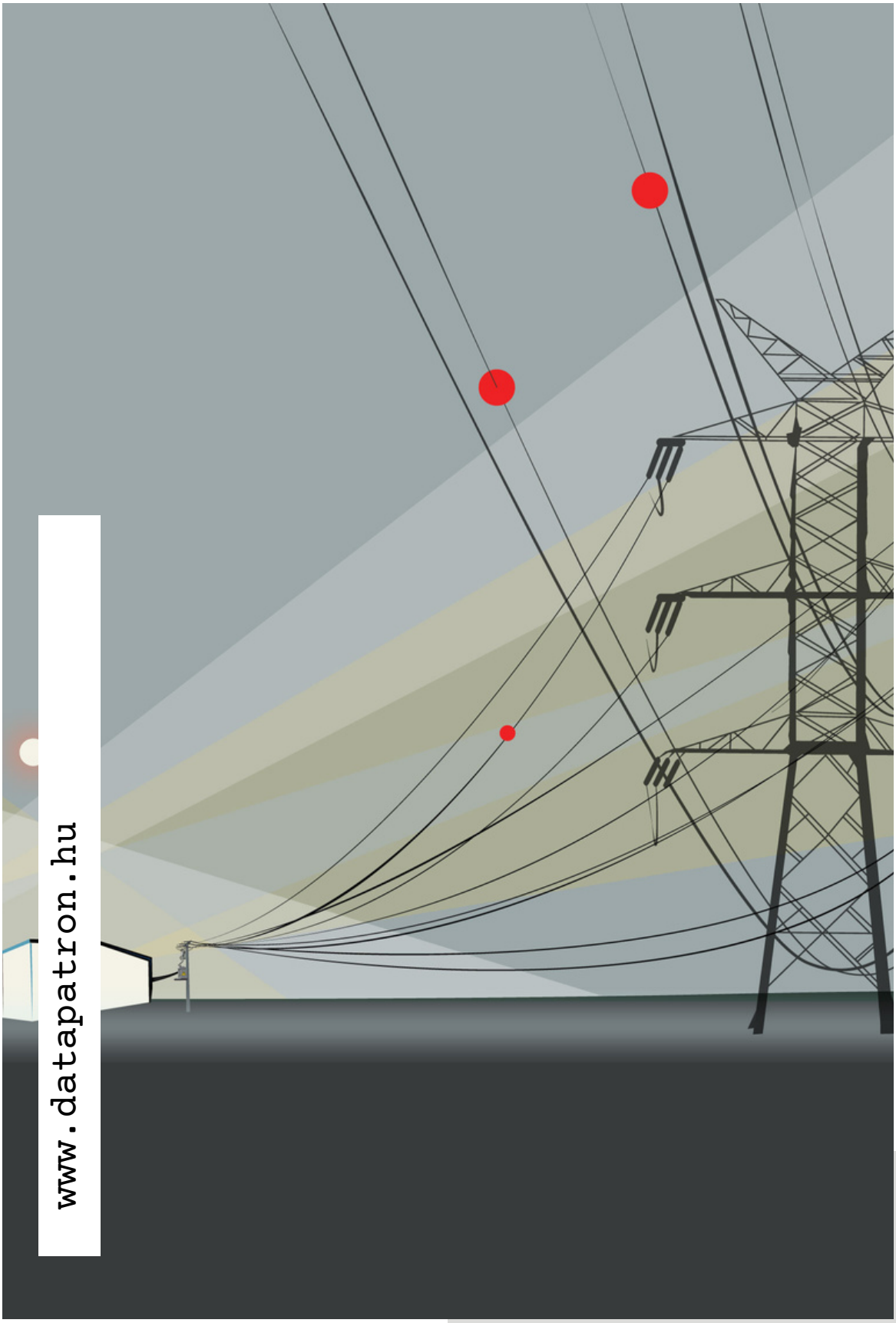
2022. DECEMBER

DATAPATRON



www.datapatron.hu

NO. 1.

DATAPATRON MAGAZIN

Adatvédelmi- és adatbiztonsági folyóirat
negyedéves elektronikus kiadvány

IMPRESSZUM

Kiadó:Ivánka-Csontos Andrea e.v.
5000 Szolnok, Dr. Kronberg J. u.9.
Kiadásért és szerkesztésért felelős: Ivánka-Csontos Andrea
Elérhetőség: info@datapatron.hu

NO.1.||2022.december

DATAPATRON

Előszó

Igazi kihívást jelentő feladat egy olyan világban adatvédelemről, információbiztonságról, kibervédelemről beszélni, ahol az online élvezetek hajszolását és a magamutogatást világversenyeket megszégyenítő kitartással űzik a felhasználók, a cégek pedig ezt kihasználva addiktív módon gerjesztik a mértéktelen fogyasztást.
Ha ehhez a képlethez hozzáadjuk a technikai újdonságok és az ezek fejlesztésén szányra kapott óriás tech cégek tényked̈eseit- amik valljuk be sokszor kibillenek az etikai határvonalról is- és itt nem a mainstream, új felfogásokra gondolok- akkor egy szakértőnek igazi celeb polihisztornak kell lenni ezen a területen ahhoz, hogy munkája célba érjen. Ez a magazin ezeket szakmai hangokat hivatott hallatni.

Szeretnék köszönetet mondani az első kiadvány szerzőinek, akik elfogadták a felkérést, és munkájukkal támogatták a magazin létrejöttét.

Ivánka-Csontos Andrea

Főszerkesztő

A VÉDELMI IGAZGATÁS VÁLASZA A BIZTONSÁGI KIHÍVÁSOKRA

SZERZŐ: DR. NOVÁKY MÓNIKA TŰ. ALEZREDES, NEMZETI KÖZSZOLGÁLATI EGYETEM RENDÉSZETTUDOMÁNYI KAR KATASZTRÓFAVÉDELMI INTÉZET, ADJUNKTUS

Egy alkotmányosan működő állam kötelessége, hogy megvédje állampolgárait. Ennek megvalósítása érdekében alkotja meg jogrendszerét, építi fel az államigazgatás rendszerét és létrehozza azon szervezetek, melyeken keresztül ellátja ezen funkcióját.

Az elmúlt évtizedekben a biztonsági környezet drasztikusan megváltozott. A biztonságot fenyegető események globálissá váltak, és az állam által erre adott válasz is globális kell, hogy legyen.

A szükséges válaszok kialakításának első lépése, a fenyegetések detektálása. Magyarország Nemzeti Biztonsági Stratégiája [1] (a továbbiakban: NBS) megfogalmazta azokat a kiemelt kockázatokat, amellyel hazánk biztonságát fenyegetik. Az NBS célja *„Biztonságos Magyarország egy változékony világban”.*

Ennek a gondolatnak a mentén a feltárt kockázatokra adott kormányzati választ fogalmazza meg. Az NBS a következtő, hazánk biztonságát fenyegető kockázatokat nevesítette: illegális migráció, váratlan fegyveres támadás, kibertámadások, terrorcselekmények, tartós népességfogyás, nemzetközi gazdasági válság, ellátási válsághelyzet, bűnszervezeteket, szervezetett bűnözői csoportok térnyerése, ipari balesetek, katasztrófák, lakosság súlyos, tömeges megbetegedése, nagyobb r- és belvizek, globális felmelegedés hatásai. [1] Ezekkel a kockázati tényezőkkel számolva stratégiai cél a biztonság szavatolása, intézkedések hatékonyságának, valamint rugalmasságának erősítése, továbbá a nemzetközi együttműködés megszilárdítása. [2] A biztonság valamennyi dimenzióját: politikai, gazdasági, pénzügyi, társadalmi, technológiai, környezeti, egészségügyi, információs, rendészeti, valamint kibertérbeli összetevőivel szembeni fenyegetések, kihívások és az ezekkel szembeni felkészülés és védekezés megvalósítása a feladat. [3]

Magyarország Alaptörvénye (a továbbiakban: Alaptörvény)[4] az alapvető jogokon keresztül határozza meg az állam és az egyén viszonyát.

[1]Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020.(IV.21) Kormányhatározat. https://uj.jogtar.hu/#doc/db/1/id/A20H1163.KOR/ts/20200423/ (letöltés ideje: 2022.12.13.)
[2]Csiki V.T.-Tálas P.: Magyarország új nemzeti biztonsági stratégiájáról. Stratégiai Védelmi Kutatóintézet ELEMZÉSEK 2020/17. pp 1-18. NKE Eötvös József Kutatóközpont Stratégiai Védelmi Kutatóintézet. https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKI_Elemz%C3%A9sek_2020_17_Az%20%C3%BAj%20magyar%20Nemzeti%20Biztons%C3%A1gi%20Strat%C3%A9gi%C3%A1r%C3%B3l%20_(Csiki%20Varga%20T.%20%20-%20Talas%20P.).pdf (letöltés ideje: 2022.12.13.)
[3]Ambrusz J.: Rendvédelmi ismeretek. NKE Katasztrófavédelmi Intézet, Budapest 2014. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/8587/Teljes%20sz%c3%b6veg%21?sequence=2&isAllowed=y (letöltés ideje: 2022.12.13.)
[4]Magyarország Alaptörvénye. https://uj.jogtar.hu/#doc/db/1/id/A1100425.ATV/ts/20230101/ (letöltés ideje: 2022.12.13.)

Az állam elsőrendű feladata az alapjogok tiszteletben tartása és védelme, amely a közrend és közbiztonság elleni külső-, belső támadás, az élet- és vagyonbiztonságot veszélyeztető események megelőzése és a gyors beavatkozással valósítja meg. Ennek érdekében működtette- a 2022.november 01-jén hatályon kívül helyezett- a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény (a továbbiakban Honv.tv.) [5] alapján a védelmi igazgatás rendszerét. [6]

A védelmi igazgatás rendszere a közigazgatás rendszerén belül magában foglalta a honvédelmi-, katasztrófavédelmi igazgatást, és a rendészeti igazgatást, melyen keresztül a szervezetek megvalósítják az állampolgárok élet- és vagyonbiztonságát. [5] A megváltozott biztonsági környezet tette szükségessé a jogszabályok újra gondolását. Az Alaptörvény 9. módosítása (a továbbiakban: Alaptv. mód.)[7]

2020. decemberében megteremtette a feltételét a védelmi-biztonsági igazgatás[9] rendszere kiépítésének, és 2021.áprilisában megjelent a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban: Vbö.) [8], amely újra tervezte a védelmi igazgatás rendszerét és létrejött a védelmi és biztonsági igazgatás.

A különleges jogrend átalakításával 2022. november 01-jével hadiállapot, szükségállapot, valamint veszélyhelyzet kihirdetésére lesz lehetőség. [4] Átláthatóbbá válik a különleges jogrend kihirdetésére okot adó események, körülmények rendszere, a fokozatosság elvét betartva a legsúlyosabb eseteket figyelembe véve, az állam képes hatékonyan reagálni a változó biztonsági kihívásokra, környezetre a jogi szabályozásba épített garanciális elemek támogatásával. A gyors reagálás eleme, hogy a Kormány a különleges jogrend kihirdetését követően a felelős döntéshozatalt biztosítja azzal, hogy hadiállapot esetén az Országgyűlés által átruházott jogokat gyakorolja, dönt a Magyar Honvédség külföldi, vagy hazai alkalmazásáról. Rendelet alkotási jogköre szavatolja az operatív, jogi és politikai döntéshozatalt. A különleges jogrendre vonatkozó szabályok mellett a Vbö-vel létrejött egy olyan rendszer, amely képes az összehangolt felkészülésre és védekezésre, képes megfelelni a változó biztonsági környezet kihívásainak és fenyegetéseinek, a civilizációs és természeti események, valamint az emberi magatartás okozta támadások hatékony elhárítására és kivédésére. [8]

[5]2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. https://uj.jogtar.hu/#doc/db/1/id/A1100113.TV/ts/20220728/ (letöltés ideje: 2022.12.13.)

[6] Honv.tv. „ 80.§ 32. pont védelmi igazgatás: a közigazgatás részét képező feladat- és szervezeti rendszer, amely a Kormány - a honvédelemért felelős miniszter útján gyakorolt - irányítása mellett a Magyarországot veszélyeztető fenyegetésekkel és támadásokkal szemben az állam feladatainak megvalósítására létrehozott, valamint egyes védelmi feladatok ellátásra kijelölt közigazgatási szervek által végzett tervező, végrehajtó, rendelkező tevékenység.” https://uj.jogtar.hu/#doc/db/1/id/A1100113.TV/ts/20210101/(letöltés ideje: 2021. 11. 08.)

[7]Magyarország Alaptörvényének kilencedik módosítása. (2020.december 22.) https://uj.jogtar.hu/#doc/db/1/id/A2001222.ATV/ts/20230701/ (letöltés ideje: 2022. 12.13.)

[8]2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról. https://uj.jogtar.hu/#doc/db/1/id/A2100093.TV/ts/20221102/ (letöltés ideje: 2022.12.13.)

[9] Vbö. „5.§ 16. védelmi és biztonsági igazgatás: a közigazgatás részét képező feladat- és szervezetrendszer, amely a Kormány irányítása mellett a Magyarországot és annak lakosságát veszélyeztető fenyegetésekkel és támadásokkal szembeni fellépésre létrehozott, illetve jogszabályban ilyen feladatra kijelölt állami szervek központilag összehangolt tervező, végrehajtó és rendelkező tevékenysége, különös tekintettel a válsághelyzetek kezelésére, a különleges jogrend kihirdetésére, valamint a védelem- és biztonságtudatosság polgári és állami fokozásával összefüggő feladatokra és az ezekre való felkészülésre, beleértve a honvédelmi igazgatást és az annak részét képző katonai igazgatást, továbbá a kapcsolódó rendvédelmi szervek által ellátott igazgatást” https://uj.jogtar.hu/#doc/db/1/id/A2100093.TV/ts/20221102/ (letöltés ideje: 2022.12.14.)

A honvédelem[10] és a katasztrófavédelem[11] mellett a Vbö. hazánk védelmét és biztonságát nemzeti ügynek[12] tekinti.

Ennek érdekében hazánk fegyveres védelmét három pillérre helyezi: honvédelem rendszere és a Magyar Honvédség, rendvédelem rendszere és a rendvédelmi szervek, nemzetbiztonsági szolgálatok, továbbá kiemelt feladat hárul a közigazgatási szervekre, amelyek kötelesek az együttműködésre. A védelmi és biztonsági igazgatás központi szerve a Védelmi Igazgatási Hivatal, amely koordinációs, szervezési és igazgatási feldatokkal összehangolja a biztonsági és védelmi feladatokat. Az új jogi környezet, és a védelmi és biztonsági igazgatás rendszerének jogi és szervezeti kialakítása jelenleg is folyamatban van. A tervezettek szerint a Vbö. 2023.július 1-jn lépett volna hatályba, azonban mind a szomszédos országban kitört fegyveres konfliktus, mind a migrációs és gazdasasági helyzet felgyorsította a folyamatot, így 2022. november 01-én az Alaptörvény különleges jogrendre vonatkozó módosítása és a Vbö. is hatályba lépett. A védelmi és biztonsági igazgatással összefüggésben számos törvény módosítása - többek között a honvédelemről és Magyar Honvédségről szóló 2021.évi CXL.tv, a katasztrófavédelemről és a hozzá tartozó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény- történt meg.

Folyamatban van a Kormány végrehajtási- és a kapcsolódó ágazati rendeleteinek megalkotása.

A védelmi igazgatás új alapokra helyezése és átfogó, Magyarország védelmének és a nemzet biztonságának szavatolása hozta létre a védelmi és biztonsági igazgatás új struktúráját, amely az ágazati sajátosságokat érintetlenül hagyja, fenntartja az ágazati irányítás rendszerét, és a válságkezelésre való felkészülés, továbbá a válsághelyzeti működés koordinálásnak fokozása érdekében korszerűsíti a válságkezelési szabályozást és a hangsúlyt a felkészülés és a biztonságtudatosság fokozására építi. Megteremti a feltételeit a gyors és hatékony válságkezelésnek, a megváltozott körülményekhez való gyors alkalmazkodási képesség kialakításának.

[10]A honvédelemről és Magyar Honvédségről szóló 2021.évi CXL.tv. 1.§ (1) bekezdés.https://uj.jogtar.hu/#doc/db/1/id/A1100113.TV/ts/20221101/lr/chain14(letöltve: 2022. 12.13.)
[11] A katasztrófavédelemről és a hozzá tartozó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 1.§ (1) bekezdés.
https://uj.jogtar.hu/#doc/db/1/id/A1100128.TV/ts/20230101/ (letöltve: 2022. 12.13.)
[12] Vbö. 1.§

KIBERPAJZS

SZERZŐ: BIRÓ GABRIELLA A MAGYAR NEMZETI BANK INFORMATIKAI FELÜGYELETI FŐOSZTÁLY VEZETŐJE, AZ (ISC)2 HUNGARY CHAPTER ELNÖKSÉGI TAGJA ÉS A WITSEC ALAPÍTÓ ELNÖKSÉGI TAGJA

A KiberPajzs projekt keretében alapító tagként a Magyar Nemzeti Bank (MNB), a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság (NMHH), a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitányság átfogó oktatási programot indított az ügyfelek digitális pénzügyi tudatosságának fejlesztése érdekében.

KiberPajzs
Védelem a pénzügyekben

A projekt célja, hogy egységes arculatú, folyamatos kommunikációval felhívja az ügyfelek, a fogyasztók figyelmét a biztonságos digitális pénzügyek alapvető tudnivalóira és segítse őket a csalások idejében történő felismerésében, megakadályozásában, hatékony kezelésében. Erről az öt szervezet 2022. november 7-én együttműködési megállapodást írt alá és ezzel egy időben elindult a www.kiberpajzs.hu honlap is.

Az együttműködési megállapodás megkötését hosszú hónapok előkészítő munkája előzte meg, amelynek során számos egyeztetést, tapasztalatcserét tartottak az aláíró szervezetek szűkebb és szélesebb körben, a kereskedelmi bankok, a kártyatársaságok, különböző rendőri szervek, a fogyasztóvédelem és az adatvédelmi hatóság szakembereinek bevonásával. Minden résztvevő megerősítette, hogy egyre több és egyre kifinomultabb visszaéléssel találkoznak az online térben, ezért a KiberPajzs együttműködés szükséges és időszerű.

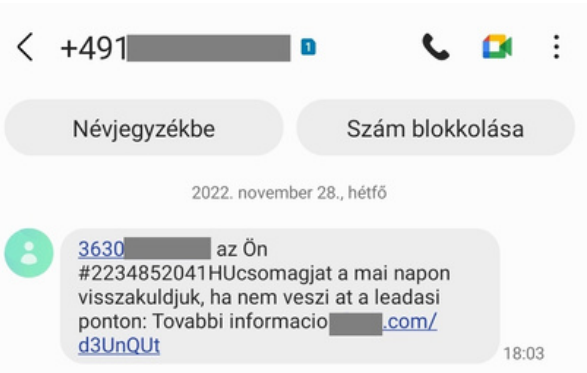
A kommunikációs kampány mellett a kezdeményezés másik nagyon fontos hozadéka a szakértők közti tudásmegosztás, a csalások forgatókönyveinek, elkövetési módjainak, ismérveinek és trendjeinek elemzése, a megelőzés és védekezés folyamatainak hatékonyabbá tétele. A szakértői egyeztetések, megbeszélések mellett eddig két szélesebb körű tudásmegosztó eseményt is rendeztünk 2022 májusában és októberében,

melyek során az előadók esettanulmányokat és elemzéseket mutattak be a visszaélésekkel, hatósági eszköztárral és kommunikációs lehetőségekkel kapcsolatban. A résztvevők visszajelzései alapján nagyon hasznos az eltérő megközelítéseket - a felügyeletek (MNB, NMHH), a bűnüldöző szervek, a bankok és a Pénzügyi Békéltető Testület tapasztalatait - egyben látni és megismerni a munkájuk során alkalmazott különböző megközelítéseket. Úgy tervezzük, hogy a továbbiakban is évente két alkalommal rendezünk hasonló tudásmegosztó alkalmakat hibrid módon, online és személyes részvétellel a projekt résztvevői és támogatói számára.

A projekt egyeztetései során a résztvevőktől kapott adatok alapján is látható, hogy az utóbbi időben felerősödtek azok a támadások, amelyek az erős banki-pénzügyi biztonsági rendszerek helyett -megtévesztés vagy/ és pszichológiai manipuláció révén - közvetlenül az ügyfeleket célozzák. Már az amúgy pénzügyekben járatos, pénzügyileg tudatos banki ügyfelek is áldozatul eshetnek a csalóknak, akik az utóbbi időszakban egyre kifinomultabb technikákat alkalmaznak. Néhány gyakori példa, a teljesség igénye nélkül:

Mostanában gyakori az az SMS-ben érkező üzenet, amely egy honlap felkeresésére vagy alkalmazás letöltésére és adatai megadására kéri a címzettet annak érdekében, hogy átvehessen egy csomagot. Mivel a karácsonyi időszak közeledtével a szokásosnál is többen és több árut rendelnek online, sajnos sokan jóhiszeműen áldozatul esnek ennek a fajta csalásnak.

Nagyon elterjedt visszaélési típus az is, amikor telefonon hívnak magánszemélyeket és úgy tesznek, mintha a bankjuk nevében tájékoztatnák őket. A csalók elmondják, hogy gyanús utalási vagy bankkártyás vásárlási kísérleteket észleltek a számlákról, illetve a bankkártyákkal. Emiatt, úgymond egy (hamis) „technikai számlára” továbbküldve azonnal biztonságba kell helyezni az ügyfél megtakarítását. A telefonos azonosításhoz szükséges pár személyes azonosítón túl pl. „további adategyeztetésre”, „netbanki letiltásra” hivatkozva a bizalmas banki adatokat (számla vagy/és kártyaszám, a PIN és netbanki belépési kód) is elkérik,



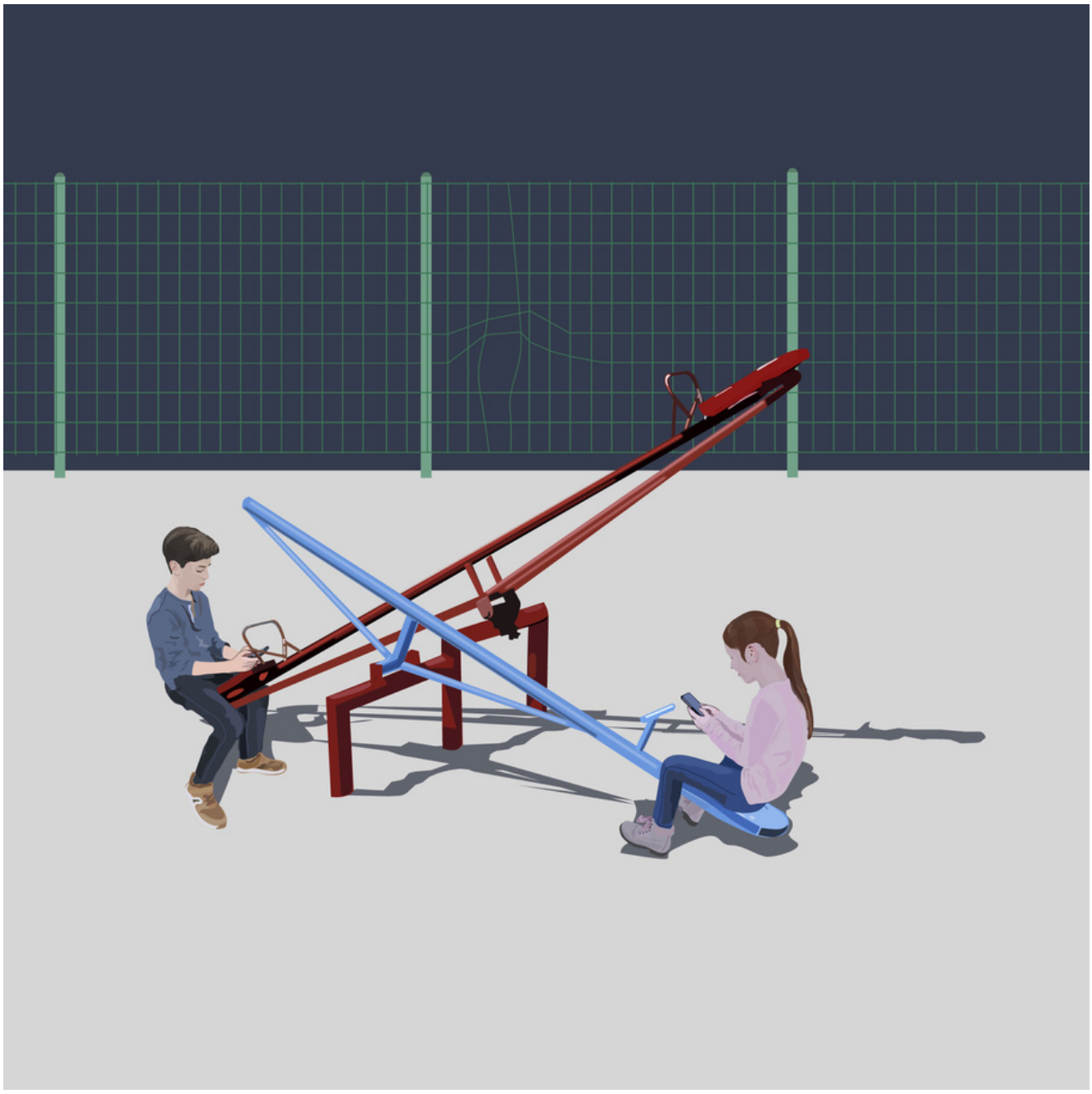
vagy a csalók számára távoli hozzáférést biztosító alkalmazás telepítését kérik, és az így megszerzett információkat felhasználva ellopják az ügyfél szálmájáról az ott lévő összeget. Egyre gyakrabban tapasztaljuk azt is, hogy az ilyen hívások hamisított számról, azaz látszólag a tényleges banki ügyfélszolgálati telefonszámról érkeznek.

Ehhez kapcsolódóan a legújabb gyakorlat, hogy a bűnözők nem csak a bankszámlát ürítik ki, hanem a megszerzett adatokkal visszaélve az ügyfél nevében személyi kölcsönt is igényelnek.

További új bűnözői módszer, amikor a fogyasztók internetes portálon hirdetnek eladásra egy árut, és a csalók vevőként jelentkeznek. Azt kérik az eladótól, hogy egy csomagküldő szolgálat internetes oldalán banki azonosítóik megadásával indítsanak fizetési kérelmet feléjük, s akkor ott kifizetik az árut. Csakhogy az általuk megküldött csomagküldő weboldal hamis, s az azon szereplő internetes banki linkeket is ők alakították ki, így a banki adataikat begépelve az ügyfelek maguk adják meg az információkat a csalóknak.
Az elsősorban cégeket, intézményeket érintő úgynevezett számlaváltásos csalások (vagy angolosan Business Email Compromise visszaélések) is egyre gyakoribbak. Ezeknél az eseteknél a bűnözők egy várható költséggel kapcsolatban azt a látszatot keltik, mintha a számla jogosultjának megváltozott volna a számlaszáma és kérik, hogy másik bankszámlára utalja át az összeget. Jellemzően csak akkor derül fény a bűncselekményre, mikor a számla fizetési határideje letelik és a pénz jogos várományosa keresi az összeget.

Bár összességében rendkívül biztonságos a hazai elektronikus pénzforgalom, s a visszaélések aránya elenyésző, mégis jól láthatóan emelkedik a kibercsalások száma, és mostanra szinte mindenki találkozott egy-egy esettel a fent felsorolt példák közül is. Ezért is fontos - a szabályozás/adminisztratív védelem és a technikai eszközök alkalmazása mellett - a fogyasztók biztonságtudatosságának fejlesztése, a figyelemfelhívás. Az MNB a KiberPajzs kezdeményezés mellett is sokat tett és tesz azért, hogy a problémára felhívja a figyelmet: több szakmai cikket jelentetett meg a témában, a fogyasztók tájékoztatására megújította Pénzügyi Navigátor oldalának digitális biztonsággal kapcsolatos fejezetét.

A jegybank mellett a pénzügyi intézmények, hatóságok és különböző szervezetek is folytatnak figyelemfelhívó kampányokat: teljesen világos, hogy csak összefogással, a résztvevők eszközeinek együttes alkalmazásával léphetünk fel hatékonyan. A novemberben indított első kampány során a plakátokon három olyan „mindennapi példakép” személyiséget jelenítettünk meg, akik élethelyzete hasonlít a legtöbb pénzügyi fogyasztóéhoz. Terveink között szerepel, hogy további karaktereket mutatunk majd be, illetve a jövőben szeretnénk kampányfilmekben, rádiókban, valamint egyéb csatornákon is ismertetni a főbb csalási formákat.



OKOSTELEFONOK KIBERBIZTONSÁGI ÉS ADATVÉDELMI KÉRDÉSEI

SZERZŐ: DR. KRASZNAY CSABA A NEMZETI KÖZSZOLGÁLATI EGYETEM DOCENSE, AZ EÖTVÖS JÓZSEF KUTATÓKÖZPONT KIBERBIZTONSÁGI KUTATÓINTÉZETÉNEK VEZETŐJE,A TALLINNI MŰSZAKI EGYETEM TUDOMÁNYOS MUNKATÁRSA

Az okostelefon a legszemélyesebb tárgyunkká vált az elmúlt évtizedben. Minden titok, minden személyes információ ezen az eszközön tárolódik, vagy legalábbis hozzáférhető az azon beállított hozzáféréseken keresztül.

Valószínűleg mindenkinek megvan az a pillanat, amikor a leginkább kedvelt közösségi hálózat hirdetései között feltűnik egy olyan téma, amiről épp nem rég beszéltünk, vagy akár csak gondoltunk rá. Ezek a kimondott szavak vagy ki nem mondott gondolatok sem lennének hirdetéssé konvertálható információk, ha nem lenne folyamatosan mellettünk egy olyan eszköz, ami minden adatot rögzít és továbbít a nagy adatkapitalista cégeknek rólunk és a környezetünkről. A 2020-as évek adatvédelmi kihívásai sokkal kevésbé lennének jelen az okostelefonok nélkül. A 2020-as évek digitális gazdasága azonban működésképtelen lenne a mobilitás, a mindenkinél jelen levő okoseszközök nélkül. Ennek az évtizednek tehát az egyik legfontosabb feladata megtalálni az egyensúlyt a mindenki számára hasznos digitalizáció és privát szféránk fenntartása, a személyes kiberbiztonság megteremtése között.

De mit jelent a személyes kiberhigiénia? Milyen veszélyek leselkednek ránk az okostelefon használata közben?

Ezek azok a kérdések, amit az indokoltnál sokkal kevesebbszer tesz fel a modern kor embere. Pedig a kiberbiztonsági szakember szemszögéből a teljes mobil ökoszisztéma olyan időzített bomba, ami csoda, hogy még nem robbant ránk teljesen. Ehhez persze hozzá kell tenni, hogy probléma van bőségesen. Vegyük is sorra azokat a szempontokat, melyeket mindenképpen érdemes megfontolni!

Kezdjük az eszköznél! A kibertámadások az elmúlt években egyre többször veszik célba a hardveres réteget, hiszen egy olyan komplex eszköznél, mint például az okostelefon, könnyen előfordulhat, hogy olyan részegységek kerülnek beépítésre, melyek ismert sebezhetőséggel rendelkeznek és viszonylag könnyen támadhatóvá teszik a platformot.

Olcsóbb vagy régebbi eszközöknél például könnyen jöhet olyan hír a sajtóban, mely után eszközök százmillióinak biztonsága válik kérdésessé, ahogy történt az az Apple eszközök esetében is a biztonságot megvalósító egyik chip sebezhetősége után (https://ipon.hu/magazin/cikk/javithatatlan-sebezhetoseget-talaltak-az-apple-biztonsagi-chipjen). Az ilyen sérülékenységek kihasználásához persze fizikailag hozzá kell tudni férni az eszközhöz, de ez még ilyen eszközöknél is előfordul időnként. Jelen sorok szerzője például mindig hevesen dobogó szívvel adja le okostelefonját a Nemzetibiztonsági Szakszolgálat zárható szekrényeibe. Első lecke: az újabb és a drágább biztonsági szempontból jellemzően jobb, a fizikai hozzáférés pedig sokszor sikeres támadást tesz lehetővé.

Ugorjunk tovább az operációs rendszerre!

A világ szinte kizárólag két operációs rendszert használ: az Apple iOS és a Google Android rendszerét. Mindkét cég gyorsan és hatékonyan javítja rendszereinek biztonsági hibáit, a kérdés csak az, hogy vajon a végfelhasználók ezeket a javításokat mennyi idő után telepítik? Illetve, egy régebbi eszköz mennyi ideig kapja meg egyáltalán a biztonsági frissítéseket?

Egy-egy biztonsági frissítés azt jelenti, hogy az éppen használt operációs rendszer változat valamilyen biztonsági hibát tartalmaz, amelyet kibertámadók ismerhetnek és potenciálisan ki is használhatnak. Ergo, ha nem telepítjük a frissítést, lehetséges támadásnak vagyunk kitéve. Ennek ellenére a felhasználók nem elhanyagolható része akkor sem telepíti a legújabb változatokat, ha a telefon ezt egyébként határozottan szeretné. A referenciaként használt iOS frissítések esetében például a felhasználók nagyjából 40%-a olyan verziót használt, melynél volt már frissebb és biztonságosabb (https://gs.statcounter.com/ios-version-market-share/). Ez az arány az Android felhasználóknál sokkal rosszabb, mivel ahány gyártó, annyiféle operációs rendszer változat, nincsen olyan egységes frissítési séma, mint az Apple-nél. Második lecke: frissítsünk, ahogy tudunk, különösen akkor, ha ezt már a telefon is nagyon szeretné. Az elavult telefonok pedig jellemzően elavult operációs rendszereket jelentenek, melyek az idő múlásával egyre könnyebben támadhatók.

Folytassuk az alkalmazásoknál! Hány alkalmazás van a Nyájas Olvasó telefonjára telepítve? Néhány? Több tucat? Százas nagyságrendű? És mikor frissítette ezeket utoljára? Biztonsági szempontból talán az applikációk okozzák a legtöbb gondot.

A „csak kipróbálom”, az „úgyis ingyen van” mentalitás hozza magával azt, hogy telefonunk tele van biztonsági és adatvédelmi szempontból erősen kérdéses minőségű alkalmazásokkal. Az szinte már természetes, hogy az adatvédelmi szabályozást el sem olvassuk, így azok a felhasználói adatok, melyek egy alkalmazás használata közben keletkeznek, rövid úton a Metánál (azaz Facebook) vagy a Google-nél kötnek ki, hiszen „ha valami ingyen van, mi magunk vagyunk az áru”, azaz a remek „ingyenes” játékszoftverek jellemzően abból élnek, hogy a náluk keletkezett adatokat ezeknek az adatkapitalista cégeknek adják el. Ennél sokkal rosszabb a helyzet akkor, amikor az applikációk eleve csalárd szándékkal kerülnek megírásra. Szerencsére a nagy alkalmazás boltok (Google Play, Apple App Store) kínálatába ezek egyre nehezebben kerülnek be, de az „alternatív” boltok kínálatában, ahol például normál esetben fizetős szoftvereket ingyen ajánlanak vagy olyan alkalmazásokat kínálnak, melyek a nagy boltoknál illegálisak lennének, nyugodtan számíthatunk egy kis „meglepetésre”. Ezek olyan, az alkalmazásokba írt kártékony kódok, melyeket szándékosan adatlopásra, esetleg kriptovaluta bányászatra írtak. Harmadik lecke: mindig olyan alkalmazást használjunk, ami megbízható forrásból jön, olvassuk el az adatvédelmi tájékoztatót és persze mindig frissítsük az applikációt, hogy az ezekben levő biztonsági sebezhetőségek se okozzanak gondot.

A helyhiány miatt biztonsági gyorstalpalónkat fejezzük be a felhasználóknál!

A kiberbiztonsági szakma egyik legtöbbet emlegetett aranyköpése szerint a kiberbiztonsági problémák túlnyomó többségét a szék és a billentyűzet között kell keresni, azaz az emberi hibák nélkül a kibertámadások túlnyomó többsége meg sem történne. Statisztikailag ez minden kétséget kizáróan igaz, de annyival finomítani kell ezt az állítást, hogy a felhasználókat, jellemzően senki sem figyelmezteti arra, hogy a nem körültekintő használatból baj lehet. Erre kiváló példa a FluBot trójai terjedése (https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/). Talán sokakban megmaradt az a 2021. márciusi eset, amikor magyar (és egyébként más országbeli) telefonszámok milliói kaptak SMS értesítést arról, hogy a csomagküldő szolgálat hamarosan kézbesíteni fogja a rendelt csomagot, aminek követése érdekében telepítsünk egy alkalmazást, amit az SMS-ben levő linkről lehet letölteni. Az alkalmazás telepítése után a netbanki hozzáférést próbálta megszerezni, a belépéshez szükséges egyszeri, SMS-ben érkező jelszóval együtt.

Ha a felhasználó először végiggondolja, hogy vár-e egyáltalán csomagot, ha nem kattint a linkre, ha nem telepíti az alkalmazást, a telepítés közben nem kattint többször is a továbbengedésre, az operációs rendszer figyelmeztetése ellenére, a FluBot nem tudott volna ilyen sikeresen terjedni. Negyedik és egyben utolsó lecke: gondolkodjunk! Ami kicsit is gyanús, az valószínűleg megér egy utánaolvasást vagy legalábbis egy kérdést egy információbiztonsághoz értő ismerőstől. A kiberhigiénia ugyanis nem csak személyes ügy. A teljes kibertér biztonsága nagyban függ attól, hogy az egyes felhasználók hogyan viszonyulnak a biztonsághoz.

PSZICHOLÓGIA A JOGBAN - KVERULÁTOROS TÉBOLYBAN SZENVEDŐK A JEGYZŐI BIRTOKVÉDELMI ÉS AZ ADATVÉDELMI HATÓSÁGI ELJÁRÁSOKBAN

SZERZŐ: DR. KAJÓ CECÍLIA,A BOJTÁR TELEFONOS ÁLLATVÉDELMI JOGSEGÉLY-SZOLGÁLAT EGYESÜLET TITKÁRA, A MAGYAR BIRTOKVÉDELMI SZÖVETSÉG TANÁCSADÓJA, HATÓSÁGI JOGALKALMAZÓKÉNT DOLGOZIK AZ ÜLLŐI POLGÁRMESTERI HIVATALBAN

Aki valaha foglalkozott birtokvédelmi ügyekkel, bizonyosan ismer kverulátoros avagy perlekedési tébolyban szenvedő embereket.

Ez a személyiségzavar a paranoiának az egyik fajtája, és leegyszerűsítve azt jelenti, hogy a benne szenvedő akár egész élete során harcban áll a világgal - a fülemüle-perek, a szomszédháborúk pedig kiváló táptalajt képeznek az ilyen harcokhoz. A harcokhoz a fő motívum nyilvánvalóan a bosszúállás hajtóereje.

A személyiségzavaros fél vélt vagy valós sérelmei orvoslása érdekében (a sérelem nagyságától függetlenül) azonnal hivatalos utat keres, eljárásokat, pereket indít, és amennyiben elégedetlen a meghozott döntéssel - így rögtön kódoltan a döntéshozó munkájával is - nemcsak a döntés ellen megy tovább jogorvoslatért hanem egészen bizonyosan magát a döntéshozót is bepanaszolja feletteséné, felügyeleti szervénél vagy más teljesen random, a döntéshozóval egyébként szervezési-irányítási-felügyeleti viszonyban egyáltalán nem lévő intézménynél is.

Egy-egy ilyen személy élete során több száz vagy akár ezer megindított eljárással, perrel „dicsekedhet” vegyesen a polgári jogi, a büntetőjogi és a közigazgatási jogterületekből is. Saját birtokvédelmi jogalkalmazói gyakorlatomból emlékszem olyan félre, aki havonta 4-5 birtokvédelmi kérelmet nyújtott be osztatlan közös tulajdonon élő családtagjai ellen és büszkén mutatta mindig a nála lévő fekete mappát, melyben a kérelmeket tartotta és amelyben a kérelmek alatt sok-sok ívnyi illetékbélyeg is lapult (akkor még illetékköteles volt a jegyzői birtokvédelmi eljárás - ma már ez a „visszatartó erő” sincs meg az eljárásban).

Az ikonikus fekete mappából olyan kérelmek kerültek elő többek között, melyek sok-sok évnyi munkát jelentettek a hivatalban: birtoklást sértő kezdő tényezőként jelezte például a kérelmező fél, hogy családtagjai kutyájukat az ingatlanon szabadon tartják, és ebből nőtt ki aztán a hosszú éveken át elhúzódó folyamat. Amikor a családtagok az ebnek kennelt építettek, állította, hogy (emlékszünk: osztatlan közös tulajdon - és itt fontos részletkérdés, hogy használati megállapodás nem létezett) a „saját" területére épült a kennel amire ő engedélyt nem adott, majd (egy másik eljárási szál részeként) állatkínzás gondolata is felmerült részéről, hiszen ki zárna kennelbe egész napra egy kutyát (paranoiája mellett nyilván részleges amnéziában is szenvedve, hogy miatta történt az egész), végül az eb pusztulása után az elbontott kennel „visszafordíthatatlan" károkat okozott az ő „saját" területén. Mindezekről természetesen több száz órányi kamerafelvételt is becsatolt minden esetben.

Amikor a visszafordíthatatlan kárral kapcsolatban a hivatalnál nem jutott előbbre, és bemondásra nem részesült több millió forintos kártérítésben, természetesen következett a közigazgatási jogkörben okozott kár miatt benyújtott keresetlevél (az ezt elutasító ítéletet hozó bíróság ellen „természetesen" több panasz érkezett a bírósági szervezetrendszerben magasabb fórumokhoz illetve más, bírósági szervezetrendszertől teljesen független közigazgatási szervekhez is). Amikor mindkét oldal számára bizonyossá vált, hogy hosszú idő óta megfigyelik egymást a kölcsönösen egymásra irányított, ingatlanon belül felszerelt kamerarendszereik segítségével, természetesen eljött az ideje a NAIH-hoz fordulásnak is. Egyszerre szomorú és vidám idők voltak ezek az akkori hatósági munkacsoportomban.

Ahogyan egy konfliktus létrejöttéig sokakat nem érdekel személyes adataik jogszerű kezelése, és csak a konfliktus kapcsán keresik meg a NAIH-ot (jellemzően például: volt munkavállalók indítanak eljárást munkáltatójuk ellen illetve más hasonló viszonyrendszerben létező felek), ugyanez nagyon jellemző a már említett jegyzői birtokvédelmi vagy például a jegyzői társasházi törvényességi felügyeleti hatáskör gyakorlásával kapcsolatban is. Az ilyen ügyek mögött meglapuló mögöttes szál is sokszor tartalmaz bosszúfaktort vagy egyszerűen olyan nemlétező sérelmekről van szó, melyekkel kapcsolatban a kérelmezőn kívül mindenki felismeri a nemlétező probléma természetét.

Birtokvédelmi jogalkalmazói tapasztalataim mellett immáron frissen végzett adatbiztonsági és adatvédelmi szakjogászként lenyűgözött, ahogyan a „kamerás szomszédkonfliktusok" kapcsán

végzett kutatómunkám során nagyon hasonló eseteket találtam a NAIH gazdag jogesettárában is. Nézzünk ilyen bosszúfaktort vagy mögöttes, meglapuló szálat néhány adatvédelmi jogesettel kapcsolatban!

Az első kiválasztott ügyben a beadványozó azzal fordult a hatósághoz, hogy egészségügyi szolgáltató munkáltatója telephelyein jogosulatlanul figyeli meg munkavállalóit, továbbá az ellátásra érkező betegeket.

Az eljárás lefolytatása során a területileg illetékes kormányhivatal arról értesítette a NAIH-ot, hogy a beadványozó a munkáltatója jogsértő tevékenységével kapcsolatban bejelentést tett, így világossá vált, hogy a beadványozónak elsődlegesen a munkaviszony nem megfelelő teljesítésével összefüggésben áll fenn jogsérelme.[1]

A második ügyben panaszos a szomszédja által a saját tulajdonára felszerelt kamerákat panaszolta, azonban az eljárás során a NAIH tudomást szerzett arról, hogy a panaszos folyamatosan zaklatja különböző magatartásokkal (szemét valamint galambtetemek átdobálása más tulajdonára, kerítés megrongálása) szomszédjait, köztük azt is, aki a kamerákat ingatlanjára felszerelte.[2]

A harmadik ügyben osztatlan közös tulajdonú területre került felszerelésre kamera, amely üzemeltetésének célja a panaszos szerint az ő személyének valamint családjának megfigyelése volt. A NAIH az eljárás során tudomást szerzett arról, hogy a panaszos és a panaszolt között közel 20 éve folyamatos családi viták állnak fenn.[3] (Az anonim jogesetet olvasva teljesen meggyőződésemmé vált, hogy korábbi ügyfeleim érintettek az ügyben.)A negyedik ügyben a panaszos azért kérte a NAIH eljárását, mert a telke határán lévő kutat szomszédja álláspontja szerint jogosulatlanul figyeli meg. Az eljárás során a NAIH feltárta, hogy a kutat mind a panaszos, mind a panaszolt megfigyeli kamerával, a háttérben egy régóta elhúzódó szomszédjogi vita áll.[4]

Az ötödik ügyben a panaszos azért tett bejelentést a rendőrséghez, mert állítása szerint szomszédja az osztatlan közös tulajdont képező kertrészt jogosulatlanul kamerával megfigyeli. Az eljárás során fény derült arra, hogy a kamera felszerelésére azért volt szükség, mert a panaszos szomszéd több módon is rongálta panaszolt tulajdonát, értéktárgyait, valamint több ízben veszélyeztette testi épségét.[5]

A hatodik ügyben panaszos állítása szerint több, a szomszédai házán elhelyezett kamerákkal készült videófelvételt (amelyen hang is

[1] NAIH-903/2022.
[2] NAIH-2660/2022.
[3] NAIH-3722/2022.
[4] NAIH-4831/2022.
[5] NAIH-5480/2022.

hallgató) továbbítottak panaszos munkáltatójának, továbbá a rendőrség részére. Maga a panaszos is elismerte ügyindító beadványában, hogy a felvételeket készítő szomszédaival több bírósági és rendőrségi eljárás is folyamatban van konfliktusaik miatt. [6]A szakdolgozatomhoz nyújtott segítség kapcsán a NAIH levelében megjegyezte, hogy „Az esetek jelentős többségében már magából az ügyindító iratból is világos a NAIH számára, hogy egy rossz szomszédi viszony vagy megromlott munkaviszony szolgál a panaszos bejelentése alapjául. Számos esetben előfordul, hogy az ügy során derül ki, hogy mind a panaszos mind a panaszolt „egymást kamerázza" a köztük fennálló konfliktusok miatt, így a jogsérelem alapja nem adatvédelmi hanem inkább polgári jogi vonatkozású."

Aki részt vett már bírósági panasznapon vagy például polgármesteri hivatal ügyfélszolgálatán pro bono jogsegély-szolgálaton, az tudja, hogy az emberek problémáinak nagy része nem éri el a jog ingerküszöbét, amelyik pedig elérni, azok közül sokban legalább annyi pszichológiai mint jogi ismeretre van szükségünk.

Adatvédelmi joggal foglalkozó szakemberként se felejtsük el soha a pszichológiai faktort: ami elsőre adatvédelmi problémának látszik, az az esetek nagy százalékában rejt egy másik konfliktust és nagyon valószínű, hogy az alapkonfliktus kapcsán meg fog jelenni a bosszúállás motívuma az ismertetett jogesetek kapcsán főként például szomszédkonfliktusok vagy munkavállaló-munkáltató konfliktusában is.

[6] NAIH-7173/2022.


EUR
HUF
ATM
ATM

ADATVÉDELMI ÖRÖKMOZGÓ MEGOLDHATATLAN FELADVÁNYOK A GDPR-BÓL

SZERZŐ: DR. DÓSA IMRE, JOGÁSZ, JOGI INFORMATIKUS, 2004. ÓTA FOGLALKOZIK INTENZÍVEN ADATVÉDELEMMEL

Az általános európai adatvédelmi rendelet megalkotói alapjogi hevülettel láttak neki munkájuknak.
A jogszabály szigorát általános fogalmakkal igyekeztek széleskörűvé tenni.

Egy lépésben kívánták letudni a rendkívül egyszerű - mondhatjuk úgy is, hogy a hétköznapi jogalanyok számára ingerküszöb alatti - és az egyes emberek számára áttekinthetetlenül komplex adatkezelések szabályozását. Az eredmény első látásra tetszetős volt. Sőt, az adatkezelések nagy dögkeselyűivel szemben kiszabott látványos bírságok látszólag megerősítették ezt. A cél érthető és méltánylást érdemlő volt. Sem új technikai vívmányokkal, sem bagatellizáló kivételekkel ne lehessen kibújni a szabályok alól. A GDPR, mint eszköz azonban ott tévesztett célt, hogy az “egy méret mindenkire jó” elve nem mérkőzött meg az ókori Rómában kidolgozott “omnis definitio in iure civili periculosa est” (minden definíció a polgári jogban veszélyes) gondolatával.

A GDPR-ból hiányzik az elvárhatóság elve. Ezen kívül felállítja azt a vélelmet, hogy az átlagos érintett képes megérteni az adatkezelés részleteit, összetettségét, majd a megértés alapján akár le is mond azon előnyökről, jogviszonyokról, melyek érdekében adatait kezelik az adatkezelők. Nagyon ritkán van alkalmunk ilyen tudatossággal találkozni. Sőt, sokan az adatvédelmi tudatosságot csodabogár tulajdonságnak tekintik. Ez persze nem véletlen. A GDPR (az alapjául szolgáló irányelv modelljét követve) nagyon egyszerű adatkezeléseket tekint mintának. Erre fűzte fel mind az adatkezelői kötelezettségek, mind az érintetteket megillető jogok rendszerét. Közben a bennünket övező világ - benne az adatkezelések - komplexitása annyit fejlődött, hogy a GDPR modellje minden adatkezelőt jogsértővé tett. Ez azért rontja jelentősen az adatvédelem hatékonyságát, mert többségünk vonakodva indul eleve vesztes csatába.

Kárhoztatható az adatkezelő, ha formális megfelelésre (vagy még arra sem) törekszik olyan adatkezeléseknél, melyek esetén bármikor megbüntethetik? Nehezen. Ezért érdemes áttekinteni néhány olyan példát, melyet mindenki használ, és amely esetén az adatvédelmi hatóságok a homokba dugják a fejüket, az "amit nem látok, azt nem bánom" elve alapján. Pedig fontos lenne, hogy hatóság is kimondja a GDPR alkalmazhatatlanságát. Szembesüljön a GDPR követelmények egyes esetekben mutatkozó gyakorlati képtelenségével, és azzal, hogy ez nem az adatkezelők, hanem a szabályozási logika hibája.

Spam szűrő

Mindenki használja, mert nélküle leállna az email forgalom. Működéséről az átlag érdeklődő annyit szokott tudni, hogy nagy nemzetközi szolgáltatóknál érdemes előfizetni, akik hatalmas levél forgalmat elemezve állapítják meg, hogy melyik levél spam.A szűrés szabályait titkolják, azért hogy a kéretlen levelek küldői ne tudják megkerülni azokat. Annyit azért lehet tudni, hogy számtalan esetben a szűrés nem csak egy adott tárgyú levélre vagy egy adott feladóra terjed ki, hanem akár a feladóval azonos levelező szerveren lévőkre is. Ha egy spam szűrő kiszűr egy levelet, akkor törli, de erről semmilyen értesítést nem küld. Hiszen ha küldene, a hibaüzenetek lavinája indulna el a hamisított feladók miatt.

A rövid leírás sejteti, miért nem lehet találkozni a spam szűrésre vonatkozó dokumentációkkal. Személyes adatok kezelése megvalósul? Igen. Születik automatizált döntés a levél célba juttatásáról? Igen. Érintheti jelentősen a címzett jogait, ha például álláspályázatot nyújtott be egy céghez? Igen. Biztosítható az érintett bármilyen adatvédelmi joga? Például a tájékoztatáshoz (beleértve az alkalmazott logikáról tájékoztatáshoz való jogot is), a tiltakozáshoz, a törléshez, a helyesbítéshez, az emberi felülvizsgálathoz való jogot? Rendre nem. Teljesíthető a harmadik országba történő adattovábbítással, adatfeldolgozói szerződéssel kapcsolatos adatkezelői kötelezettség? Ezek sem. Ennek okai könnyen beláthatók. Például a korlátozott tárolhatóság, majd a törlés nem alkalmazható, mert a szűrés hatékonyságát veszélyeztetné. A szűrő program üzemeltetője pedig saját céljára (a minták finomítására, gazdagítására) használja fel a vizsgált adatokat, tehát nem köt adatfeldolgozói megállapodást. Sérti a GDPR-t a spam szűrés? Minden elemében. Mondhatjuk, hogy felhagyunk a tömeges, jogellenes adatkezeléssel? Nem. Hogyan lépi át az adatvédelem a feloldhatatlan problémát? Létezéséről sem vesz tudomást. Nem lenne tisztességesebb kimondani, hogy világunknak vannak adatkezelési vakfoltjai, melyek szabályozására a GDPR alkalmatlan?

Szerintem igen. Sokan fellélegeznének. Persze csak azok, akik komolyan veszik az adatvédelmet, nem törődnek bele abba, hogy a GDPR politikai-hatalmi fenyegetés eszközévé legyen lezülleszthető.

Céges mobil

A GDPR 2. cikk (2) c) pontja kiveszi a jogszabály hatálya alól az adatkezelést, ha azt természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik. Az Európai Adatvédelmi Testület szerint ezt a kivételt nem szabad kiterjesztően értelmezni. Ezt az az értelmezést követi az adatvédelmi hatóságok gyakorlata is. Ezért a céges mobiltelefon nem vonható az idézett kivétel alá. Ha belegondolunk, vajon Európa-szerte mennyi adatkezelést érint ez a szemlélet? A korszerű készülékek híváslistái, sms tárai több száz hívás, üzenet adatait is megőrizhetik. Vessünk egy pillantást ennek adatvédelmi megfelelésére:

Abban egységes az adatvédelmi szakma, hogy a telefonszám önmagában azonosíthatja az előfizetőt, használót, ezért a telefonszám magában is személyes adat. Felhívtam egy céges mobilszámot. A híváslistába bekerült a hívószámom, a hívás ideje, időtartama. Utólag törölhető, de nem hallottam olyan készülékről, amelyen kikapcsolható lenne.

Mi ezen adatkezelés célja? Leginkább az, hogy visszahívhassanak. Ha pusztán ez a cél, a cégek, hatóságok hoztak olyan szabályt, hogy a visszahívással nem érintett hívásokat a munkavállaló haladéktalanul törölje? Aligha. Pedig a célját veszített adatkezelés jogellenes. Sérti a korlátozott tárolhatóság elvét. Tömeges, alapelvi sérelem történik. Ezért már vastagon fog a hatóság ceruzája a büntető csekken. Pedig még csak az elemzés elején tartunk. Az érintett az adatkezelésről semmilyen tájékoztatást nem kap. Ezért adatvédelmi jogait sem tudja gyakorolni, ami további alapelvi sérelemre vezet. Ha a telefon használója - valljuk be, többségünk ilyen - nem tudja memghekkelni a telefont, akkor a készülék a címjegyzéket a telefon operációs rendszerének megfelelő - tipikusan USA-ban letelepült - szolgáltató felhő alkalmazásában tárolja. Erre az adatfeldolgozásra akkor sem köthetnénk adatfeldolgozói megállapodást, ha szeretnénk. A munkáltatók mobil device management rendszerei sem támogatják a telefonok ilyen irányú adatvédelmi megfelelését. Abba is ijesztő belegondolni, egy telefon elvesztése esetén miként értesíthetők az adatvédelmi incidens kárvallottjai.

A mobiltelefon többi szolgáltatása, az üzenetek több platformos kezelése, az alkalmazások engedélyezhető adat összekapcsolásai, a helyadatok, fényképek kezelése mind-mind megoldhatatlan adatvédelmi rémálom. Ennek ellenére használjuk. Azok sem tolják el maguktól arcukon enyhe undorral, akik adatvédelmi tudatosságot élnek meg - például azért, mert adatvédelmi hatóságnál dolgoznak.

Van kiút?

Remélem a példák jól szemléltették, hogy a való élet, a három dimenziós világ adatkezeléseinek hétköznapjai milyen konokul ellenállnak a GDPR két dimenziós, papírra nyomtatott világának - és a sematikusan ezt követő egysíkú hatósági gyakorlatoknak. Ha ennek tudatalatti hátterét keressük, könnyű eljutni az “ingerküszöb alatti adatkezelés” fogalmához. Melyet nem az elméleti megfelelés, hanem a tömeges, háborítatlan használat tesz társadalmilag elfogadottá. A valóság azt mutatja, ez fontosabb, mint az elméleti adatvédelmi tisztaság. Ezt a jelenséget más jogágak már tudják kezelni. A korábban említett elvárhatósági mérce bevezetésével az adatvédelmi megfelelés iránti igény a valóban fontos irányokra, területekre fókuszálhatna.

EGY ATIPIKUS ADATKEZELÉSI JOGALAP TIPIKUS HELYZETBEN

SZERZŐ: DR. KOZÁK ANDRÁS LL. M. ADATBIZTONSÁGI ÉS ADATVÉDELMI SZAKJOGÁSZ

Az emberi élet, a testi épség és az egészség jogi és morális értelemben egyaránt a legfontosabb, legjobban preferált érték, melynek védelme az oktatási intézmények gyakorlatában az utóbbi időben jelentős mértékben felértékelődött a gyermekek, a legfiatalabb nemzedék tagjait fenyegető különféle veszélyek, így az étel- és gyógyszerallergia, valamint más egészségkárosító hatások miatt, melyek tekintetében a személyes adatok kezelése is releváns kérdésként vetődik fel nem utolsó sorban az egészségügyi adatok, mint különleges adatok révén.

Írásomban a gyermekek, a tanulók életének, egészségének védelme érdekében történő cselekvésekhez szükséges személyes adatkezelések tételes jogi, jogelméleti alapjait és a köznevelési intézmények gyakorlatával összefüggő kérdéseit kívánom taglalni, melyeket egy fiktív jogeset elemzésével is megvilágítok.

A GDPR [1] 6. cikk (1) bekezdésének d) pontja értelmében a személyes adatok kezelése jogilag megalapozott, ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

A joggyakorlat által vis maior vagy d) pontos adatkezelésnek nevezett személyes adatkezelés lényegi eleme a létfontosságú érdek, melynek helyes értelmezése a jogszerűség elemi feltétele. A létfontosságú érdek bármely természetes személy védelmét szolgálhatja, és nem lehet kiterjesztően alkalmazni: az élethez vagy az abból folyó testi épséghez, egészséghez való jog lényeges mértékű fenyegetése esetén alkalmazható. E jogalap jellegzetessége, hogy egyrészt az érintettre és az adatkezelőre egyaránt vonatkozhat, feltéve, hogy az adatkezelő természetes személy, és ezenkívül bármely élő ember védelmében alapítható rá személyesadat-kezelés, másrészt e jogalappal kell is élni, ha egy természetes személy életének a védelme válik szükségessé.

Létfontosságú érdek „az életet vagy testi épséget közvetlenül fenyegető veszély elhárításához fűződő érdek.”[2] A GDPR (46) preambulumbekezdése elvi éllel mutat rá arra, hogy az adatkezelést jogszerűnek kell tekinteni akkor, amikor az az érintett életének vagy más fent említett természetes személy érdekeinek védelmében történik.

[1]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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

[2] Jóri András (szerk.) (2018): A GDPR magyarázata. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft.154. old.

Más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre elvben csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető. A személyes adatkezelés néhány típusa szolgálhat egyszerre fontos közérdeket és az érintett létfontosságú érdekeit is, például olyan esetben, amikor az adatkezelésre humanitárius okokból, ideértve, ha arra a járványok és terjedéseik nyomon követéséhez, vagy humanitárius vészhelyzetben, különösen természeti vagy ember által okozott katasztrófák esetében van szükség.

Az óvodákban, iskolákban, kollégiumokban sajnos igen gyakran fordulnak elő olyan helyzetek, amikor a gyermekek, tanulók megsérülnek, balesetet szenvednek, vagy más módon veszélybe kerül az egészségük, fizikai épségük. Ennek dokumentálása a köznevelési intézmény obligát adatkezelési teendője.
Ha adott esetben az intézmény orvosának távollétében mentőt kell hívni a szülő haladéktalan értesítésével egyidőben, közömbös, hogy milyen forrásból származik a szülő elérhetőségi adata (meg nem adott mobiltelefonszám, titkosított vezetékes vonal, munkahelyi telefonszám stb.), mert a védendő érték elsődlegessége annulálja a személyes adat védelméhez fűződő jogi érdeket. S ez a helyzet a gyermek- és tanulóbaleseti statisztikák magas számaiból ítélve nem atipikum a napi gyakorlatban.

Különösen fontos ez az 1-es típusú diabétesszel élő gyermekek, tanulók nevelési-oktatási intézményben akut esetben történő ellátása vonatkozásában. A nemzeti köznevelésről szóló 2011. évi CXC. törvény 62. §-nak 2021. szeptember 1. napján hatálya lépő (1e) bekezdése elrendeli, hogy az intézményvezető az inzulinfüggő cukorbeteg gyermek, tanuló esetleges rosszulléte esetére az egészségügyről szóló 1997. évi CLIV. törvény előírásaival összhangban álló speciális ellátási eljárásrendet alakít ki.

A létfontosságú érdek által megalapozott adatkezelés esetén meg kell különböztetni az általános értelemben vett személyes adat és az egészségügyi adat, mint különleges adat kategóriáját.

A különleges adat - így az érintett testi vagy pszichikai egészségi állapotára, továbbá a számára nyújtott egészségügyi szolgáltatásokra (pl. kezelésekre) vonatkozó egészségügyi adat - csak akkor kezelhető jogszerű keretek között, ha az adatkezelés alóli tilalmat a GDPR feloldja

A GDPR 9. cikk (2) bekezdésének c) pontja feloldja az adatkezelési tilalmat azoknak a különleges adatoknak a vonatkozásában, amelyek esetében az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni. Ebben az esetben tehát az adatkezelés az érintett kifejezett akarata ellenére is megtörténik, mert az „érintett létfontosságú érdekében történő adatkezelés az érintetti hozzájárulás beszerzésének lehetetlenségét igényli."[3]

A különleges adatok létfontosságú érdek védelme céljából történő kezeléséhez a GDPR többletkövetelményt állít, nevezetesen az érintett jogi vagy fizikai cselekvőképtelenségét, melynek vonatkozásában kiemelendő, hogy a 14. életévét be nem töltött kiskorú személy megdönthetetlen jogi vélelem (praesumptio iuris et de iure) szerinti cselekvőképtelensége az óvodák és az általános iskolák tekintetében releváns, amelyhez hozzátehetjük, hogy a kiskorúsága miatt cselekvőképtelen személy jognyilatkozatának érvényességéhez törvényes képviselőjének hozzájárulása szükséges. Erre utal Jóri András értelmezése is. „A Rendelet[4] szabályozása abban az esetben kívánja az érintett hozzájárulását kiváltva megteremteni az az adatkezelés jogalapját, amikor az érintett ideiglenesen és/vagy fizikai állapotánál fogva válik cselekvőképtelenné. Ezért a szabályozás nem alkalmazandó akkor, ha az érintett - akár életkora, akár gondnokság alá helyezése miatt - korlátozottan cselekvőképes vagy cselekvőképtelen. Ilyen esetben az adatkezeléshez álláspontunk szerint a Ptk.[5] vonatkozó szabályai szerint vagy az érintett, vagy törvényes képviselője hozzájárulását kell beszerezni.
A rendelkezés helyes értelmezése nézetünk szerint az, amely szerint az a Ptk. 2:9. §-ában meghatározott cselekvőképtelen állapot esetében alkalmazható, vagyis akkor, ha az érintett »a jognyilatkozat megtételekor olyan állapotban van, hogy az ügyei viteléhez szükséges belátási képessége teljesen hiányzik«, így gondnokság alá helyezés nélkül is cselekvőképtelen."[6] [7]
A d) pontos adatkezelés alól tehát az egészségügyi adatok kezelése képez kivételt, melyből az következik, hogy a „GDPR 6. cikk (1) bekezdés d) pontja abban az esetben jelenthet jogalapot, ha az adatkezelés tárgya nem egészségügyi adat "[8], mert ekkor a GDPR 9. cikk (2) bekezdésének c) pontja alapozza meg a jogszerű adatkezelést.

Mindezek alapján - végezetül - a tárgyalt kérdéskört az alábbi kitalált jogeset elemzésével kívánom összegezni.

[3] Sepsi Tibor (2019): GDPR útikalauz adatkezelőknek. Budapest, Wolters Kluwer Hungary. 158. old.
[4] GDPR
[5] A Polgári Törvénykönyvről szóló 2013. évi V. törvény
[6] Jóri András (szerk.) (2018): A GDPR magyarázata. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft.187. old.
[7] Semmis annak a személynek a jognyilatkozata, aki a jognyilatkozat megtételekor olyan állapotban van, hogy az ügyei viteléhez szükséges belátási képessége teljesen hiányzik [Ptk. 2:9. § (1) bek.].
[8] Péterfalvi Attila-Révész Balázs-Buzás Péter (szerk.) (2021): Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary. 144. old.

Az erdei iskolai foglalkozáson részt vevő második osztályos tanuló gyógyszerallergiájáról a szülő nem nyilatkozott a programra való jelentkezés során. A tanuló a program második napján rosszul lett, orvost kellett hozzá hívni. A gyermek gyógyszerérzékenységéről a tanulót és családját már régóta ismerő, az osztályt az erdei iskolai programra elkísérő pedagógiai asszisztens tudott, így a gyermek édesanyját az iskolának meg nem adott közvetlen munkahelyi telefonszámán hívta fel, s megkérdezte őt e fontos egészségügyi adatról, melyet a kiérkező orvossal haladéktalanul közölt.

A tanuló gyógyszerallergiája az egészségi állapotával összefüggő, a személyes adatok különleges kategóriájába tartozó személyes adata, amely a tanuló egészségének, életének megóvása érdekében, tehát az érintett természetes személy létfontosságú érdekének védelmében lehet szükséges esetleges egészségügyi ellátása esetén, melyre a jogesetben foglalt történetben sor is került. Ennek a különleges adatnak a megismerése érdekében a szóban forgó, az adatkezelő iskola nevében eljáró személy olyan, a személyes adat általános kategóriájába tartozó adatot használt fel, amely az adott helyzetben elengedhetetlennek tűnt a gyermek egészségének, életének megóvása érdekében, noha a használt személyes adatot egyéb érvényes jogalap nem kezelhette volna.

A jogesetben szereplő tanuló egészsége, adott esetben az élete az, ami különleges jogi preferenciát élvez, mert létfontosságú érdeke, hogy ne kapjon olyan gyógyszert vagy kezelést, amely reá nézve egészségi állapotát súlyosítaná. Ehhez volt szükséges a továbbított információ. Az érintett polgári anyagi jogi értelemben vett kiskorúsága okán cselekvőképtelennek minősül, így nem volt nélkülözhető a szülő elérhetőségi adatának kezelése. Az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének d) pontjában foglalt vis maior jogalap volt.

Az ilyen és hasonló esetben, „ha az érintett hozzátartozójának a telefonszáma szükséges annak érdekében, hogy az érintett olyan egészségügyi adatát kérdezhessék meg tőle (például gyógyszerérzékenység vagy vércsoport), amely hirtelen rosszullét vagy baleset esetén lényeges információ lehet a mentőorvos vagy az orvos számára”[9], megalapozza a d) pontos adatkezelést.

Az adatkezelést a GDPR 30. cikk (1) bekezdésében foglalt adatkezelési tevékenységek nyilvántartásába fel kell venni.

[9] Péterfalvi Attila-Révész Balázs-Buzás Péter (szerk.) (2021): Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary. 144. old.

AZ ADATVÉDELMI SZAKMAI EGYESÜLET BEMUTATÁSA

SZERZŐ: DR. POKRÓCOS GYÖRGY, MÉDIAJOGI SZAKJOGÁSZ, ADATBIZTONSÁGI ÉS ADATVÉDELMI SZAKJOGÁSZ, AZ ADATVÉDELMI SZAKMAI EGYESÜLET ELNÖKE, DOKTORJELÖLT

Az Eötvös Loránd Tudományegyetem Jogi Továbbképző Intézet adatbiztonsági és adatvédelmi szakjogász és szakember képzés 2018/2019-es évfolyam tanulóiként egymás felkészülésének támogatása céljából hoztunk akkor létre egy hallgatói levelezőlistás e-mail csoportot, ahol szakmai vitákat folytattunk és osztottunk meg különféle adatvédelmet érintő tartalmakat.

A kezdeti kezdeményezés olyan sikeres volt, hogy a csoport néhány tagja 2021-ben elhatározta, hogy a tevékenységét egyesület formájában folytatja tovább. Így mindazokkal, akik a hallgatói csoportból velünk tartottak, nekikezdtünk az egyesület megalakításának. Időközben a nagy érdeklődésnek köszönhetően tagságunk kiegészült további szakemberekkel is.

Az egyesületünk 2022-ben került nyilvántartásba vételre a Fővárosi Törvényszék által, Adatvédelmi Szakmai Egyesület (röviden: ASZAKE) néven. Ettől kezdve megújult erővel és hivatalos formában folytatjuk azt, amit annak idején az iskolapadban elkezdtünk. Időközben elkészült a honlapunk (www.aszake.hu), Facebook oldalunk, illetve egy sportesemény szervezőinek meghívását elfogadva, személyesen is bemutatkoztunk a rendezvényen.

Egyesületünk azokból a célokból jött létre, amelyek a személyes adatok védelmét és biztonságát, valamint a közérdekű

és közérdekből nyilvános adatok, továbbá a közszféra egyéb információinak kezelésére vonatkozó kultúrát mozdítják elő, illetve fejlesztik.

Célunknak tűztük ki többek között, hogy országos szinten egységbe szervezzük az adatbiztonsághoz, adatvédelemhez, információszabadsághoz, valamint a közszféra egyéb információihoz akárcsak marginálisan is köthető területeken dolgozó szakemberek tevékenységét, illetve a társadalom tagjai részére az adatvédelmi tudatosság növelése érdekében felvilágosító, tájékoztató munka végzését is.

Feladatunkként vállaltuk az adatvédelmi tanácsadás és jogsegély nyújtását, beleértve a - az Európai Parlament és Tanács 2020/1828 irányelvével, valamint annak magyarországi átültetésével összhangban - a kollektív jogi érdekérvényesítést is; az adatvédelmi, adatbiztonsági és információszabadsággal kapcsolatos szakmai anyagok kidolgozását, tudományos tevékenységet és kutatást; nevelés, oktatás, képzés és szakmai továbbképzés szervezését és tartását; az adatvédelem, adatbiztonság és információszabadság népszerűsítését.

A "BELEFOGLALT CÉLOK" KONCEPCIÓJA A DIGI-ÜGY TÜKRÉBEN

SZERZŐ: DR. BÁRTFAI ZSOLT ADATVÉDELMI SZAKÉRTŐ, KÖZEL MÁSFÉL ÉVTIZEDES ADATVÉDELMI TAPASZTALATÁT RÉSZINT AZ ADATVÉDELMI BIZTOSOK MUNKATÁRSAKÉNT, RÉSZINT NAGYVÁLLALATI ÉS NEMZETKÖZI KÖRNYEZETBEN SZEREZTE, SZÁMOS CIKK ÉS EGY KÖNYVRÉSZLET SZERZŐJE

2022. október 20-án hirdette ki az Európai Unió Bírósága a C-77/21. sz. ügyben hozott ítéletét,[1] amelyet a Fővárosi Törvényszék előzetes döntéshozatal iránti kérelmére hozott a Digi Távközlési és Szolgáltató Kft-nek a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) azon elmarasztaló határozata ellen folyamatban lévő közigazgatási perében.

A döntés lényege, hogy az Európai Unió Bírósága (a továbbiakban: Bíróság) szerint nem ütközik a célhoz kötöttség GDPR-beli elvébe [GDPR 5. cikk (1) bek. b) pont], *„ha az adatkezelő egy tesztek elvégzése és hibák kijavítása céljából létrehozott adatbázisban rögzíti és tárolja a korábban más adatbázisban gyűjtött és tárolt személyes adatokat, amennyiben az ilyen további adatkezelés megfelel azon konkrét céloknak, amely célokból a személyes adatokat eredetileg gyűjtötték”*.

Ezzel a megállapítással a Bíróság szembe megy a NAIH azon megállapításával, amely szerint a „hibajavítási” célú adatkezelést az adatkezelés eredeti céljától („szerződés teljesítése”) elkülönülő célnak tekinti, azaz - a NAIH értelmezésében - két különböző célú adatkezelésről van szó.

Eltekintve a Bíróság ítélete (és a főtanácsnok indítványa[2]) egyes nehezen értelmezhető és még nehezebben érvényesíthető megállapításaitól, mind a Fővárosi Törvényszék végzését, mind a főtanácsnok indítványát, mind pedig a Bíróság ítéletét tanulmányozva az lehet az olvasó érzése, hogy e jogi fórumok annak lehetőségét keresték, hogy ne kelljen/ne lehessen a célhoz kötöttség elvébe ütközőnek tekinteni a Digi eljárását, nevezetesen azt, hogy egy technikai hiba esetén a hibajavítás céljából, eredetileg ideiglenesnek szánt külön adatbázisba másolta át az előfizetői egy bizonyos körének adatait.

[1]Lsd. az Európai Unió Bírósága: C-77/21. sz. ügy, Digi Távközlési és Szolgáltató Kft. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság ECLI:EU:C:2022:805, 30-31. bekezdés. Letöltve: https://curia.europa.eu/juris/document/document_print.jsf?mode=lst&pageIndex=0&docid=267405&part=1&doclang=HU&text=&dir=&occ=first&cid=1592568 (Utolsó letöltés: 2022. december 10.)

[2] Lsd. Priit Pikamäe főtanácsnok indítványa a C-77/21. sz. ügyben (ECLI:EU:C:2022:248), 59-60. bekezdés. Letöltve: https://curia.europa.eu/juris/document/document.jsf?text=&docid=256964&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=958094 (Utolsó letöltés: 2022. december 10.)

A kérdés tehát a körül forog, hogy mi tekinthető egy adatkezelésnek, az adatkezelési műveletek mely körét és milyen megfontolások szerint egységbe foglalva lehet egy adatkezelésről beszélni, illetve - másik oldalról - hol és hogyan lehet elhatárolni egymástól egy adatkezelő által egy adott folyamatban végzett adatkezelési műveleteket úgy, hogy azok két vagy több adatkezelésnek minősüljenek. A GDPR 2. cikk (1) bekezdése értelmében vett „adatkezelés" (azaz amire a GDPR hatálya és egyes rendelkezései vonatkoznak) ugyanis több mint az adatkezelési műveletek tetszőleges együttese, „adatkezelés" talán úgy határozható meg, mint adatkezelési műveletek egy bizonyos körének minimálisan az adatkezelési célok és jogalapok által homogén egységgé formált együttese (a kritériumok köre adott esetben bővíthető az adatkezelés időtartamával is). Az egyes adatkezelési műveleteket (GDPR 4. cikk 2. pont) önmagukban nem lehet külön adatkezeléseknek tekinteni, hiszen, ha így tennénk, akkor minden egyes adatkezelési művelethez külön jogalapot is kellene rendelni és - ami ennél praktikus szempontból is jelentősebb - külön adatkezelési tájékoztatót kellene készíteni és az érintettekkel megismertetni.

A Digi ügy tehát azt a kérdést feszegeti, hogy két látszólag különböző (különálló) cél mikor tekinthető és tekintendő egy célnak, aminek következtében az eredeti cél egy újabb céllal történő esetleges bővülése sem eredményez új „adatkezelést". Más szavakkal ez azt jelenti, hogy egy adott adatkezelési célú folyamatnak lehetnek ugyan „részcéljai", de ezeket a részcélokat az adatkezelés egészének célja magába olvasztja. Ilyen helyzet akkor állhat elő, ha ezek a részcélok szolgálják az adatkezelés egésze céljainak megvalósulását, nem pedig felváltják a korábbi célt.

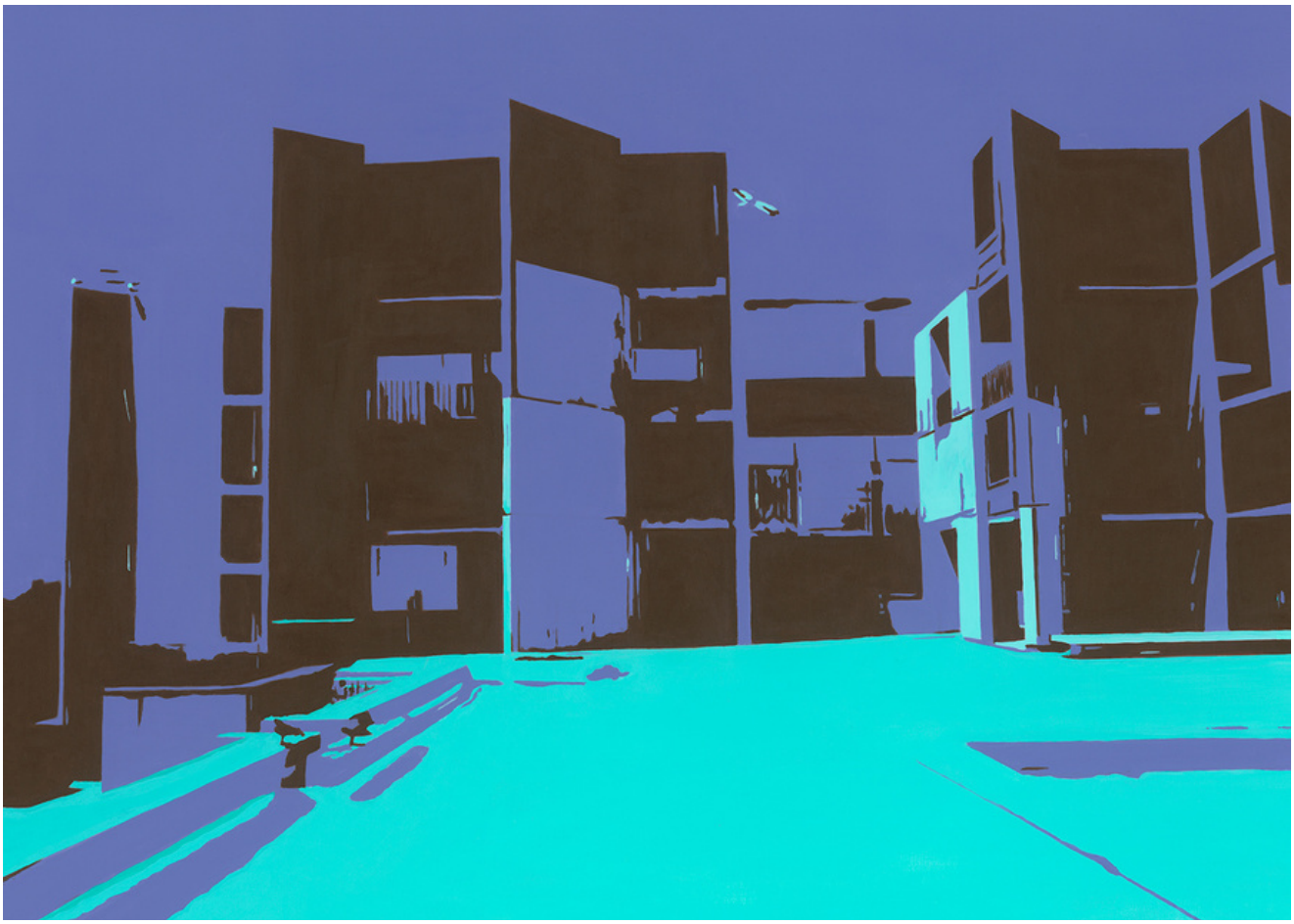
A Digi ügyben ez akként valósult meg, hogy a hibajavítási célú adatkezelés (tesztadatbázis létrehozása és felhasználása a szolgáltatás folyamatosságának biztosítására) az adatkezelővel szemben a GDPR-ban (5. cikke (1) bek. f) pont és 32. cikk) írt, az adatkezelés biztonságára vonatkozó kötelezettség teljesítését célozta és ezt nem lehet úgy tekinteni, mint amely új vagy elkülönült célt követ. Az adatbiztonság biztosítása érdekében teendő adatkezelési műveletek tehát egy olyan „belefoglalt célt" követnek, amely „belefoglalt cél" az adatkezelés eredeti céljában is benne van vagy abba anélkül belevonható, hogy az eredeti adatkezelés egy másik, a korábbitól eltérő adatkezelésbe fordulna át.

Nem hagyható figyelmen kívül az sem, hogy az adatkezelések az adatkezelő és az érintett jogviszonyának részei. Nyilvánvalóbb, hogy jogviszony fejlődése olyan intézkedések (és ezzel együtt járó adatkezelési műveletek) megtételét teszi, teheti szükségessé, amely intézkedésekre (adatkezelési műveletekre) az adott jogviszonyban nem feltétlenül kerül sor, de a jogviszony alakításának (alakulásának) „természetes" velejárói, így az adatok ilyen célú felhasználására akkor is sor kerülhet, ha ezt külön nem határozták meg az adatkezelés céljaként.

A „belefoglalt célok" koncepciója tehát az olyan célú adatkezelési műveletek megengedhetőségét jelenti, amely adatkezelési műveleteket anélkül meg lehet (adott esetben meg kell) tenni, hogy ehhez teljesíteni kellene mindazokat az adminisztratív feltételeket, amelyeket az adatkezelések bevezetésére, módosítására a GDPR egyébként előír (pl. külön jogalapot keresni, külön adatkezelési tájékoztatót készíteni[3]).

Ha tehát azt szeretnénk meghatározni, hogy milyen adatkezelési műveleteket lehet az adatkezelés eredeti céljába foglaltnak tekinteni,akkor - a Digi ügyben már említett eseten (azaz az eredeti célt támogató, kiszolgáló adatbiztonsági intézkedésként végrehajtott adatkezelési műveleteken) túl - ilyen eset még az adatoknak az adott adatkezeléssel kapcsolatos jogi igények érvényesítése érdekében (igényérvényesítési céllal) történő felhasználása is (azaz ahhoz, hogy egy jogviszonyban akár az adatkezelő, akár az érintett igényt érvényesítsen a másik féllel szemben, nem szükséges külön célt és ehhez jogalapot azonosítania, mert a jogviszony léte feljogosítja bármelyik felet az adatok igényérvényesítési célú felhasználására is).

[3] A Digi ügyben a főtanácsnok indítványa értelmezi olyan módon a GDPR-t, ami alapján - a véleményt szó szerint véve - az adatkezelő minden új adatkezelési művelet előtt köteles lenne tájékoztatni az érintetteket az „új célú" adatkezelésről, pontosabban új célú adatkezelési műveletekről. Egy ilyen értelmezés azonban nem életszerű.



BLOKKLÁNC, OKOSSZERZŐDÉSEK ÉS ADATVÉDELEM

SZERZŐ:DR. ESZTERI DÁNIEL JOGÁSZ, A NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG INCIDENSBEJELENTÉSI OSZTÁLYÁNAK VEZETŐJE, AZ EÖTVÖS LORÁND TUDOMÁNYEGYETEM JOGI TOVÁBBKÉPZŐ INTÉZET ÉS A NEMZETI KÖZSZOLGÁLATI EGYETEM MEGBÍZOTT OKTATÓJA ADATVÉDELMI JOGBÓL, 2015-BEN PH.D. FOKOZATOT SZERZETT A PÉCSI TUDOMÁNYEGYETEMEN A VIRTUÁLIS TULAJDONJOGRÓL ÍRT DISSZERTÁCIÓJÁVAL

1. **A blokklánc alapú adatkezelés**

A blokklánc egy adatok tárolására és kezelésére szolgáló rendszer, az úgynevezett elosztott főkönyvi technológiák egyik képviselője. Olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják. A hálózaton nincs alá-fölé rendeltségi viszony az egyes gépek között, amelyek úgynevezett csomópontokként (angolul: node-okként) funkcionálnak és mindegyik csomópont összeköttetésben áll az összes többivel. Az ilyen típusú hálózat előnye, hogy egy csomópont kiesése semmilyen fennakadást nem okoz a rendszer működésében, feladatait azonnal át tudják venni másik csomópontok.

A blokklánc alapú hálózatokon az adatok tárolása az ún. blokkokban történik. Ezek olyan adattárolási egységek, amelyekben bármilyen információ eltárolható, az adott blokklánc létrehozásának céljától függően.

Az információkat tartalmazó blokkok láncszerűen, utólag megváltoztathatatlanul kapcsolódnak egymáshoz, ami annyit jelent, hogy az újabb blokkokat és a bennük lévő új adatokat mindig csak a lánc végére lehet felfűzni.

A rendszer az egyes felhasználók „digitális aláírásaival” látja el a blokkokban tárolt adatokat és azokkal végzett tranzakciókat, műveleteket, és ez alapján ítéli meg, hogy pl. adott blokkban tárolt adathalmaz feletti rendelkezés, vagy hozzáférés joga kit illet meg.

A láncszerűen felépülő és így egyre növekvő adatbázishoz az újabb adatokat újabb blokkokban adják hozzá. A blokkokban tárolt adatokkal végzett valamennyi művelet naplóját is az egyes blokkokban tárolják, a tranzakciók összefoglalása pedig az úgynevezett Merkle-fát eredményezi. Ezen műveletek naplóját nevezzük összefoglaló néven „blokktörténetnek”.

A csomópontok feladata az is, hogy a blokkokban tárolt adatokkal végzett adatkezelési műveletek hitelességét algoritmikus úton ellenőrizzék. A művelet jóváhagyása során azt ellenőrzik, hogy a tranzakció digitálisan megfelelően alá van-e írva a műveletet indítványozó felhasználó által, és van-e bármilyen hiteles előzménye a blokkláncon. Amennyiben a csomópontok (vagy előre meghatározott számú csomópont) jóváhagyják a műveletet, úgy az rögzítésre kerül a blokkban, ami ezentúl megmásíthatatlanul hozzákapcsolódik a teljes lánchoz.

A blokkláncot legegyszerűbben egy olyan adatkezelési technológiának írhatjuk le a fentiek alapján, amely az adatok kezelését egy közös, elosztott hálózaton teszi lehetővé, amely központi ellenőrző szerv felügyelete nélkül is működőképes. Az adatokkal végzett műveletek hitelesítése a hálózaton algoritmikus alapú önellenőrző mechanizmusokkal biztosított.

2.Okosszerződések a blokkláncon

Nick Szabo volt az, aki először - az „okos szerződés” koncepcióját és kifejezését használva 1996-ban az elosztott hálózat adatkezelési műveleteinek automatizálását írta le.

Szabo szerint az okos szerződés olyan szerződés, amely automatikusan megvalósul, ha a korábban meghatározott feltételek teljesülnek, így a szerződés gyakorlatilag „önmagát teljesíti” és ezért megszeghetetlen. A szerződés teljesítését, biztonságát és megszeghetetlenségét egy számítógépes hálózat biztosítja, amelyikben a felek azt elkészítették, ezért nincs szükség a hitelesítéshez harmadik fél (pl. ügyvéd) közreműködésére.

Amint az a gyakorlatban már látható, a blokklánc egy teljesen életképes technológia az okosszerződéses alkalmazások futtatásához: a felhasználók részére automatikus szerződések megkötésének lehetőségét a blokklánc-alapú platform, az Ethereum vezette be először. Lényegében a hálózaton futó program automatikusan végrehajt egy bizonyos döntést, ha a szükséges feltételek teljesülnek.

Az okosszerződések esetében is a csomópontok hitelesítik a folyamatot és az azzal összefüggésben kezelt adatokat, így például egy adásvételnél a szerződő felek számlaszámait, az összeget, az időpontokat (pl. határidő), egyéb feltételeket, de akár más személyes adatokat (pl. név) vagy szöveges egyéb információkat (pl. közlemény) is rögzíteni lehet. A szerződés létrejöttét ugyanúgy a csomópontok hitelesítik algoritmikus módon, az adatok és mozgásuk naplója

pedig megváltoztathatatlanul rögzül a blokkláncban.

Az automatizálásért felelős okosszerződés alkalmazás a hálózat minden résztvevője számára elérhető, hozzáférhető és használható. Az okosszerződések fő célja a legtöbb helyzetben a blokkláncon lévő tranzakciók automatizálása és hitelesítése, ha bizonyos feltételek teljesülnek.

3.A GDPR-nak való megfelelés kérdése

A blokklánc-alapú adatkezelés komoly kihívást okozhat a GDPR (az Európai Unió adatvédelmi rendelete) előírásainak való megfelelést illetően.

Például a célhoz kötöttség elve alapján a személyes adatokat csak meghatározott, egyértelmű és jogszerű célból szabad gyűjteni, és azokat nem szabad az említett célokkal összeegyeztethetetlen módon kezelni. Az adattakarékosság elve szerint pedig a kezelt személyes adatoknak megfelelőnek és relevánsnak kell lenniük az adatkezelés céljai szempontjából és az e célokkal kapcsolatban szükségesre kell korlátozódniuk. Mindkét elv tiltja a túlzott, felhalmozott, szükségtelen adatok kezelését.

A blokklánc működésének egyik alapelve az, hogy az összes adat megőrzési időkorlát nélkül tárolódik az adatbázisban, a velük eszközölt, pl. okosszerződéses műveletek naplójával együtt. Az adatok és azokon végzett adatkezelési műveletek naplója felfűződik a régebbiekre az integritás és a biztonság garantálása érdekében. Az adatokat és tranzakciónaplókat határozatlan ideig tárolják a rendszerben, abból a célból, hogy pontosan nyomon lehessen követni az egyes adatkezelési műveletek és az adatok sorsát. Minden csomópont továbbá az adatbázis teljes másolatát tárolja önellenőrzési célokból. Első látásra ezek a jellemzők ellentétben állnak a GDPR fent említett alapelveivel.

A blokklánc-alapú adatkezelés jogszerűségének megítéléséhez azonban egy fontos előkérdés, hogy az ilyen típusú technológia alkalmazása egyáltalán kompatibilissé tehető-e az bármiféle adatkezelési céllal.Az alapelveknek való megfelelés szempontjából tehát meg kell vizsgálni, hogy a személyes adatok ilyen típusú kezelése (pl. adatok határozatlan ideig történő tárolása a láncban) összeegyeztethető-e bármilyen legitim céllal. Vannak olyan típusú adatkezelések, amelyek alapvetően nem alkalmasak erre. Például egy az érintett hozzájárulásán alapuló adatkezelés (pl. egy direkt marketing célú hírlevél-küldő szolgáltatás)

szinte soha sem lesz ilyen, mivel a GDPR szerinti, a személyes adatok törlésére vonatkozó kötelezettség teljesítése a hozzájárulás visszavonása esetén nem teljesíthető.

A jogszabályi kötelezettség teljesítésén alapuló adatkezelés, például ingatlan-nyilvántartások vagy állami levéltárak vezetése esetén azonban könnyebb a helyzet, hiszen ezeknek az adatbázisoknak a célja az összes személyes adat és az azokkal végzett valamennyi művelet megőrzése és eltárolása, archiválása. A közérdekű archiválási cél tehát könnyebben állhatja ki az alapelvi megfelelés próbáját blokklánc alkalmazása esetén. Egy adott blokklánc-alapú adatkezelés ezért csak eseti alapon értékelhető a jogszerűség és a GDPR-megfelelés szempontjából.

4. Megoldások az adatvédelmi megfelelés érdekében

Mielőtt személyes adatokat kezelésére használnánk a blokkláncot, pontosan tisztáznunk kell, hogy milyen feladatra használjuk fel az adatokat, és ezért korlátozni kell a felhasznált adatok körét a cél szempontjából releváns adatokra. Ez az ún. beépített adatvédelem elvének alkalmazása szempontjából is kulcsfontosságú követelmény.

Habár a személyes adatok törlésének lehetősége jelenti a legfőbb problémát egy blokklánc alapú adatkezelésnél, ennek kivitelezésére is léteznek már - igaz, inkább kísérleti szinten - megoldások. Ezek szerint a törlést az adathoz való hozzáférés blokkolásával, ellehetetlenítésével lehet a gyakorlatban kivitelezni egy blokkláncban. Erre a vonatkozó irodalom az adathoz való hozzáférést biztosító privát kulcs törlését (elégetését) hozza megoldásként. A hozzáférési kulcs törlésével az adat megmarad a blokkláncban, azonban az ahhoz való hozzáférési/olvashatósági lehetőség a dekódoláshoz való kulcs hiányában végérvényesen elveszik. A kapcsolat megteremtéséhez való lehetőség végleges törlése tehát a GDPR szerinti „elfeledtetéshez való jog” érvényesítését szolgálhatja a blokkláncon.

Ezzel egybevágó vélemények szerint a megfelelő technológiával titkosított olyan személyes adatok, amelyekhez senkinek sincs hozzáférése, nem tartoznak többet a GDPR hatálya alá, kvázi elveszítik a rendelet által jelentett jogi garanciákra való érdemességüket. A titkosítási technológia elavulása és a potenciális újbóli hozzáférés veszélye azonban újraéleszti a jogi védelmet.
Egy másik lehetőség az ún. „felejtő” vagy „rövidített” blokkláncok koncepciója.

Egy ilyen alapon működő adatbázisban a hozzáférési kulcsokat tartalmazó blokkokat folyamatosan újrakalibrálják (hashelik) egy bizonyos, előre meghatározott idő után, így a hozzáférési lehetőség is elveszik. Ez tipikusan olyan célú adatkezeléseknél lehet jó megoldás, ahol az adatokat bizonyos idő után automatikusan törölni kellene.

Végül meg kell említeni a személyes adatok „láncon kívüli" („off-chain") tárolási lehetőségét, ahol a személyes adatokat nem magában a blokkláncban, hanem egy elkülönült adatbázisban tárolják, de kezelésük hash-kulcsok használatával összeköttetésben áll a háttértechnológiát adó alapadatbázissal, amely már blokklánc-alapon működik. A láncon kívüli adatokból való törléssel az alap blokklánc nem változik, csak az azzal összekötött, személyes adatokat is tartalmazó ráépülő adatbázis. Ezzel a megoldással kiküszöbölhető a blokklánc megváltoztatásának nehézsége és a személyes adatokat megillető védelem is érvényesül.

5. Összegzés

Mint láttuk a blokklánc egy rendkívül stabil adatkezelési megoldás, amely bármilyen személyes adat, információ kezelésére szolgálhat.

A technológia azonban működési alapelveit tekintve számos adatvédelmi kérdést felvet, amelyekre még nem léteznek megfelelően kiérlelt megoldások, habár azokkal folyamatosan kísérleteznek.

Fontos ezért, hogy az adatvédelmi megfelelés vizsgálata elsődleges legyen az olyan blokkláncok fejlesztésénél és tervezésénél, amelyek egyben személyes adatok kezelésére is szolgálnak, főleg ha okosszerződések megkötésére is használják azt. Az ilyen típusú, még nem kellően kiforrott, új technológiáknál ezért már előzetesen, annak használata előtt fontos elvégezni a GDPR által is előírt adatvédelmi hatásvizsgálatot.

Források:

-Bacon, J. et. al. (2017) Blockchain Demystified. Queen Mary School of Law Legal Studies Research Paper No. 268/2017
-Buterin V. (2013): A Next-Generation Smart Contract and Decentralized Application Platform. Online: https://ethereum.org/en/whitepaper
-Európai Központi Bank. (2017) How could new technology transform financial markets? 19th April 2017. Online: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html
-Finck, M. (2019) Blockchain and the General Data Protection Regulation. European Parliamentary Research Service, PE 634.445.
-Giuseppe Ateniese - Bernardo Magri - Daniele Venturi - Ewerton Andrade: „Redactable Blockchain or Rewrtinig History in Bitcoin and Friends" in Proceeding of the 2nd IEEE European Symposium on Security and Privacy - EuroS&P 2017, eprint.iacr.org/2016/757.pdf
-Győrfi András et .al.: Kriptopénz ABC. Budapest, HVG Könyvek, 2019.
-Hossein Kakavand - Nicolette Sevres De Kost - Bart Chilton: The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. SSRN Electronic Journal, (2017). Online: http://dx.doi.org/10.2139/ssrn.2849251
-Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. Masaryk University Journal of Law and Technology, Vol. 13. No. 2. Online: https://doi.org/10.5817/MUJLT2019-2-8
-Nemzeti Adatvédelmi és Információszabadság Hatóság: Állásfoglalás a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, Online: https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf
-Nick Szabo: „Smart Contracts: Building Blocks for Digital Markets" 1996 (részlegesen átdolgozva: 2018), www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf
-Rosanna Mannan - Rahul Sethuram - Lauryn Younge: „GDPR and Blockchain: A Compliance Approach" European Data Protection Law Review 3/2019.
-Schrepel, T. (2021): Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach. European Commission. Online: https://ssrn.com/abstract=3947174
-Xing, B. és Marwala T. (2018): The Synergy of Blockchain and Artificial Intelligence. Online: http://dx.doi.org/10.2139/ssrn.3225357

INTERJÚ DR. PÉTERFALVI ATTILÁVAL

A FŐSZERKESZTŐ KÉRDEZ CÍMŰ ROVAT

dr. Péterfalvi Attila András: jogász, a NAIH elnöke, egyetemi oktató

ICSA: A NAIH feladatai közül mit tart 2023. év legnagyobb kihívásának, és miért?

PA: A legnagyobb kihívásnak a következő évre az adatvédelem területén az Európai Adatvédelmi Konferencia megszervezését tartom. Magyarország először 2006-ban volt helyszíne a Konferenciának, majd 10 évvel később 2016-ban ismét mi rendeztük meg a találkozót. Nagy megtiszteltetés a magyar hatóság számára, hogy 2023-ban újból Budapest ad otthont ennek a fontos eseménynek.

Ezek a konferenciák zártkörű rendezvények, hozzávetőlegesen 100 fő részvételével. 2016-ban Giovanni Buttarelli - az akkori európai adatvédelmi biztos - vetette fel, hogy hasznos lenne az érdeklődő adatkezelők és szakemberek számára a konferenciához kapcsolódóan egy nyílt napot szervezni. Miután eddig ez a felvetés nem valósult meg, arra gondoltunk, hogy mi most megvalósítjuk és jövőre az érdeklődők számára szervezünk egy nyílt napot, melyre olyan érdekes témákat tervezünk, mint pl. a mesterséges intelligencia adatvédelmi vonatkozásai, illetve az adatvédelmi tisztviselők szerepe.

Emellett a hatóság szempontjából kihívás lesz az információszabadság területén a megváltozott átláthatósági szabályok alkalmazása és a hatóságot megillető új hatósági jogkör gyakorlása. Ezek a szabályok az uniós pénzekhez való hozzáférés miatt a jogállamisági eljárás lezárása érdekében kerültek beépítésre az információs önrendelkezési jogról és az információszabadságról szóló törvénybe (Infotv).

Egyébként az a most megvalósult módosítás, hogy a NAIH kapjon hatósági jogkört bizonyos információszabadságot érintő esetekben nem újkeletű, hiszen erre korábban már én is tettem javaslatot (bírságolási jogot nem indítványoztam, hiszen a költségvetési szervek esetében a bírság a költségvetés egyik zsebéből kerül át a másikba, nem jelent új bevételt). Én azt indítványoztam, hogy azokban az esetekben, amikor jogszabály kötelezi az adatkezelőt a közzétételre és ennek nem tesz eleget, akkor hatósági jogkörben lehessen elrendelni az adatok nyilvánosságra hozatalát. A bírság maximális összege ötven millió forint lehet, amely eltér az Infotv. alapján az adatvédelmi jogsértés estén kiszabható bírság maximális összegétől, amely húszmillió forint lehet. Jó lett volna ezeket egységesíteni.

A napokban zárul az az európai uniós információszabadság projekt, amelynek kedvezményezettje a NAIH, a tárgya az volt, hogy az első vonatkozó törvény hatályba lépése - 1992 - óta feltérképezze az információszabadság érvényesülését Magyarországon. A projekt keretében külső szakértők közreműködésével négy területen vizsgáltuk a nyilvánosság érvényesülését: központi kormányzás, önkormányzatok, közpénzek átláthatósága és az információszabadság érvényesüléséért felelős intézmények.

A tapasztalatokat összefoglaló tanulmány alapján a NAIH a nyilvánosság szélesítésére vonatkozó javaslatokat is meg fog fogalmazni, melyek érinthetik a hatályos jogszabályi rendelkezéseket. Elmondható, hogy bennünk is megfogalmazódott javaslat olyan központi interneten elérhető felületre, amelyen az érdeklődők számára könnyen hozzáférhetővé tehetők a legfontosabb közérdekű és közérdekből nyilvános adatok, beleértve a közpénzek felhasználására vonatkozó adatokat és szerződéseket is. Tulajdonképpen ez most a közadattárra vonatkozó rendelkezések hatályba lépésével többé-kevésbé meg is valósul. Az átláthatósági eljárásra vonatkozó szabályok hatályba lépésével fejest ugrunk az ismeretlenbe, hiszen nem tudjuk hány ilyen hatósági eljárásunk lesz, melyre nagyon rövid, 45 napos határidők vonatkoznak és ezekkel a döntésekkel szemben jogorvoslatként bírósághoz lehet fordulni.

Emellett az európai uniós jogalkotásban is születtek olyan jogszabályok, amelyek a jövő évben alkalmazandóvá válnak és új feladatot adnak a hatóság számára.

2023. májusában lesz 5 éve, hogy a GDPR alkalmazása elkezdődött. Érdemes áttekinteni a tapasztalatokat, hogy esetleg szükséges-e a rendelet módosítása.

Nem várható változtatás a GDPR rendelkezéseiben, ugyanakkor az megállapítható, hogy a tagállami jogalkalmazás során lehetnek eltérések, melyek akár jogértelmezési különbségekből is eredhetnek. Gondolok itt például arra a magyarországi bírósági döntésre, amely elvitatta a NAIH hatáskörét abban, hogy hivatalból elrendelje a jogellenesen kezelt adatok törlését. Az Európai Adatvédelmi Testület értetlenül állt a döntés előtt, a Bizottság képviselője pedig kötelezettségszegési eljárást helyezett kilátásba. Az ügy végére az Alkotmánybíróság tett pontot azzal, hogy megállapította: a bíróság korlátozta a NAIH jogkörét, ugyanis hivatalból is el lehet rendelni a jogellenesen kezelt adatok törlését. A konkrét ügyben a bíróság helyben hagyta a hatóság határozatának azon részét, amelyben megállapította, hogy az adatkezelő jogellenesen gyűjtött kb. 600.000 aláírást, nem volt megfelelő a tájékoztatás és a bírság összegével is egyetértett, azonban úgy ítélte meg, hogy kérelem hiányában hivatalból nem rendelhető el az adatok törlése. Az Európai Bizottság az eljárási szabályokat abból a szempontból értékeli, hogy biztosított-e a GDPR egységes alkalmazása.

ICSA: Tervez-e a hatóság oktató anyagokat, témaspecifikus tájékoztató anyagokat jövőre?

PA: A jogpropaganda számunkra nagyon fontos, de a különböző tájékoztató anyagok készítése már kapacitás kérdése. Természetesen igyekszünk minél szélesebb körben tájékoztatást adni mind az adatvédelem, mind pedig az információszabadság területén. Az új hatáskörünket illetően is készülnek majd tájékoztató anyagok.

Megjelentettünk tájékoztatást például azzal kapcsolatban, hogy az átalakuló egyetemekre vonatkozóan hogyan kell alkalmazni a nyilvánosság szabályait. Ahogyan korábban említettem hozzáférhető lesz az információszabadság projekt záró dokumentuma is.

Tekintettel arra, hogy a GDPR értelmezésére a tagállami adatvédelmi hatóság nincs feljogosítva, így az adatvédelem területén a lehetőségeink korlátozottak. Az Európai Adatvédelmi Testület által elfogadott iránymutatásokat, dokumentumokat azonban a NAIH honlapján közzétesszük, ezek a legtöbb esetben magyar nyelven is elérhetőek.

Ahol nagyobb mozgásterünk van, azok az adatkezelések, amelyek tagállami kompetenciába tartoznak.

Így például a választásokkal kapcsolatosan adtunk ki olyan tájékoztatást, amelyben jeleztük az adatkezelők felé, hogy ezt fogjuk számon kérni.

Emellett konkrét ügyekben hozott határozatokat, állásfoglalásokat is közzéteszünk általában anonimizálva, illetve azonosító adatokkal együtt, amennyiben szankcióként ezt a határozat elrendeli. Ugyanezt megtesszük információszabadság ügyekben is.

Fontosnak tartom megemlíteni ebben a körben, hogy a hatóság éves beszámolója is elérhető a honlapunkon. Külön érdekességként emelném ki, hogy a közeljövőben - 2023. év elején - egy animációs filmmel is készülünk, melyben s közérthetően magyarázva szeretnénk a nyilvánosságot tájékoztatni adatvédelemről és információszabadságról.

ICSA: Hogyan készül a hatóság a technológia változásokra újdonságokra? (gondolok itt pl. AI, Blokklánc technológia)

PA:Mint ahogyan korábban említettem a GDPR hatálya alá tartozó adatkezeléseknél a tagállami adatvédelmi hatóság mozgástere szűkebb. A rendelet bevezette az “egyablakos ügyintézést”. Amennyiben a tech-cég adatkezelése ezen illetékességi szabály körébe tartozik és az eljáró vezető hatóság nem a NAIH, általában minden olyan ügyben bejelentkezünk úgynevezett „érintett hatóságként”, amely új technológiához kötődik vagy közösségi médiához kapcsolódik, mert a döntés meghozatalának részesei kívánunk lenni. Ezt az eljárásban a határozat-tervezet véleményezése teszi lehetővé számunkra. Gondolkodunk egyébként abban is, hogy meghívunk olyan gazdasági szereplőket, akikkel közvetlenül átbeszélhetjük a technikai újdonságokat, lehetőséget adva arra, hogy bemutathassák hol állnak a fejlesztésekkel és azok milyen adatvédelmi kérdéseket érintenek. A mesterséges intelligenciával kapcsolatban a legutóbbi nemzetközi adatvédelmi konferencián az Európai Bizottság egyik képviselője arról beszélt, hogy egyedül a tagállami adatvédelmi hatóságok azok, amelyek rendelkeznek arra nézve hatáskörrel, hogy a mesterséges intelligencia működését ellenőrizni tudják. Ez azért fontos, mert a mesterséges intelligencia öntanulása miatt nem elegendő a bevezetése előtti hatásvizsgálat, hanem rendszeresen, időszakonként visszatérően kell ellenőrzi a működését, adatkezelését.

Fontos, hogy hogyan tudjuk bevonni, felhasználni, a javunkra fordítani ezeket a technológiákat úgy, hogy közben ne legyünk kiszolgáltatottak és ne csökkenjen a magánszféránk.

ICSA: Mint magánember, mennyire hallja meg a köz hangját, mennyire olvas a híreknek utána? Mennyire fogékony véleményekre, tartalmakra?

PA: Muszáj. Nem tudom szétválasztani az énjeimet: a magánembert, a hatóság elnökét és az oktatót. Nagyon izgalmasnak is tartom az adatvédelmet és az információszabadságot, hiszen a társadalmi létünk minden elemét, mozzanatát átfogják, így nem is tudnék nem figyelni ezekre a tartalmakra.

Volt már több olyan hír is, amelyre azt mondtam, hogy hivatalból nézzünk utána, nézzük meg mi is ez. A közelmúltban pont egy olyan mesterséges intelligenciáról olvastam, amely verset írt. Nagyon érdekes volt, hogy hogyan teszi ezt, mi az eredménye. Ezek magánemberként is nagyon érdekelnek.

ICSA: NAIH elnökeként, több évi oktatóként- mi motiválja ilyen hosszú időn keresztül?

PA: Az adatvédelem, információszabadság területével igen rég óta foglalkozom, az 1980-as évek vége óta. Ha jól emlékszem 1988-ban jelent meg az első írásom ebben a témában. Izgalmas terület, rengeteg újdonsággal, és ez önmagában motiváló. Rendszeresen részt veszek konferenciákon előadóként és több egyetemen is tanítok.

Az oktatás természetes közeg a számomra, hiszen a családomban szinte mindenki pedagógus volt, és ha az ember fiatalok között mozog, az fiatalon is tartja.

(Ezt némiképp árnyalja a Covid járvány miatti távoktatás, amely önmagában rengeteg adatvédelmi, adatbiztonsági kérdést vetett fel.)

Azért sem lehet megunni, mert mindig jönnek újabb kérdések, kihívások. A hatóság területén is folyamatos a változás: új feladatok, hatáskörök, az ember nem tud unatkozni.

A kiadvány aktív támogatója a kortárs művészetnek!

No.1. magazin képeinek alkotója: **WEILER PÉTER**

Képek forrása: www.peterweiler.com

2022 DECEMBER | NO.1.

DATAPATRON