Magyar Rendészet 2025/1. 97–110.
DOI: 10.32577/MR.2025.1.6

RENDÉSZETTUDOMÁNY

Az adatokkal kapcsolatos visszaélések margójára

On the Margins of Data Abuse

GYARAKI Réka[1]

Az információs technológia és az ahhoz kapcsolódó eszközök folyamatos fejlődése magával hozza az adatrobbanást, amivel együtt nő annak veszélye, hogy minden egyes, a felhasználók által önként vagy kötelezően megadott adat egyre több veszélyforrást jelent.

A tanulmány bemutatja a személyes adatok, a különleges adatok, illetve az ezekhez nem tartozó, egyéb adatokkal összefüggő kiberbiztonsági és adatbiztonsági problémákat, valamint az elmúlt időszakban történt kiberbiztonsággal összefüggő incidenseken keresztül érzékelteti, hogy az azok kezelésével foglalkozó szervezetek kezében milyen lehetőségek vannak.

Kulcsszavak: adat, eKréta, adatbiztonság, rendvédelem, nemzetbiztonság

The continuous development of information technology and related devices brings with it the explosion of data, which increases the risk that each piece of data voluntarily or compulsorily provided by users represents an increasing source of danger.

The study presents personal data, special data, as well as cybersecurity and data security problems related to other data that do not belong to them, and through incidents related to cybersecurity that have occurred in the past period, it shows what opportunities are available to the organisations dealing with its management.

Keywords: data, eKréta, data security, law enforcement, national security

[1] Rendőr őrnagy, adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kiberbűnözés Elleni Tanszék, e-mail: Gyaraki.RekaEszter2@uni-nke.hu

A tanulmány célja és a kutatás módszere

A tanulmányban célul tűztem ki, hogy egy jogeseten keresztül mutatom be azt, hogy jelenleg milyen kötelezettségei vannak a személyes adatokat kezelő szervezeteknek és a védelmi oldalon milyen feladataik és lehetőségeik vannak egy informatikai támadás után az állami szereplőknek.

A kutatáshoz a kvalitatív módszert választottam, mivel igyekeztem a jelenleg rendelkezésre álló jogszabályi kereteket összegyűjtve választ adni arra, hogyan fordulhat az elő még a látszólag jól szabályozott „feladatok" rendszerében, hogy a felhasználók csak a hírekből értesülhetnek az olyan rendszerek elleni támadásokról, amelyben tárolják, kezelik az adataikat.

A kiberbiztonság napjainkban minden szinten kulcsfontosságú szerepet játszik, hiszen a digitális infrastruktúrák és informatikai rendszerek alapvetően határozzák meg a társadalmak működését. Az állami és magánszektor, valamint az oktatási intézmények mindegyike egyre inkább támaszkodik az informatikai rendszerekre az adminisztrációs feladatok elvégzésében, az adatkezelésben és a napi működés biztosításában. A Köznevelési Regisztrációs és Tanulmányi Alaprendszer (eKréta rendszer), a magyar oktatási rendszer digitális nyilvántartó rendszere, e feladatok elvégzésére szolgál, és alapvető szerepe van a diákok adatainak kezelésében, valamint az oktatás irányításában.

A tanulmány központi része a 2022-es eKréta rendszer elleni támadás elemzése, mivel ezen keresztül lehet a legjobban bemutatni a kiberbiztonsági hiányosságokat, valamint a szervezetek feladatait és az együttműködésük közötti hiányosságokat. A támadás rávilágít arra is, hogyan határozzák meg a jogszabályok, a felelősségi körök és az intézményi együttműködés struktúrája a kibertámadások kezelését. Emellett fontos szerepet kap a szervezeti kultúra és a kiberbiztonságra vonatkozó oktatás is, amelyek elősegíthetik a hatékony védekezést.

A tanulmány végső soron arra törekszik, hogy hozzájáruljon a kiberbiztonsági kultúra fejlesztéséhez, valamint a szervezetek közötti hatékony együttműködés elősegítéséhez, amely nélkül a kibertér védelme nem lehet teljes.

A kiberbűnözők különféle támadási vektorokat használhatnak a kibertámadások indításához, beleértve a rosszindulatú programokat, az adathalászat jellegű támadásokat, a zsarolóprogramokat és például a Man-in-the-Middle[2] jellegű támadásokat. E támadások mindegyikét egy szervezet információs rendszerének eredendő és fennmaradó kockázatai teszik lehetővé.

A szervezetek informatikai rendszerei bizonyos eredendő kockázatokkal rendelkeznek, azaz minden rendszernek vannak sebezhetőségei, például gyenge jelszavak, elavult szoftverek vagy nem megfelelő biztonsági intézkedések.

A fennmaradó kockázatok alatt pedig azokat a veszélyeket értjük, amelyek még a védekezési intézkedések bevezetése után is megmaradnak. Tehát például hiába alkalmaz

[2] Man-in-the-Middle támadás: vagyis közbeékelődéses támadás egy olyan, a hálózati lehallgatáshoz sokban hasonlító kibertámadás, amely során a támadó az elektronikus hírközlési hálózaton továbbított adat küldője és fogadója közé „ékelődik be", és a továbbított információt, adatot megváltoztatja. A cél, hogy a fogadó személyt megtévessze és tőle érzékeny információkat szerezzen meg (pl. jelszót), amellyel utána visszaélhet.

egy szervezet tűzfalat, vírusirtót és más biztonsági megoldásokat, ha a felhasználók nem elég körültekintők, vagy a támadók új módszereket dolgoznak ki.

A kiberbűnözők célja az információs rendszer elleni támadások során lehet:

- pénzszerzés;
- adatlopás, amikor szervezetektől pénzügyi vagy üzleti titkokat próbálnak ellopni, ezzel manipulálva akár egy adott ország gazdasági helyzetét;
- politikai vagy ideológiai célok, befolyásolás;
- információszerzés, a vállalatok, kormányzati szervek vagy egyéb nagy szervezetek elleni támadások során a versenyelőny biztosítása érdekében, például új technológia vagy üzleti titok megismerése útján;
- tudományos és kutatási adatok;
- kritikus szervezetek infrastruktúrái (kommunikációs vagy más, alapellátást biztosító szervezetek) elleni támadások.

A kiberfenyegetések a rosszindulatú szoftverek, például rosszindulatú programok vagy zsarolóprogramok (például a WannaCry) kisvállalkozások elleni telepítésétől a kritikus infrastruktúrák, például a helyi önkormányzatok vagy kormányzati szervek ellen is irányulhatnak. A kibertámadások egyik gyakori melléktermé ke az adatszivárgás, amikor (személyes) adatok vagy más érzékeny információk kerülnek illetéktelenekhez vagy nyilvánosságra. A személyes adatok kezelésének biztonsága, és ezért annak kiberbiztonsága is az adatvédelem sarokköve.[3]

A kibertámadások során az elkövetők leginkább személyes, pénzügyi adatok vagy üzleti-ipari titkok[4] (know-how, szabadalmi titkok, szerződések stb.) megszerzését tűzik ki célként.

Egy eset vagy több?

Az elmúlt időszakban jelentős növekedés figyelhető meg az adatvédelmi és kiberbiztonsági incidensek számában, annak ellenére, hogy az adatok védelmét, valamint az információs rendszerek és az azokban tárolt elektronikus adatok biztonságát átfogó jogszabályi keretrendszer szabályozza.

Ugyanakkor például egy zsarolóvírus-támadás vagy ransomware esetén, amennyiben az olyan szervezetet érint, amelyik személyes adatot kezel és a támadás vagy fenyegetés során a személyes adatok biztonsága sérül, és azok arra jogosulatlan személyhez vagy személyekhez kerülnek, úgy a többi szervezetet is értesíteni kell, továbbá azokat a személyeket is, akiknek személyes adatait megszerezték. Ennek az értesítési „kötelezettségnek" a hiányosságait mutatom be egy jogeseten keresztül.

Az általános és középiskolákban kötelezően használt, hétköznapokban „eKrétának" nevezett rendszerrel (Köznevelési Regisztrációs és Tanulmányi Alaprendszer) összefüggésben történt adatvédelmi incidens során a tanulók személyes adatai sérültek, ami miatt

[3] Az Európai Parlament és a Tanács (EU, Euratom) 2023/2841 rendelete.

[4] European Commission: Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs 2018.

a rendszert üzemeltető céget 110 millió forintra bírságolta meg a Nemzeti Adatvédelmi és Információszabadság Hatóság (röviden: NAIH).

Az adott eset 2022 novemberében jutott a hatóságok tudomására, amikor a *Telex* hírportálnak küldött üzenetben a támadó(k) nyilvánosságra hozták azt, hogy adathalász támadást hajtottak végre, amelyben az egyik munkavállaló jelszavait megszerezték (az a munkavállaló vált áldozattá, akinek mindenhez volt hozzáférése a rendszeren belül), és annak birtokában sikeresen hozzáfértek a cég más adatbázisaihoz és a forráskódokhoz, illetve a fejlesztők belső kommunikációjához is. Amikor az esetet az adott munkavállaló észlelte, csak napokkal később értesítette a munkahelyét, ahol lecserélték az adathalász-támadás áldozatául esett munkavállaló gépét, törölték a belépési azonosítóit, jogosultságait, majd a munkavállaló új számítógépet és új jelszavakat kapott, vagyis nem tették meg az ilyenkor szükséges intézkedéseket.[5] Sem a NAIH felé nem jelezték az esetet a személyes adatok megsértése miatt (adatvédelmi incidens), sem a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet felé nem történt bejelentés (kibervédelmi incidens miatt), valamint elmulasztották, hogy a rendőrségen bűncselekmény elkövetése miatt feljelentést tegyenek.

A támadás súlyossága és annak következményei az oktatási szektor kiberbiztonságának érettségével és felkészültségével kapcsolatban is komoly kérdéseket vetettek fel, mindemellett felhívták arra a figyelmet, hogy az oktatási rendszerben lévő adatok is célpontjai lehetnek rosszindulatú tevékenységeknek. A támadást követően számos elemzés és vizsgálat indult azért, hogy feltárják a hiba okait, és megoldásokat dolgozzanak ki a jövőbeni hasonló események megelőzésére.

Az eset nyilvánosságra kerülése után a NAIH 110 millió forint bírság megfizetésére kötelezte az e-Kréta Informatikai Fejlesztő Zrt.-t. A Hatóság az 1245-29-2023. számú határozatában[6] részletesen kiemelte a bírság indoklását, amely szerint a cég a GDPR „32. cikk (1) bekezdés b) pontjában, valamint a 32. cikk (2) bekezdésében foglalt kötelezettségének azzal, hogy az informatikai fejlesztői környezetének adatbiztonsági beállításai során nem vette kellőképpen figyelembe az adatkezelésből eredő olyan kockázatokat, amelyek a személyes adatok jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek, és emiatt a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét nem garantálta.” Megállapította továbbá, hogy „(...) nem tett eleget az általános adatvédelmi rendelet 33. cikk (2) bekezdésének azzal, hogy az adatvédelmi incidenst nem jelentette be indokolatlan késedelem nélkül az adatkezelőknek.”[7]

[5] Pilling 2024.
[6] NAIH 4667-10/2022 sz. határozat.
[7] NAIH 4667-10/2022. sz. határozat

Incidensek a kibertérben

Magyarország az új kiberbiztonsági törvénnyel[8] a NIS2 irányelvvel összhangban igyekszik megteremteni a különböző állami és nem állami, a törvényben meghatározott szervezetekre vonatkozóan a kiberbiztonságot, úgy, hogy feladatokat és kötelezettségeket állapít meg.

A tanulmányban feldolgozott eset (is) ugyanakkor jól demonstrálja azt, hogy a kibercselekmények kategorizálása vagy megítélése nem annyira egyszerű, és a jelenlegi szabályozásokkal sem lehet hatásosabban kezelni, különösen nem a felhasználóknak.

Az adatvédelem fogalmát a NAIH a következőképpen határozza meg: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.[9]

Az adatok védelme ugyanakkor nemcsak a felhasználók, hanem az adatkezelők szakszerű feladata és érdeke is, hiszen például a nemzeti adatvagyon birtokosaként fokozott polgárjogi felelősséggel is tartozik azok védelméért, míg a nem nemzeti adatvagyon körébe tartozó adatok esetében üzleti érdek fűződik a védelem megfelelő megteremtéséhez.[10]

A biztonság fogalma szubjektív érzet, amely a *Magyar értelmező kéziszótár* egyik meghatározása szerint *veszélyektől vagy bántódástól mentes (zavartalan) állapot*.[11] azaz az adatok biztonsága tekintetében a kezelt adatok veszélyektől és bántódástól mentes állapota (ez viszont már nem lehet véleményem szerint szubjektív érzés).

Az Európai Unió általános adatvédelmi rendeletének (GDPR)[12] 2. szakasza az Adatbiztonság címet viseli, amit sem az adatvédelmi rendelet, sem más nemzetközi vagy hazai jogszabály nem határoz meg pontosan, jelentése a GDPR 32. cikkben „Az adatkezelés biztonsága" alatt keresendő. A NAIH adatvédelmi szótára szerint: az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.[13]

Az adatbiztonságnak – hasonlóan az információbiztonsághoz – alapelveknek kell megfelelnie, úgymint a sértetlenség, bizalmasság és rendelkezésre állás, amelyek a fent említett esetekben sérültek.[14]

Az adatkezelőknek és adatfeldolgozóknak elsőként képesnek kell lenniük felismerni az adatvédelmi incidenseket. Az általános adatvédelmi rendelet (GDPR) 4. cikkének 12. pontja szerint az „adatvédelmi incidens olyan biztonsági sérülés, amely személyes adatok – akár továbbított, tárolt vagy más módon kezelt adatok – véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan közlését vagy illetéktelen hozzáférését eredményezi".

Az Európai Parlament és a Tanács 95/46/EK irányelvének 29. cikke alapján létrejött, és a személyesadat-feldolgozás vonatkozásában az egyének védelmével foglalkozó

[8] 2024. évi LXIX. törvény.
[9] Lásd: https://www.naih.hu/adatvedelmi-szotar
[10] Péterfalvi 2012.
[11] O. Nagy – Juhász – Szőke 1985.
[12] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet).
[13] Lásd: https://www.naih.hu/adatvedelmi-szotar
[14] A Kréta rendszerrel kapcsolatos incidens esetében egyébként más hatóságnak, így a KR Nemzeti Nyomozó Irodának, valamint az NBSZ NKI-nek is feladata volt.

munkacsoport[15] személyes adatok megsértésével kapcsolatos 03/2014. számú véleménye és a 29. cikk szerinti munkacsoport WP 250. számú iránymutatása alapján az adatvédelmi incidensek három fő kategóriába sorolhatók:

- titoksértés: amikor személyes adatok jogosulatlanul vagy véletlenül kerülnek nyilvánosságra, illetve illetéktelenek férnek hozzá;
- sértetlenségi adatsértés: amikor személyes adatok illetéktelen vagy véletlen módosítása történik;
- hozzáférhetőségi adatsértés: amikor a személyes adatok véletlen vagy jogosulatlan módon elvesznek, illetve megsemmisülnek.

Az ilyen incidensek súlyos következményekkel járhatnak az érintettek számára, beleértve fizikai, vagyoni és nem vagyoni károkat. A GDPR szerint ezek a károk többek között magukban foglalhatják az érintettek adatai feletti ellenőrzés elvesztését, jogaik korlátozását, hátrányos megkülönböztetést, személyazonosság-lopást vagy azzal való visszaélést, pénzügyi veszteséget, az álnevesítés jogosulatlan visszafejtését, a jó hírnév sérülését, valamint a szakmai titoktartási kötelezettség alá eső adatok bizalmasságának megsértését. Emellett az érintettek számára jelentős gazdasági vagy társadalmi hátrányokat is okozhatnak.

Az adatkezelő egyik legfontosabb feladata az ilyen kockázatok felmérése, valamint azok kezelésére megfelelő technikai és szervezési intézkedések bevezetése.[16]

A személyes adat és szabályozása

A személyes adattal kapcsolatban elsődlegesen a GDPR, vagyis az EU adatvédelmi rendelete jut az eszünkbe, de annak büntetőjogi védelme, vagyis a személyes adattal visszaélés törvényi tényállása (Btk. 219. §)[17] kevésbé.

A személyes adat fogalmát a GDPR alapján a következőképpen egyszerűsíthetjük: „azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható."[18]

A személyes adatok védelméhez fűződő jog mindenkit megillet. Az Alkotmánybíróság 15/1991. (IV. 13.) számú határozatában az adatvédelemhez való jogot – annak pozitív oldalát is figyelembe véve – információs önrendelkezési jogként határozta meg, az alkotmány emberi méltóságra vonatkozó rendelkezéseiből. A jelenleg hatályos Alaptörvény a VI. cikk (2) bekezdésében nevesíti a személyes adatok védelméhez fűződő alapvető jogot.

A személyes adatoknak egy másik csoportja a különleges személyes adatok, amelyek egy adott személy vagy személyek különleges tulajdonságaira utalnak, vagyis az adatoknak

[15] A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv 29. cikke alapján.
[16] EDPB 01/2021. számú iránymutatás.
[17] 2012. évi C. törvény.
[18] GDPR 4. cikk 1. pontja.

speciális fajtája, sokszor használják erre az „érzékeny adatok" kifejezést. *Különleges adatok azok, amelyek az ember faji eredetére, a nemzetiségére, a politikai véleményére vagy pártállására, a vallásos vagy más világnézeti meggyőződésére, a szexuális életére vonatkoznak, ahogy ide tartoznak az egészségi állapothoz vagy a káros szenvedélyhez kapcsolódó adatok is.*[19]

Az adatokkal kapcsolatos büntetőjogi szabályozás

Az információs rendszerben tárolt adatokkal kapcsolatban a magyar jogalkotók egyik kiemelt feladata, hogy büntetőjogi szabályozás keretében olyan eszközöket biztosítsanak, amelyek hatékonyan védik az információs rendszerek integritását, ugyanakkor megfeleljenek a jogbiztonság követelményének. Az információs rendszerben tárolt adatok ellen elkövetett, az információs rendszer vagy adat megsértése bűncselekményének hazai szabályozásával összefüggésben az egyik legfontosabb uniós szabályozás az információs rendszerek elleni támadásokról szóló irányelv,[20] amely rögzítette, hogy az EU tagállamainak szankciókat kell megállapítani az információs rendszerek elleni támadások esetére, amely szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.

Ez az irányelv meghatározza az információs rendszer fogalmát, ami szerint minden olyan eszköz, illetve összekapcsolt vagy kapcsolódó eszközökből álló eszközcsoport, amelyek közül egy vagy több valamely program alapján automatikus adatfeldolgozást hajt végre a számítógépes adatokon, valamint működése, használata, védelme és karbantartása céljából az ezen eszköz vagy eszközcsoport által tárolt, feldolgozott, helyreállított vagy továbbított számítógépes adatokon.[21]

A Btk. értelmező rendelkezése szerint információs rendszernek minősül az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.[22]

A hazai büntetőjogi szabályozás foglalkozik a személyes adatok megsértésének büntetőjogi tényállásával is, hiszen az információs társadalom korában az kiemelt jelentőségűvé vált, mivel az adatvagyonnak nemcsak gazdasági értéke van, hanem a személyhez fűződő jogok és az Alaptörvényben lefektetett szabadságjogok alapját is képezi.

Az egyik alapvető büntetőjogi szabályozásunk a Btk. 219. §-a, a személyes adattal visszaélés, amelynek tartalmát a GDPR adja meg, amit annyival egészíti ki, hogy szükséges tényállási elemként határozza meg, hogy az elkövetés haszonszerzési céllal vagy az érdeksérelem okozásával történt meg. Ennek a szabályozásnak az egyik legnagyobb hibája, hogy az érdeksérelem okozása a bírói gyakorlat szerint az, ha csorbát szenved a sértett szakmai elismertsége vagy erkölcsi megbecsültsége. Az „érdeksérelem" mint tényállási elem bizonyítása a büntetőjogban objektív kategória, vagyis nem a sértett szubjektív érzése, megélése a deliktum tárgya, hanem például csorbát szenved a sértett szakmai elismertsége vagy erkölcsi megbecsültsége, vagyoni hátrány elszenvedése, vagy amennyiben a sértett

[19] 2011. évi CXII. törvény 3. § (3) bekezdés.
[20] Az Európai Parlament és a Tanács 2013/40/EU irányelve.
[21] Az Európai Parlament és a Tanács 2013/40/EU irányelve.
[22] 2012. évi C. törvény.

családi kapcsolataiban következik be hátrányos változás.[23] A tényállás megvalósulásakor ugyanakkor – figyelembe véve a GDPR elég szigorú szabályozását – a büntetési tétel, tekintve, hogy vétségként kezeli a jogalkotó, csupán egy évig terjedő szabadságvesztés, aminek egyik indoka lehet, ahogy Péterfalvi Attila is rámutatott, a jogalkotó csak a kirívó, így a különleges személyes adatra, illetve hivatalos személyként történő elkövetést kívánja szankcionálni, két év büntetési tétellel.[24]

A személyes adattal visszaélés mellett a Btk. 423. §-a szankcionálja az információs rendszer és adat megsértését is, amely bűncselekmény során az elkövetők jogosulatlan belépéssel bejutnak az információs rendszerbe illetéktelenül (angol kifejezéssel hacking), azaz a rendszer védelmét és biztonságát szolgáló intézkedést megsértik vagy kijátsszák, a jogosultság kereteit túllépik, illetve azzal ellentétesen a rendszerben *bennmaradnak*.

A bűncselekmény jogi tárgya az információs rendszerek megfelelő működéséhez és a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint titokban maradásához fűződő érdek.[25] A jogosulatlan belépés objektíve akkor valósulhat meg, ha az adott rendszer eleve védett a jogosulatlan használattól, felhasználói azonosító és jelszó, ujjlenyomat stb. alkalmazásával, tehát egy eleve nyílt hálózati rendszer nem lehet jogi tárgya a bűncselekménynek.[26]

Ugyanúgy büntetendő, ha az elkövető ugyan jogosult a rendszerbe való belépésre, de annak kereteit túllépi. Így például olyan esetekben, ha valaki a rendszert csak hivatali célra, vagy azt csak munkaidőben használhatja, s ezzel a jogosultságot megsértve cselekszik.

A tényállás (2) bekezdésének *a)* pontja szerinti alakzat, az információs rendszer működésének jogosulatlan akadályozását, megbénítását eredményezi. Ennek *konkrét elkövetési magatartásai* lehetnek az adat bevitele, továbbítása, törlése, illetve egyéb más műveletek végzése is. Az adatbevitel történhet bebillentyűzéssel vagy másolással, weboldalról való letöltéssel. Az elkövetési magatartások jogosulatlansága azt jelenti, hogy azokra nincs az elkövetőnek felhatalmazása. Az adatvisszaélés második fordulatának *eredménye* az akadályozás, ami akkor valósul meg, ha a cselekmény a számítástechnikai rendszer működését zavarja, függetlenül annak tartamától és mértékétől.

Hazai szervezetek fellépése a kibertérrel kapcsolatos jogsértéseknél

Az e-Kréta-ügy nagyon jó példája volt tehát annak, hogy bemutassa azt, hogy Magyarországon számos szervezet feladata a kibertérből érkező támadások és fenyegetések kezelése, kivédése és az állampolgárok vagy hazai szervezetek tudatosítása, felügyelete, ugyanakkor azt nem lehet kijelenteni, hogy csak e szervezetek fellépésén múlik a kibertér védelme, hiszen az adatkezelőkre vonatkozó szabályok a jogszabályokban tisztán vannak lefektetve,

[23] Kúria 1/2012 BJE határozata.
[24] Eszteri–Péterfalvi 2017.
[25] Karsai 2013.
[26] Karsai 2013.

ugyanakkor az azok betartására vonatkozó szankcióknak lehet, hogy nincsen megfelelő visszatartó erejük.

Az utolsó lépésben sorra veszem azokat a hatóságokat, amelyek felé az adatok elleni támadások esetében az érintett szervezeteknek bejelentési kötelezettsége van.

Az adatvédelemmel kapcsolatban legszélesebb feladatkörrel rendelkező hatóság a korábban már említett NAIH. Ennek az autonóm államigazgatási szervnek a feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának elősegítése.[27] A NAIH adatvédelmi feladatkörében bejelentésre vagy hivatalból vizsgálatot folytat, az érintett kérelmére vagy hivatalból adatvédelmi hatósági eljárást folytat, illetve hivatalból titokfelügyeleti hatósági eljárást folytat.

A NAIH feladatait részletesen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) szabályozza, és egyben ide telepíti a GDPR szerinti felügyeleti hatóság feladat- és hatáskörét.[28]

A NAIH feladatai közül leginkább az adatvédelmi incidensekkel összefüggőket említem, hiszen az említett eset is egy azok közül. Az *adatvédelmi incidens* az adatokat érintő olyan biztonsági esemény, amelyért az adott vállalkozás vagy szervezet felel (lehet ez a kibertérrel összefüggően vagy a fizikai térben), és amelynek eredményeképpen sérül a titoktartási kötelezettség, az adatok hozzáférhetősége vagy azok integritásához fűződő érdek.[29] Ha a sérülés bekövetkezik és az incidens feltehetően kockázatot jelent az érintettek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül, legkésőbb 72 órával azután, hogy az adatvédelmi incidensről az adatfeldolgozó tudomást szerzett, a NAIH felé be kell jelenteni. A tudomásszerzés azt jelenti, hogy az adatkezelő észszerű mértékű bizonyosságot szerzett arról, hogy biztonsági esemény történt.[30]

Adatvédelmi incidens lehet tehát zsarolóvírus-támadás során a személyes adatok megszerzése, törlése vagy egy olyan adathordozó (például pendrive, laptop stb.) elvesztése, a szervezet birtokából való kikerülése, amelyen egy szervezet vagy vállalkozás által kezelt személyes adatok találhatók, és ezek védelme jelszóval vagy egyéb más, logikai vagy fizikai védelemmel nincs biztosítva, így annak megtalálása, megszerzése esetén reális lehetőség van arra, hogy azt mások is megismerjék.

Az adatvédelmi incidenssel összefüggésben megjelenik az *adatbiztonság* fogalma, amit tévesen kevernek az adatvédelem kifejezéssel, hasonlóan a kibervédelem és kiberbiztonság fogalmakkal. Az *adatbiztonság* az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszerét jelenti.[31]

Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, őket is haladéktalanul tájékoztatni kell. Ez a tájékoztatás mellőzhető egyes esetekben, így például, ha a korábban bevezetett – és az incidenssel érintett adatokra is alkalmazott – technikai vagy szervezési védelmi

[27] Infotv. 38. § (2) bekezdés.
[28] Infotv. 38. § (2a) bekezdés.
[29] GDPR 4. cikk 12. pontja.
[30] Lásd: https://www.naih.hu/adatvedelmi-szotar
[31] Lásd: https://www.naih.hu/adatvedelmi-szotar

intézkedések (például titkosítás) a hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat.[32]

Szervezetként létfontosságú a megfelelő technikai és szervezési intézkedések végrehajtása a személyes adatok esetleges megsértésének elkerülése érdekében.

Mivel a bemutatott cselekmény egyben a büntetőjog által megfogalmazott tényállásokat is megvalósított, így az ügyben általános nyomozóhatóságként a rendőrség is eljárt.

A rendőrség feladatait az Alaptörvény, valamint a Rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.) szabályozza. A rendőrség az Alaptörvényben, valamint az Rtv.-ben és annak felhatalmazása alapján egyéb más jogszabályban meghatározott bűnmegelőzési, bűnüldözési, államigazgatási és rendészeti feladatkörében általános nyomozó hatósági jogkört gyakorol, végzi a bűncselekmények megelőzését és felderítését, illetve az Európai Unió kötelező jogi aktusából vagy nemzetközi szerződésből eredő egyéb feladatokat.[33]

A kiberbűncselekmények megjelenése óta a rendőrség számára szükségessé vált, hogy a kiberfenyegetésekkel lépést tartva, arra is felkészülve megfelelő szakmai és technikai tudással rendelkezzen. A kibertérrel kapcsolatos tevékenységek nyomozásáról a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet mellékletei határoznak.

Az említett e-Kréta-ügyben az elkövetők felelősségre vonására a rendőrség a Btk. 423. § (1) bekezdésbe ütköző és aszerint minősülő, folytatólagosan elkövetett információs rendszer vagy adat megsértése vétsége, és a Btk. 424. § (1) bekezdés a) pontjába ütköző és aszerint minősülő információs rendszer védelmét biztosító technikai intézkedés kijátszása vétsége, a Btk. 367. § (1) bekezdésébe ütköző és aszerint minősülő zsarolás bűntettének kísérlete – mivel az elkövetők megfenyegették az alkalmazottat, hogy csak ellenszolgáltatás esetében hajlandók visszaadni a megszerzett jelszavakat és az informatikai eszközök feletti irányítást –, továbbá a Btk. 375. § (1) bekezdésbe ütköző és aszerint minősülő információs rendszer felhasználásával elkövetett csalás bűntette, valamint a Btk. 338. § (1) bekezdésbe ütköző és aszerint minősülő közveszéllyel fenyegetés bűntette miatt folytattak hivatalból eljárást.

Az új törvényi változások

Az új kiberbiztonsági törvény már kiberbiztonsági hatóságként említi azokat a szervezeteket, amelyek feladata többek között a kiberincidensek kezelése. Összesen négy hatóságot bízott meg ezzel a feladattal, a nemzeti kiberbiztonsági hatóságot, a honvédelmi kiberbiztonsági hatóságot, a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH), továbbá a pénzügyi szektorral összefüggésben a Magyar Nemzeti Bankot.

A törvény további szabályozása szerint, amennyiben „az elektronikus információs rendszert olyan jelentős kiberbiztonsági incidens éri vagy annak közvetlen bekövetkezése fenyegeti, amely a rendszer felett rendelkezési jogosultsággal rendelkező szervezet vagy a felhasználó szervezet működéséhez szükséges alapvető információk vagy

[32] GDPR 34. cikk (3) bekezdés.
[33] Rtv. 1. § (2) bekezdés 1. és 1a. pontja.

személyes adatok sérülésével jár",[34] vagyis jelentős eseményként vagy incidensként értékelhető. A NIS2 irányelv alapján egy esemény akkor tekintendő jelentősnek, ha súlyos működési zavart okozott vagy képes okozni a szolgáltatásokban, vagy pénzügyi veszteséget okozott az érintett szervezetnek; illetve az esemény jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni.[35]

A nemzeti kiberbiztonsági incidenskezelő központ a védelmi feladatainak ellátása érdekében kötelezheti a rendszer felett rendelkezési jogosultsággal rendelkező szervezetet, hogy a jelentős kiberbiztonsági incidens megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg.[36]

Kiberbiztonsági incidensnek tekinthető minden olyan esemény, amely veszélyezteti az elektronikus információs rendszerben tárolt, továbbított vagy kezelt adatokat vagy az ilyen rendszeren keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát.

A jogszabály értelmében annak érdekében, hogy a szervezet által kezelt adatok védelme a potenciális kockázatokkal arányosan biztosítható legyen, a szervezet köteles az általa az elektronikus információs rendszerben kezelt adatokat bizalmasság, sértetlenség és rendelkezésre állás szempontjából osztályozni, a vonatkozó 418/2024. (XII. 23.) kormányrendelet előírásainak megfelelően.

A szabályozás értelmében az adatosztályozási kötelezettség elsősorban abban az esetben áll fenn, ha a szervezet nem privát felhőszolgáltatást vesz igénybe. Az osztályozás célja e környezetek kockázatainak felmérése és kezelése. Ennek keretében a szervezet köteles egy költség-haszon elemzést elvégezni, amely során összehasonlítja a jelenleg alkalmazott technológia és a külföldi adatkezelés vagy a nem privát felhőszolgáltatás alkalmazásának előnyeit és hátrányait. Emellett egy kilépési tervet kell kidolgoznia, amelyben részletezi a felhőalapú megoldásról helyi infrastruktúrára vagy privát felhőre való visszaállás lépéseit, annak következményeit és költségeit.

Az adatosztályozás elsődleges célja, hogy az elektronikus információs rendszerben tárolt és kezelt adatok védelmének mértékét a bizalmasság, sértetlenség és rendelkezésre állás (CIA-elv) szerinti besorolás alapján, kockázatarányos módon határozza meg. Az osztályozás egyben segíti annak egyértelmű meghatározását, hogy az adatok milyen feltételek mellett kezelhetők külföldön vagy felhőszolgáltatásokban.

A bizalmasság szerinti osztályozás négy kategóriát határoz meg:

- B1 szint: az adatok bizalmasságának sérülése vagy elvesztése elhanyagolható vagy nem jelentős anyagi és reputációs kockázatot jelent a szervezet számára.
- B2 szint: az adatok bizalmasságának sérülése vagy elvesztése kis mértékű anyagi vagy reputációs veszteséggel járhat.
- B3 szint: az adatok bizalmasságának sérülése vagy elvesztése jelentős anyagi vagy reputációs veszteséget okozhat.
- B4 szint: az adatok bizalmasságának sérülése vagy elvesztése kritikus mértékű anyagi vagy reputációs veszteséget eredményezhet.

[34] 2024. évi LXIX. törvény.
[35] NIS2 irányelv.
[36] 2024. évi LXIX. törvény.

A sértetlenség és rendelkezésre állás tekintetében az osztályozás két szintet különböztet meg:
- SR1 szint: az adatok sértetlenségének vagy rendelkezésre állásának sérülése elhanyagolható kockázatot jelent.
- SR2 szint: az adatok sértetlenségének vagy rendelkezésre állásának sérülése jelentős vagy kritikus anyagi vagy reputációs veszteséggel járhat.[37]

A jelenlegi besorolási rendszer egyik fő kihívása az tehát, hogy az anyagi és reputációs veszteségek előzetes becslése nehezen objektivizálható, különösen incidensek bekövetkezése előtt. Az intézmények számára komoly nehézséget jelenthet a besorolási kritériumok gyakorlati alkalmazása, mivel az anyagi károk előzetes meghatározása tanácsadói szinten sem mindig triviális, míg a reputációs veszteség mérése az értékelési szempontok szubjektivitása miatt problémás.

Ezen túlmenően az adatok külföldi vagy nem privát felhőszolgáltatásokban való kezelésének korlátozása nem csupán a bizalmassági sérülésekből eredő anyagi és reputációs kockázatok mérséklésére irányul, hanem a nemzeti adatvagyon védelmét is szolgálja. A szabályozás mögöttes célja, hogy minimalizálja annak kockázatát, hogy a magyarországi szervezetek által kezelt stratégiai jelentőségű adatok külföldi piaci vagy állami szereplők számára hozzáférhetővé váljanak, különös tekintettel az ellenséges hírszerző tevékenységekre és a versenyhátrányt eredményező adatvesztésekre.

A kiberbiztonsági törvény végrehajtási rendelete az adatosztályozás vizsgálatára a nemzeti kiberbiztonsági hatóságot (NBSZ NKI) jelöli ki, amely ellenőrzi és értékeli azt a biztonsági osztályba sorolás megalapozottságának vizsgálatára irányuló eljárás keretében. Ha a vizsgálat eredménye alapján nem egyértelmű az adatosztályozás szerinti besorolás, a nemzeti kiberbiztonsági hatóság eljárása keretében tisztázza, hogy a szervezet milyen és mekkora mennyiségű adatot kezel vagy tervez kezelni az elektronikus információs rendszerben, amely osztályozás egyet nem értése esetén felülvizsgálatra kötelezheti a szervezetet.[38]

Összegzés

Az adatvédelmi incidens és kiberbiztonsági incidens bekövetkezése során első körben az érintett szervezetnek az a feladata, hogy detektálja a támadást, valamint arról tájékoztassa az érintetteket, legyen az szervezet vagy személy. Innentől kezd érdekessé válni a helyzet.

Amennyiben egy incidens során bizonyíthatóan személyes adatok sérültek, akkor a szervezet adatvédelmi tisztviselőjének 72 órán belül a NAIH honlapján található bejelentő oldalon keresztül kell megtenni a bejelentést.

A GDPR 32. cikke alapján a NAIH többek között azt vizsgálja, hogy az adatkezelés és az adatfeldolgozás a tudomány és a technológia állásának megfelelően történt-e a megfelelő technikai és szervezési intézkedések végrehajtása mellett (teljesült-e a bizalmasság,

[37] 418/2024. (XII. 23.) Korm. rendelet.
[38] 418/2024. (XII. 23.) Korm. rendelet. Az egyéb kötelezettségeket a terjedelmi korlátok miatt nem ismertetem.

sértetlenség, rendelkezésre állás és az ellenálló képesség). A vizsgálat a beérkezett bejelentésből történik, szükség esetén kiegészítő információkat kérnek.

Az új kiberbiztonsági törvény ugyanakkor, hasonlóan az adatvédelmi incidensek bejelentésére vonatkozó kötelezettségekhez, szintén azonnali bejelentési kötelezettséget ír elő a törvény hatálya alá tartozó kiberincidensek esetében.

Ha az adott szervezet az említett kiberbiztonsági törvény hatálya alá (is) tartozik, akkor a támadás miatt, a szervezet besorolásától függően jeleznie kell a négy kiberbiztonsági hatóság felé, amelyek vizsgálják a hozzájuk érkező biztonsági eseményt. Amennyiben a bejelentés tartalmából nem állapítható meg egyértelműen a biztonsági eseménnyel érintett szervezetek köre, akkor az eljárás megindítására a bejelentésnek az NBSZ NKI felé való továbbítása és a szervezet vizsgálata után kerülhet sor.

A fent nevezett szervezeteknél tehát, amennyiben a személyes adatokkal kapcsolatos biztonság sérül, akkor a NAIH felé való bejelentés elmulasztása adatvédelmi bírsággal jár (ha kiderül).

A rendőrség felé történő mulasztás ugyanakkor semmilyen szankciót nem eredményez, vagyis első esetben lehet visszatartó ereje annak, ha a bejelentési kötelezettségnek nem tesznek eleget, míg a másik két esetben nincs ilyen.

A NAIH a bejelentett incidenst követően vizsgálja azt is, hogy a szervezet tájékoztatta-e az érintett feleket, míg a másik két szervezetnek jogszabály ilyen kötelezettséget nem ír elő.

A Nemzeti Kibervédelmi Intézet hírlevelekben és a hivatalos internetes honlapján keresztül küld tájékoztatást, és figyelemfelhívást[39] tesz közzé szoftverek sérülékenységéről vagy adathalász weboldalakról, míg a Rendőrség jellemzően a már elterjedt, ismertté vált esetek (például online banki csalások) megelőzéséről, veszélyeiről tájékoztat általánosságban, ugyanakkor a ténylegesen bekövetkezett kiberincidensek számáról vagy kiberfenyegetésekről sokszor a bejelentések elmulasztása miatt sincs valós számadat.

A legnagyobb probléma tehát az e-Kréta-rendszerhez hasonlóan bekövetkezett és bekövetkező eseményeknél, hogy bár az adatok fontosságát, védelmét és biztonságát kiemelten kezelik mind a szervezetek, mind pedig a jogi szabályok, a hatóságok közötti együttműködés és tájékoztatás nincs szabályozva, így azok feladatai és vizsgálatai során nincs biztosítva az adatok elleni incidensek esetén az együttes fellépés.

Felhasznált irodalom

Eszteri Dániel – Péterfalvi Attila (2017): A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlata. In Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme: az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* Budapest: ELTE ÁJK, 405–420.

[39] Figyelemfelhívás fogalma: a Központ által a magyar kiberteret általánosan veszélyeztető, különös figyelmet érdemlő fenyegetettségekről, új támadási módszerekről, eseményekről kiadott tájékoztatás. 418/2024. (XII. 23.) Korm. rendelet, Értelmező rendelkezések 2. § 8. pontja.

European Commission (2018): *The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2873/48055

Karsai Krisztina szerk. (2013): *Kommentár a Büntető Törvénykönyvhöz.* Budapest: CompLex Kiadó. Online: https://m2.mtmt.hu/api/publication/2402217

O. Nagy Gábor – Juhász József – Szőke István (1985): *Magyar értelmező kéziszótár.* I. kötet. Budapest: Akadémiai Kiadó.

Péterfalvi Attila szerk. (2012): *Adatvédelem és információszabadság a mindennapokban.* Budapest: HVG-ORAC.

Pilling Zoltán (2024): A KRÉTA ügy tanulságai adatvédelmi szempontból – Megjelent az adatvédelmi eljárást 110 milliós bírsággal lezáró NAIH határozat! *Jogi Fórum,* 2024. március 6. Online: https://www.jogiforum.hu/cikk/2024/03/06/a-kreta-ugy-tanulsagai-adatvedelmi-szempontbol/

Jogi források

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2012. évi C. törvény a Büntető törvénykönyvről

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv)

EDPB 01/2021. számú iránymutatása az adatvédelmi incidensekkel kapcsolatos bejelentésekről

Kúria 1/2012 BJE határozata a személyes adatok vétsége tárgyában