnüldözési, bűnfelderítési és bűnmegelőzési célból.

Az adatkezelő 30 napon belül köteles tájékoztatást adni közérthetően az adatkezelés megtagadásáról, különben bűncselekményt követ el.

A közérdekű adattal visszaélés

„Aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével
a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közlésére kötelezte, tájékoztatási kötelezettségének nem tesz eleget,
b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít, illetve
c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz […].”[36]

A bűncselekmény elkövetési (tevékenységi) tárgya: közérdekű adat. Fogalmát lásd fentebb.

A bűncselekmény elkövetési (tevékenységi) magatartásai:

A közérdekű adat eltitkolása az adatigénylő elől jogerős bírósági kötelezés előtt vagy azt követően.

Az állami vagy helyi önkormányzati feladatot vagy közfeladatot ellátó szervnek vagy személynek lehetővé kell tennie, hogy a szervezetre vonatkozó vagy az általuk kezelt adatot bárki megismerhesse, kivéve, ha az a minősített adat védelméről szóló törvényben meghatározottak szerint minősített adat. Kivételt képeznek még a megismerési kötelezettség alól a személyes adatoknál leírt esetek és a pénzügyi vagy devizapolitikai érdekek, a külügyi kapcsolatok, a nemzetközi szervezetekre vonatkozó kapcsolatok, a szellemi tulajdonhoz fűződő jog védelmének körébe eső adatok.

A *c)* pontban említett hozzáférhetetlenné tétel a közérdekű adat elrejtését és megsemmisítését jelenti.

[36] Btk. 220. §.

A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény

„(1) Aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné teszi, ha más bűncselekmény nem valósul meg, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.”[37]

A bűncselekmény elkövetési (tevékenységi) tárgya: a nemzeti adatvagyon védelméről szóló 2010. évi CLVII. törvény 1. § (1) bekezdése szerint a nemzeti adatvagyon a „közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége”.

A bűncselekmény elkövetési (tevékenységi) magatartása: a nemzeti adatvagyon körébe tartozó adat hozzáférhetetlenné tétele, amennyiben azt az adat kezelője számára teszi hozzáférhetetlenné.

Ugyanakkor – mivel ez egy szubszidiárius tényállás, így – annak elkövetése csak akkor valósul meg, ha az elkövetési magatartás nem valósít meg másik bűncselekményt. Azaz, amennyiben az elkövetése kifejezetten a kiberterrorizmus vagy kiberhadviselés jellegével történik meg, úgy abban az esetben az annál súlyosabban minősülő deliktum miatt indul eljárás.

Információs rendszer felhasználásával elkövetett csalás

A bűncselekmény szabályozásának történetére érdemes egy pillantást vetni. Azt az ellentmondást, hogy a hagyományos csalás esetében csak természetes személy megtévesztése tényállásszerű, ugyanakkor számítógépes környezetben a számítógép (egy számítástechnikai rendszer) működésébe történik csalárd célú beavatkozás, amit természetes személy legfeljebb utólag kontrollálhat, nehezen tudta feloldani a törvényhozás, ez problémát jelentett a jogalkalmazás számára is. Bár már az 1994. évi XVII. törvényben megszületett a számítógépes csalás tényállása, egyben szabályozva a csalás és a vírus kárt okozó büntetni rendeltségét, ezt követően az 1996. évi LII. törvényben, majd az 1999. évi

[37] Btk. 267. §.

CXX. törvényben, ezt követően a 2001. évi CXXI. törvényben módosították,[38] végül 2012-ben született meg ez a diszpozíció.

A szabályozás nehézsége például szolgálhat a jövőre vonatkozóan is, hiszen az új technológiák, az új visszaélések a jövőben is vethetnek fel problémákat a jogalkotás, illetve a jogalkalmazás szintjén. Erre fel is kell készülnünk.

A hatályos rendelkezés alapján „(1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz […].”[39]

A bűncselekmény elkövetési (tevékenységi) tárgya egyrészt az információs rendszer/maga a számítógépes adat, program, másrészt a hamis, a hamisított, illetve jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz.

A bűncselekmény elkövetési (tevékenységi) magatartásai: a törvényi tényállás elnevezésében jogtalan haszonszerzés végett a számítástechnikai rendszerbe elektronikus adat bevitele, az abban kezelt adat megváltoztatása, törlése vagy hozzáférhetetlenné tétele. A tényállás ezen része a haszonszerzés végett végrehajtott, célzatos cselekményeket (amelyek csak egyenes szándékkal valósíthatók meg) foglalja magában. A haszonszerzésre való törekvés. Az elektronikus adat bevitele történhet úgynevezett offline módban vagy akár online módban is. Más (valódi) személy kártyájának jogtalan felhasználását, azzal történő fizetést nevezik Card-not-present (CNP) csalásnak.

A deliktumnál hiányoznak a klasszikus értelemben vett tényállási elemek, azaz a tévedésbe ejtés vagy a tévedésben tartás, így sokszor a csalás tényállását – amennyiben azt például internetes hirdetési oldal segítségével követik el – sok esetben összetévesztik az elektronikus információs rendszer felhasználásával elkövetett csalással.

A sértett kárának bekövetkezését az információs rendszer jogtalan befolyásolása okozza. Azaz amennyiben valaki az információs rendszerbe bármilyen valótlan vagy a jogosultsága kereteit túllépve adatot bevisz, bármilyen adathordozóról (például CD, DVD, pendrive, külső tároló) feltölt, a már bevitt adat tartalmát megváltoztatja műszaki úton, a törléssel a rendszerben tárolt adatot megsemmisíti, úgy, hogy azt visszaállítani már nem lehet.

[38] Nagy Zoltán András: A számítástechnikai rendszer és adatok elleni új bűncselekmények. *Belügyi Szemle,* 40. (2002), 11–12. 27–41.

[39] Btk. 375. §.

A hozzáférhetetlenné tétel esetében akár ideiglenesen, akár véglegesen a jogosult gátolva van az adat elérhetőségében.

A jogosulatlanul többszörözés szintén bűncselekménynek számít.

A hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával történő károkozás, vagyis a készpénz-helyettesítő fizetési eszköz hamisítása.

„Készpénz-helyettesítő fizetési eszköz a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett."[40]

Jogosulatlannak minősül a fizetőeszköz megszerzése, ha azt az elkövető lopással (akár fizikailag veszi magához a bankkártyát, vagy pedig erre készített eszközzel megszerzi az azon szereplő adatokat) vagy erőszakkal, fenyegetéssel, megtévesztéssel, illetőleg más jogellenes módon veszi birtokba.

A bűncselekmény sértettje (passzív alanya) lehet természetes és jogi személy, akinél a kár keletkezik.

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…

[40] Btk. 459. § 19. pont.

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.

(2) 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.

(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.

(4) 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."[41]

A bűncselekmény elkövetési (tevékenységi) tárgya: személyes adat, magán-, gazdasági és üzleti titok.

A bűncselekmény elkövetési (tevékenységi) magatartása: minden olyan releváns cselekmény, amely a személyes adat és a fentebb említett titkok megismerésére, rögzítésére, gyűjtésére alkalmas (immateriális tényállás).

A deliktum tettese (aktív alanya) az a személy lehet, aki a személyes adat, a magántitok, a gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja, más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy azt rögzíti, más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti, elektronikus hírközlő hálózat – beleértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkészi, és az azon észlelteket technikai eszközzel rögzíti.

Az elkövetés helye mint esetleges tárgyi elem, kiemelést érdemel, ugyanakkor ez alapján nem vonható a törvényi tényállás alá az a magatartás, amikor munkahelyi irodákban, egyéb helyiségekben kerül sor az ott történtek technikai

[41] Btk. 422. §.

eszköz alkalmazásával való megfigyelésére vagy rögzítésére. De lege ferenda kívánatos volna az elkövetés helyének kiterjesztő értelmezése.

Információs rendszer vagy adat megsértése

„(1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) Aki
a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,
bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.
(3) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint.
[…]
(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”[42]

A tényállás jogi tárgyai: a számítástechnikai rendszerek integritása, biztonsága. Btk. 423. § (1) bekezdés *b)* pontjában az információs rendszerek biztonságos működése, azaz a jogosultság kereteinek megsértése, ezáltal a számítógépen vagy az információs rendszeren tárolt adat megváltoztatása (a rendszerhez jogosult személy olyan szándékos magatartása értendő ez alatt, amikor a magatartása az adat rosszindulatú megváltoztatására irányul).

A bűncselekmény elkövetési (tevékenységi) tárgyai: az információs rendszer (a számítógép vagy számítástechnikai rendszer) és az abban tárolt számítógépes programok és elektronikus adatok.

Az információs rendszer fogalmát a Btk. 459. § (1) bekezdés 15. pontja határozza meg: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

[42] Btk. 423. §.

Az informatikai hálózat esetében megkülönböztetünk belső hálózatot (intranet), vagy az internet részét képező hálózatot (például egy bank, biztosító hálózata), vagy a szerver feltalálási helyét a valós térben vagy a virtuális térben (mint például az úgynevezett *cloud* szerverek esetében). A hálózatok egy része publikus, azaz minden felhasználó által, céljának megfelelően használható, a hálózatok másik része azonban a nyilvánosság elől elzárt és csak a beavatottak által ismert jelszóval, egyéb azonosítóval használható.

A bűncselekmény elkövetési (tevékenységi) magatartásai:

1. A *jogosulatlan belépés,* amely megtörténhet egy más által jogszerűen birtokolt, használt számítástechnikai rendszerbe, úgy, mintha jogosult használó lenne (színlelés), vagy a számítástechnikai rendszeren keresztül egy védett hálózatba.

Szükséges az, hogy a számítógép vagy az informatikai hálózat, számítástechnikai hálózat bármilyen biztonsági és/vagy védelmi megoldásokkal aktívan védve legyen (vagyis a belépéskor minden egyes felhasználó legalább külön-külön felhasználónévvel és jelszóval, illetve egyéb azonosítóval tudjon csak jogszerűen belépni).

Jogosulatlan belépés, ha valaki ezen feltételek fennállása esetén, tehát az *aktív védelem ellenére,* az (aktív) védelemmel ellátott számítógépbe vagy számítástechnikai rendszerbe vagy védett hálózatba a jogosultsága kereteit túllépve

– a biztonsági rendszer hiányosságait kihasználva jogosulatlanul belép, vagy
– más felhasználó nevével és annak belépési kódjával lép be.

A bűncselekmény elkövetése szempontjából nem számít, hogy hogyan jut a tettes a belépéshez szükséges adatokhoz, azaz a megszerzésének módja lényegtelen. Lehetséges megtévesztéssel *(social engineeringgel),* kifürkészéssel, a felhasználó hanyagságának kihasználásával – a *clean desk* (tiszta asztal) szabályának megszegésével, a monitoron, a munkaasztalon vagy egyéb elérhető/látható helyen hagyott felhasználónév és jelszó otthagyása következtében –, illetve a világhálón is elérhető kódmegismerő program segítségével.

A belépés nem tekinthető jogosulatlannak, ha a számítástechnikai rendszer nincs ellátva semmilyen védelemmel (hálózati, illetve fizikai), vagy a védelem nem aktivált.

2. A *belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével* történő bennmaradás. Ebben az esetben a tettes a saját felhasználónevével és jelszóval lép be az adott információs rendszerbe, de a felhasználói jogosultságát

túllépve olyan műveleteket akar folytatni, amelyekre a jogosultsága már nem terjed ki.

Ennek megállapítása nem igényel különleges szakértelmet, hiszen az információs rendszerekhez történő hozzáférés előre meghatározott, így annak véletlenszerű elkövetése szinte kizárt.

Sem az információs rendszer elleni támadásokról szóló 2013/40/EU irányelvben, sem a Btk.-ban nem található annak pontos meghatározása, hogy mit is értenek a jogosultság kereteinek túllépésén, és milyen helyzetben rendeli büntetni a törvény, illetve milyen esetek képezhetik ez alól a kivételt. Így előfordulhat olyan vis major eset egy rendszerben, amikor a kárelhárítás érdekében történt jogosultság kereteinek túllépése is büntethető.