Fotó: Bv. fotó

Nagyné Takács Veronika

Információbiztonság és adatvédelem – Szabályozási tapasztalatok a Büntetés-végrehajtási Szervezetnél

Information security and data protection – Regulatory experiences in the Prison Service

Az információbiztonsági és adatvédelmi jogszabályokban előírt kötelezettségek teljesítése számos feladatot telepített a közigazgatási szervekre, így a büntetés-végrehajtási szervezetre is. Ezek egy része adminisztratív – szabályozási és nyilvántartási – feladatokat jelentett, amelyek teljesítése során értelmezési és gyakorlati kérdések is felmerültek. A tanulmány néhány, információbiztonsággal és adatvédelemmel összefüggő szabályozási és nyilvántartási kérdést tekint át, megosztva a büntetés-végrehajtási szervezet általi végrehajtásból származó gyakorlati tapasztalatokat is.

Kulcsszavak: információbiztonság, adatvédelem, szabályozás, nyilvántartás

The fulfillment of obligations under information security and data protection legislation has entrusted a number of tasks to public administrations, including the administration of the prison service. Some of these involved administrative - regulatory and record-keeping - tasks, which involved construing and practical issues. The study reviews some regulatory and record-keeping issues related to information security and data protection, sharing practical experience from the implementation by the prison service.

***Keywords*:** *information security, data protection, regulation, record keeping*

Bevezető

A 2013-ban született információvédelmi és az Európai Unió adatvédelmi reformja következtében 2018-2019-ben több lépésben módosult adatvédelmi jogi szabályozás értékelése, értelmezése tárgyában számos tanulmány született és a téma – mindkét esetben – a napi közbeszédben is jelentős figyelmet kapott.

Jóval szűkebb a végrehajtást segítő módszertani javaslatok és a végrehajtási tapasztalatok megosztásának irodalma; jelen tanulmány egy speciális szempont alapján és egy konkrét szervezet nézőpontjából mutat be gyakorlati tapasztalatokat, remélve, hogy a leírtak mások számára is hasznosítható ismereteket nyújtanak.

A speciális szempont az információbiztonsági és az adatvédelmi jogszabályokból fakadó szabályozási és az ezzel szoros összefüggésben lévő nyilvántartási kötelezettségek teljesítésének feltételei és módja. A tanulmány első része az Ibtv.-ből fakadó adminisztratív feladatok végrehajtásának konkrét eseményeit és eredményeit ismerteti, a második rész az információbiztonsági és az adatvédelmi szabályozás alapvetéseit – a közös pontokat és a különbözőségeket – tekinti át, utalva a két szabályozás közelítésének lehetséges elemeire is. A konkrét szervezet a Büntetés-végrehajtási Szervezet, amelynek információbiztonsági szabályozást és nyilvántartást meghatározó szervezeti sajátosságait a későbbiekben szintén tárgyaljuk.

Információbiztonsági szabályozás és nyilvántartás

Előírások

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és végrehajtási rendeletei elsősorban az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet a szervezet vezetője által kiadandó Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) készítését írja elő,[1] amelyet az információvédelem hatósági felügyeletét ellátó Nemzeti Kibervédelmi Intézetnek (a továbbiakban: NKI) is meg kell küldeni. Az IBSZ tartalmára vonatkozó, mintegy 20 konkrét előírást az Ibtv. és a BM rendelet 4. mellékletének 3. alcíme szerinti Védelmi intézkedés katalógus rögzíti. Az idézett jogszabályok további mintegy 25 szabályzat, eljárásrend elkészítését, kialakítását is a szervezetek feladatává teszik (a számok az összevonásoknak megfelelően változhatnak, a tartalom természetesen kötött).

A szabályozás mellett – annak természetes kiindulópontjaként – meghatározott nyilvántartások kialakítását és vezetését is elvárja a jogalkotó; ezek közül a legalapvetőbb az elektronikus információs rendszerek (a továbbiakban: rendszerek) nyilvántartása. A

1 A nemzetközi példákat követve az Informatikai Tárcaközi Bizottság (ITB) 1994-ben, illetve 1996-ban kiadott 8. és 12. számú ajánlása, ezt követően a Közigazgatási Informatikai Bizottság (KIB) 2008-ban közzétett 25. számú ajánlása is alapvető dokumentumnak tekintette az IBSZ-t.

rendszernyilvántartás minden információbiztonság-irányítási rendszer (és a 41/2015. BM rendelet tulajdonképpen egy ilyen kvázi-szabvány[2] magyarított verziója) alapvető eleme, hiszen a rendszerek a szervezet alapvető vagyontárgyai, amelyek értékével és jellemzőivel minden ezekre irányuló tevékenység tervezéséhez és megvalósításához tisztában kell lennünk.

A nyilvántartott rendszerekről – az NKI elvárásai alapján – az NKI honlapján elérhető Osztályba sorolás és védelmi intézkedés űrlapot (a továbbiakban: OVI űrlap)[3] is ki kell tölteni, amely a 41/2015. BM rendelet követelményeinek való megfelelés ellenőrzését támogató, több száz soros technikai segédlet.

Az idézett adminisztratív védelmi intézkedéseket – a PDCA cikluson[4] alapuló szemléletnek megfelelően – rendszeresen felül kell vizsgálni és korrigálni kell a megfelelő működési eredmények elérése és fenntartása érdekében; a jogszabályok erre vonatkozó rendelkezéseket is tartalmaznak. Az IBSZ frissítését tekintve a Védelmi intézkedés katalógus a szervezetre bízza a szabályozás-felülvizsgálat gyakoriságának meghatározását;[5] a szervezetek általában évenkénti felülvizsgálatról döntenek. A rendszerek biztonsági osztályba sorolását az Ibtv. alapján legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.[6]

Megvalósítás

A Büntetés-végrehajtási Szervezet az információvédelmi szabályozás és a biztonsági osztályba sorolás esedékes felülvizsgálatát, frissítését – a korábbi gyakorlattól eltérően – a hagyományos, papíralapú (átiratokra támaszkodó) koordináció helyett a feladatra létrehozott munkacsoport működtetésével hajtotta végre.

A munkacsoportos megvalósítás melletti klasszikus érvek, hogy az érintettek közvetlen személyes kommunikációjával jelentősen lerövidíthető a felülvizsgálati folyamat, az egyébként jelentős koordinációs-egyeztetési munkateher megosztható a munkacsoporton belül, az adatellenőrzési munkaszakaszok csoporton belüli, egyidejű/párhuzamos végrehajtásával a tévedések, hibák esélye is csökkenthető. Természetesen nem elhanyagolható szempontot jelentenek a csoportmunka-támogató technikák alkalmazásának várható és igazolt hozadékai: az újszerű meglátások, észrevételek indította együttgondolkodás pozitív eredményei. Ez a módszer alkalmas arra is, hogy a sokszor emlegetett és elvárt, hatékony tudásmegosztást támogassa, és biztosítsa a szervezeti szinten egységes megközelítés, közös tudásminimum kialakítását is.

2 Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Rev.4 National Institute of Standards and Technology U.S. Department of Commerce. April 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Letöltve: 2019.12.04.

3 https://nki.gov.hu/hatosag/hirek/ovi-urlap-4-50/. Jelenleg a 4.50 verzió érhető el. Letöltve: 2019.12.04.

4 A PDCA-ciklus egy irányítás-fejlesztési modell, amelyben négy cselekvési szakasz (tervezés, Plan – végrehajtás, Do – ellenőrzés, Check – beavatkozás, Act) spirálszerű ismétlődése biztosítja a működés (termékek, folyamatok) optimalizálását; a közigazgatásban ez – ha nem is „szabványtudatosan" – régóta működik.

5 41/2015. BM rendelet, 4. melléklet 3.1.1.1.1.2. pont.

6 Ibtv., 8. § (1) bekezdés.

A munkacsoport három – egy szabályozási, egy nyilvántartási és egy értékelési –, előre meghatározott feladatot hajtott végre. A szabályozási feladat az átdolgozott IBSZ (70%-ban előkészített) tervezetében foglalt előírások informatikai szakmai és jogi-szabályozási szempontú ellenőrzésére, kiegészítésére, az IBSZ tartalmát is érintő egyéb szabályozó eszközök (BvOP utasítások, szakutasítások, intézkedések) hatályos tartalmának a Védelmi intézkedési katalógusban rögzített szabályozási kötelezettségek alapján történő egybevetésére, ellenőrzésére és a hivatkozások aktualizálására, valamint a Védelmi intézkedési katalógusban előírt eljárásrendek konkrét, a büntetés-végrehajtási szervezet által használt rendszerek sajátosságait figyelembe vevő tartalmának meghatározására terjedt ki. A nyilvántartási feladat a rendszernyilvántartás – EIR-alapnyilvántartás – érintett szakterületekkel előzetesen (hagyományos módon) egyeztetett adatainak ellenőrzését és véglegesítését, a jogszabályi környezet előírásainak történő megfelelésre vonatkozó adatok összegyűjtését, létrehozását jelentette. Az értékelési feladat a Büntetés-végrehajtási Szervezet által használt és üzemeltetett rendszerekre vonatkozó OVI űrlapok kitöltését foglalta magában.

A munkacsoport tíz „gyakorló" (jellemzően a büntetés-végrehajtási intézetek helyi informatikai feladatainak ellátását irányító) informatikus és tíz, a Büntetés-végrehajtási Szervezet különböző szakterületeiről (központi irányítás, illetve büntetés-végrehajtási intézet, általános jog, illetve személyügyi terület) érkező jogász munkatársból állt.

A munkacsoport a feladatokat két szakaszban hajtotta végre. Az első szakaszban az informatikus munkatársak egy 4 órás – a jogszabályi előírásokat közösen értelmező, konkretizáló – felkészítő után (több részletben bonyolított, összesen egy napos) videókonferencia keretében együtt kitöltötték az azonosított rendszerekre vonatkozó OVI űrlapokat. A 4 napos második szakaszban a húsz munkatárs informatikus-jogász párokat alkotva, témakörök (pl. incidenskezelés, informatikai beszerzés, mentés/archiválás, fejlesztés stb.) szerinti bontásban végezte a szabályozási és szabályozás-ellenőrzési feladatokat. Ezt követően az elkészült szabályozások összeolvasására és összefüggésvizsgálatára, a kitöltött OVI űrlapok tartalmi ellenőrzésére, valamint az aktualizált rendszernyilvántartás adatainak ellenőrzésére, szükség szerinti kiegészítésére, pontosítására került sor.

A csoport munkáját a Büntetés-végrehajtás Országos Parancsnoksága (a továbbiakban: BvOP) Informatikai Főosztály vezetője és a Jogi és Adatkezelési Főosztály állományában dolgozó elektronikus információs rendszer biztonságáért felelős személy (IBF) irányította, akik az említett előkészítő tevékenységek megszervezéséért és végrehajtásáért is feleltek.

Eredmények, tapasztalatok

A Védelmi intézkedés katalógus előírása szerint a szervezetnek gondoskodnia kell arról, hogy az IBSZ jogosulatlanok számára ne legyen megismerhető, módosítható.[7] A megismerés korlátozása egy Hivatalos Értesítőben közzéteendő közjogi szervezetszabályozó eszköz (országos parancsnoki utasítás) esetében nem értelmezhető. A jogalkotói szándék feltehetően az információbiztonsági szempontból érzékeny infor-

7 41/2015. BM rendelet, 4. melléklet, 3.1.1.1.1.3.

mációk védelmének biztosítása volt, erre tekintettel a BvOP kétszintű szabályozást alakított ki. Az IBSZ átfogó és keretjellegű szabályozás, amelyben említésre kerül (részletesen vagy a hivatkozások szintjén) minden, a Védelmi intézkedési katalógus szerint szabályozandó témakör; az érzékenyebb, konkrét információkat, részletesebb eljárásrendeket az Informatikai Biztonsági Kézikönyv (IBK) tartalmazza. Az egyes rendszerekre vonatkozó további részletszabályokat a rendszerdokumentáció, illetve további belső szabályozó eszközök rögzítik.

A kialakított információbiztonsági szabályozási rendszer másik alapvető vonása az információtechnológiai meghatározottságból fakadó centralizáltság. Míg a Büntetés-végrehajtási Szervezet alaptevékenysége esetében a központi (irányadó) szabályozás mellett jelentős arányt képvisel a helyi szabályozás, amely az adott intézetre, intézményre jellemző speciális végrehajtási szabályokat tartalmazza (beleértve a személyi, fizikai stb. feltételeknek megfelelő működés biztosítását), addig ilyen kettősség az informatikai és információbiztonsági szabályozás tekintetében nem áll fenn, hiszen ugyanazon informatikai szolgáltatások, ugyanazon alkalmazások szolgálják ki a középirányító szerv (BvOP) és az intézetek, intézmények informatikai felhasználóit. Az IBSZ hatálya ennek megfelelően a teljes Büntetés-végrehajtási Szervezetre kiterjed.

Az Ibtv. alapján az IBSZ-ben a szervezet, valamint – a szervezeten belüli eltérések esetén – a szervezeti egységek biztonsági szintbe[8] sorolásának eredményét és az elektronikus információs rendszerek biztonsági osztályba[9] sorolását rögzíteni kell.[10] A Védelmi intézkedés katalógus megfogalmazása szerint az IBSZ-nek tartalmaznia kell a szervezet elvárt biztonsági szintjét és egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.[11] A biztonsági szint esetében az elvárt és teljesített szint külön nem értelmezhető, a rendszerek biztonsági osztálya tekintetében azonban lehet különbség az elvárt és a teljesített osztályok között, így az IBSZ az elvárt biztonsági osztályt tartalmazza, a rendszernyilvántartás lehetőséget ad az elvárt és a teljesített biztonsági osztályra vonatkozó adat rögzítésére is.

A biztonsági szintbe sorolás a már említett centralizált informatikai működésre tekintettel történt meg. A BvOP – amely a Büntetés-végrehajtási Szervezet rendszereinek fejlesztéséért, központi üzemeltetéséért felelős – 4. biztonsági szintbe lett sorolva a 41/2015. BM rendelet alapján, amely szerint az érintett szervezet biztonsági szintje 4., ha a szervezet elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.[12] A büntetés-végrehajtási szervek – mivel önállóan nem fejlesztenek és üzemeltetnek rendszert – a 2. biztonsági szintbe kerültek besorolásra.

A Büntetés-végrehajtási Szervezet által használt és üzemeltetett rendszerek nyilvántartásába (a továbbiakban: EIR-alapnyilvántartás) felvételre kerültek a saját rendszerek és természetesen azok is, amelyeket más szervezet működtet, üzemeltet, és amelyekhez a Büntetés-végrehajtási Szervezet csak hozzáféréssel rendelkezik. Ez utóbbi rendszerek

8 Az Ibtv. szerint a biztonsági szint a szervezet felkészültsége az Ibtv.-ben és végrehajtási rendeleteiben meghatározott biztonsági feladatok kezelésére. Ibtv., 1. § (1) bekezdés 13. pont.

9 Az Ibtv. szerint a biztonsági osztály az elektronikus információs rendszer védelmének elvárt erőssége. Ibtv., 1. § (1) bekezdés 11. pont.

10 Ibtv., 10. § (8) bekezdés és 7. § (3) bekezdés.

11 41/2015. BM rendelet, 4. melléklet 3.1.1.1.4.

12 41/2015. BM rendelet, 2. melléklet 4.

esetében az OVI űrlap kitöltése nem értelmezhető, hiszen a Büntetés-végrehajtási Szervezetnek nincs (nem lehet) ráhatása a védelmi intézkedések megtervezésére és kialakítására, és teljes körű ismeretei sincsenek a megvalósított védelmi intézkedésekről.[13] E rendszerek tekintetében a rendszerhozzáférést biztosító együttműködési megállapodásban kötelezően meghatározott feladatok teljesítésével, illetve felelősségek viselésével kapcsolatos adatok (pl. kezelt, feldolgozott adatok köre, hozzáférők köre, vonatkozó jogszabályok, közjogi szervezetszabályozó eszközök, belső szabályozó eszközök stb.) rögzítése történt meg.

Az EIR-alapnyilvántartás jelenleg 59 rendszert, illetve rendszermodult tartalmaz. A modulok elkülönítésére azért volt szükség, mert rendeltetésük, az irányadó jogszabály/szabályozó eszköz, a bennük kezelt adatok köre eltérő és természetesen ezekkel összefüggésben az adatgazda (a rendszer működtetéséért felelős) szakterület is különböző.

A rendszernyilvántartásban külön mező jelzi azt, hogy az adott rendszer az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 14. § (2) bekezdése alapján zárt célúnak minősül-e. A zárt célú elektronikus információs rendszer – az Ibtv. meghatározása szerint – a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja.[14] Az adat megjelenítése a speciális kezelési igény jelzése miatt szükséges; a hivatkozott kormányrendelet szerint a zárt célú rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a zárt célú elektronikus információs rendszert működtető szerv vezetőjét – a Büntetés-végrehajtási Szervezet esetében tehát az országos parancsnokot – jelöli ki.[15] A kormányrendelet rendelkezik arról is, mely rendszerek tartoznak ebbe a körbe. A Büntetés-végrehajtási Szervezet FŐNIX rendszere (27 modullal) rendészeti területen szakmai feladatok támogatását szolgáló zárt célú elektronikus információs rendszerként, a Robotzsaru rendszer (7 modullal) rendészeti területen belső irodai és iratkezelési célt szolgáló zárt célú elektronikus információs rendszerként[16] szerepel a nyilvántartásban.

Az aktuális rendszernyilvántartás összesen húsz szakmai (nem informatikai) alapadatot tartalmaz;[17] a rendszer/modul megnevezését, rövid nevét, rendeltetését, státuszát (éles üzemben, kivezetve stb.), éles működése kezdetének és végének időpontját, a kezelt/feldolgozott adatok körét, őrzési idejét, a rendszer speciális besorolását (zárt célú), a szakmai működtetésért felelős, adatgazda szakterület/szervezeti egység megnevezését, a rendszerre vonatkozó dokumentumokra utalást (szabályozó eszköz száma, felhasználói leírás elérhetősége), az irányadó jogszabály számát, megnevezését, a hozzáférők körét

13 Ismereteink szerint a közigazgatásban nincs egységes gyakorlat e kérdés kapcsán, álláspontunk szerint nem szerencsés egyazon rendszer különböző felhasználók általi – feltehetően nem egységes – értékelése.

14 Ibtv., 1. § (1) bekezdés 47. pont.

15 187/2015. Korm. rendelet, 14. § (3) bekezdés.

16 187/2015. Korm. rendelet, 14. § (2) bekezdés c) és b) alpont.

17 Az informatikai leíró adatokat a BvOP Informatikai Főosztálya tartja nyilván és aktualizálja, elsősorban a rendszerdokumentációk alapján.

(teljes szervezet vagy BvOP, intézetek, intézmények, illetve fogvatartottak kötelező foglalkoztatására létrehozott gazdasági társaságok), külső szervek hozzáférése esetén azok megnevezését és a hozzáférés jogalapját (együttműködési megállapodás/szerződés száma, kelte), valamint a rendszer besorolás szerinti és tényleges biztonsági osztályát.

Az információbiztonsági szabályozás régóta tapasztalt, alapvető problémája az informatikai és a jogi-szabályozási ismeretek harmonizálásának megoldatlansága. Magyarul: aki mély informatikai ismeretekkel bír, ritkán ért a jogi-szabályozási tevékenység „szakmai finomságaihoz", és fordítva, a jogi-szabályozási szakma művelői számára az informatikai szakszavak és mögöttes tartalmuk használata – következetes értelmezése – jelent gondot. A probléma nemcsak a szabályozás megalkotása során merül fel, a „nem jól" megfogalmazott előírások a végrehajtást is nehezítik. A „nem jó" megfogalmazás az informatikusok szerint a fogalmi (jogászi) szőrszálhasogatást vagy éppen – ezzel látszólag ellentétes módon – a nem kellően konkrét előírásokat jelenti (megteszi a szükséges intézkedéseket, kellő mélységben részletezett forráskód stb.). Ez utóbbi megoldások oka hagyományosan a technológiasemlegesség: a jogi szabályozás nem kíván állást foglalni konkrét műszaki, informatikai kérdésekben; a műszaki, technológiai előírások forrásai inkább a műszaki szabványok, jó gyakorlatok. A jogi-szabályozási munkát végzők számára viszont az jelent problémát, hogy az informatikai tárgyú dokumentumok, jogszabályok gyakran nem vagy nem következetesen definiálják az általuk használt fogalmakat.. Mivel a szabályozás során a szakmai tartalom biztosítására irányuló és a jogszabály-szerkesztési feladatok közötti határvonal – mint azt mindannyian megtapasztalhattuk már – nehezen meghatározható, a közös munka tűnt a legcélravezetőbbnek. A feltételezés beigazolódott: nagyon rövid idő alatt informatikai szakmai és jogi-szabályozási szempontból is megfelelő, közérthető és alkalmazható szabályozás és nyilvántartás született.

Információbiztonság, adatvédelem és adatbiztonság

Az Európai Unió általános adatvédelmi rendeletének[18] előkészítési munkálatai 2009-ben kezdődtek; már akkor nyilvánvaló volt, hogy az adatvédelmi szabályozást a megváltozott körülményekhez – a kialakuló adatközpontú gazdaság[19] jellemzőihez, ugyanakkor az egyre intenzívebb adatfelhasználással kapcsolatos aggodalmak csökkentésére vonatkozó társadalmi elvárásokhoz – kell igazítani.

Az általános adatvédelmi rendelet ennek megfelelően – az adatvédelem részeként – az adatbiztonságról is rendelkezik. Az 5. cikk a személyes adatok kezelésére vonatkozó elvek között rögzíti az „integritás és bizalmas jelleg" elvét, amely szerint a személyes adatokat úgy kell kezelni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok

18 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, GDPR)

19 Az adatközpontú gazdaság fogalmát lásd A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK – Úton a prosperáló adatközpontú gazdaság felé COM(2014) 442.

jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.[20] Ugyanezt az elvet az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) Európai Unió adatvédelmi reformjával összefüggésben végrehajtott módosítása is tartalmazza.[21]

Az adatvédelem – ahogyan arra Jóri András rámutat – „*a magánszféra-védelem egyik eszköze, s mint ilyen, szükségszerűen a személyre irányul, az adatbiztonság tárgya maga az adat. Az adatbiztonság az adat integritásának és bizalmasságának védelmét jelenti, függetlenül az adat információtartalmától és jogi minősülésétől.*"[22]

Az integritás és a bizalmas jelleg, valamint a rendelkezésre állás követelménye az Ibtv.-ben is megjelenik: „Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának … biztosítása, ezáltal a kibertér védelme".[23]

Az általános adatvédelmi rendelet és az Infotv. alapján tehát az adatbiztonság garantálása érdekében technikai és szervezési intézkedéseket, az Ibtv. alapján az információbiztonság érdekében adminisztratív, fizikai és logikai (informatikai) intézkedéseket kell megtervezni és végrehajtani. A két jogszabály – bár eltérő fogalomhasználattal – gyakorlatilag ugyanarról rendelkezik; a különbség a szabályozás mélységében – konkrétságában – van.

Az általános adatvédelmi rendelet egy általános előírással kötelezi az adatkezelőt arra, hogy a tudomány és technológia állása, a megvalósítás költségei, az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajtson végre a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. A rendelkezés szerint az említett négy szempont alapján az adatkezelőnek magának kell meghatározni a szükséges intézkedéseket. Az általános előírást egy néhány elemet tartalmazó példálózó felsorolás követi, amely az információbiztonsági szabványok, jó gyakorlatok legfontosabb előírásait idézi. A javaslat között szerepel a személyes adatok álnevesítése és titkosítása, a műszaki incidenst követő helyreállítást biztosító képességek fenntartása, az intézkedések tesztelése és értékelése. Kiemelendő a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítását célzó intézkedések említése. Az Infotv. – a már hivatkozott, 2018. évi módosítást követően – szinte ugyanezen előírásokat tartalmazza, azzal a különbséggel, hogy a példálózó felsorolás nem védelmi intézkedéseket, hanem a megfelelő intézkedésekkel elérendő védelmi célokat nevesít.[24] A két szabályozás közötti hasonlóság természetes; az Infotv. 2018-ban történt módosítása – mint ismert – részben az általános adatvédelmi rendeletet

20 Általános adatvédelmi rendelet, 5. cikk.
21 Infotv., 4. § (4a) bekezdés.
22 Jóri A. (2009) p. 17.
23 Ibtv., preambulum.
24 Infotv., 25/I. § (3) bekezdés.

pontosító, kiegészítő rendelkezéseket rögzít a rendelet felhatalmazása alapján, részben a bűnügyi adatvédelmi irányelv[25] implementációját valósítja meg.

A fentiektől eltérően a 45/2015. BM rendelet több száz soros részletes intézkedéskatalógust tartalmaz, amelynek elemeit – a védendő rendszerek biztonsági osztályának figyelembe vételével – kötelező teljesíteni.

Az idézett jogszabályok hatékony és eredményes végrehajtása érdekében az információbiztonsági és az adatbiztonsági előírásokat egymásra tekintettel szükséges értelmezni és teljesíteni. Ez annál is könnyebb, mivel az információbiztonsági jogszabályokat mintegy két évtizeddel megelőző adatvédelmi jogi szabályozás (részben későbbi módosítások eredményeként) már tartalmazta és a hatályos szabályozás is tartalmazza azokat az elemeket, amelyek alapján a két tárgykört érintő szabályozási és nyilvántartási kötelezettségek közelíthetőek egymáshoz. A már említett, információbiztonsággal összefüggő előírásokhoz kapcsolódóan az adatvédelem és adatbiztonság tekintetében – jelen tanulmány tárgyára tekintettel, a Büntetés-végrehajtási Szervezetre vonatkozó előírások közül – az adatvédelmi tisztviselő kinevezésének, az Adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: AASZ) kiadásának és az adatkezelési nyilvántartás vezetésének kötelezettsége emelendő ki.[26] A szervezeten belüli egyszemélyi felelős (adatvédelmi tisztviselő, illetve az Ibtv. szerinti elektronikus információs rendszer biztonságáért felelős személy) meghatározása biztosítani tudja, hogy az adatvédelemmel, illetve az információbiztonsággal összefüggő kérdések folyamatosan és azonos megközelítésben legyenek kezelve, és lehetővé teheti azt is, hogy a két felelős a szabályozási és nyilvántartási kereteket közvetlen, egyszerűsített koordinációval, egyeztetéssel alakítsa ki és terjessze fel jóváhagyásra. Az alapszabályzatok (IBSZ és AASZ) elkészítésének kötelezettsége az egyértelmű végrehajtási keretek meghatározását és – szerencsés esetben – az azonos fogalomhasználatot és a szabályozások kapcsolódási pontjainak rögzítését garantálni tudja. A Büntetés-végrehajtási Szervezet Adatvédelmi és adatbiztonsági szabályzata az adatbiztonságra vonatkozó rendelkezések között visszautal a védelmi intézkedések Ibtv. szerinti logikai csoportosítására, ezzel egyértelművé téve, hogy a részletes intézkedések meghatározása az információbiztonsági szabályozás körébe tartozik. A legígéretesebb egyszerűsítési – konszolidációs – lehetőségeket a rendszernyilvántartás és az adatkezelési nyilvántartások összhangba hozása biztosítja.

Az általános adatvédelmi rendelet 30. cikke minden adatkezelő számára előírja az általa végzett adatkezelési tevékenységek nyilvántartását, amely tartalmazza az adatkezelő és az adatvédelmi tisztviselő nevét és elérhetőségét, az adatkezelés céljait, az érintettek és a személyes adatok kategóriáit, olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják (ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket – ez utóbbi esetben további leíró adatokat), továbbá – ha lehetséges – a különböző adatkategóriák törlésére előirányzott határidőket és az adatbiztonságot garantáló technikai és szervezési intézkedések általános leírását.

25 AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (bűnügyi adatvédelmi irányelv)

26 A Büntetés-végrehajtási Szervezet által végzett személyesadat-kezelésre vonatkozó előírásokat az általános adatvédelmi rendelet mellett az Infotv. rendelkezései

A rendelet előírja továbbá, hogy az adatkezelő köteles a felügyeleti hatósággal (Nemzeti Adatvédelmi és Információszabadság Hatóság, a továbbiakban: NAIH) együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.[27] A rendelkezés eltörölte az Infotv. korábbi előírását, amely szerint az adatkezelésekről a NAIH vezetett központi hatósági nyilvántartást, az adatkezelés nyilvántartásba vétele az adatkezelő kérelmére történt, a törvény által meghatározott határidőn belül.

Az Ibtv. 15. § (1) bekezdése szerint a felügyeleti hatóság (a továbbiakban: NKI) nyilvántartja és kezeli a törvény hatálya alá tartozó szervezet azonosításához szükséges adatokat, a szervezet elektronikus információs rendszereinek megnevezését, a rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, a rendszerek külön jogszabályban meghatározott technikai adatait, a rendszer biztonságáért felelős személy természetes személyazonosító és elérhetőségi adatait, végzettségét és a szervezet informatikai biztonsági szabályzatát.[28] A 41/2015. BM rendelet előírja a szervezet számára az információs rendszerek nyilvántartásának vezetését, amely tartalmazza többek között az információs rendszerek alapfeladatait, az információs rendszerek által biztosítandó szolgáltatásokat, az információs rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait, az információs rendszert szállító, fejlesztő és karbantartó szervezetek és kapcsolattartóik azonosító és elérhetőségi adatait. Ahhoz, hogy az érintett szervezet az NKI számára adatot tudjon szolgáltatni, értelemszerűen maga is nyilvántartja a hatóság által elvárt adatokat, valamint azokat is, amelyeket a rendelet alapján saját maga számára kell nyilvántartania.[29]

Az adatvédelmi és az információbiztonsági nyilvántartásnak vannak közös elemei, ilyen a kezelt adatok típusa (kategóriája) és a használt információs rendszerek. Ez utóbbi elem az adatkezelési nyilvántartás része is kell, hogy legyen, amennyiben elektronikus adatkezelésről van szó (az esetek meghatározó többségében ez a helyzet), és szükségessé teheti az adatbiztonságot garantáló technikai intézkedések – elvárt – rövid leírása is az információs rendszerek azonosítását.

Alapvető különbség a nyilvántartások vezetésének helyét illetően van, míg az adatkezelési nyilvántartást az érintett szervezet helyben vezeti és a felügyeleti hatóságnak kérésre hozzáférést biztosít ahhoz, az információs rendszerekkel kapcsolatos adatok nyilvántartását két helyen (szervezet és hatóság) vezetik.

Az esetleges konszolidáció során figyelemmel kell lenni arra is, hogy az alapnyilvántartások rendszerébe beletartozik az Elektronikus Ügyintézési Felügyelet (a továbbiakban: EÜF) által az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (E-ügyintézési tv.) alapján vezetett két nyilvános, központi nyilvántartás, az Információforrások regisztere, valamint az Adat- és iratmegnevezések jegyzéke. Ez utóbbi az informatikai együttműködés szempontjából jelentőséggel bíró adatokat (megnevezések, azok értelmezése, az adatok és iratok kezeléséhez szükséges információk), az előbb említett pedig – a szervezetek által megküldött Információátadási szabályzatok alapján – adatkezeléssel és elektronikus adatátadással összefüggő adatokat tartalmaz. Ugyancsak az EÜF felügyeli az egységes

27 Általános adatvédelmi rendelet, 30. cikk.
28 Ibtv., 15. § (1) bekezdés.
29 41/2015. BM rendelet, 4. melléklet, 3.1.1.4. pont.

Állami Alkalmazás-fejlesztési Környezetről és az Állami Alkalmazás-katalógusról, valamint az egyes kapcsolódó kormányrendeletek módosításáról szóló 314/2018. (XII. 27.) Korm. rendelet szerinti Állami Alkalmazás-katalógus vezetését, amely az állam működésének támogatása érdekében fejlesztett és az állam által megvásárolt alkalmazások zárt, az alkalmazások funkcionális, szakmai, tartalmi és műszaki adatait tartalmazó nyilvántartása, és amely a szervezetek elektronikus adatszolgáltatásai alapján naprakészen tartalmazza az alkalmazást használó, fejlesztő és üzemeltető szervezet adatait, az alkalmazás tulajdonosának adatait, az alkalmazás általános adatait, a kapcsolódó jogszabályi előírásokat, az alkalmazás általános működésének leírását, működési kézikönyvét, az alkalmazás műszaki tartalmára vonatkozó adatokat, az Ibtv. szerinti biztonsági osztályt és az alkalmazással kapcsolatban álló információs rendszerek és alkalmazások felsorolását.[30] [31]

Összegzés

„Megfigyelhető momentum közigazgatásunkban az, hogy ha a már szabályozott bizonyos feladatkörökkel kapcsolatban később újabb törvényeket és rendeleteket hozunk, azok a meglevő munkák mellett (…) további tennivalókat rónak a végrehajtó szervekre, anélkül azonban, hogy ezeket a később elrendelt teendőket szervesen bekapcsolnák az előbbi munkákba. Az újabb munkajárulékok azután tovább növelik a végrehajtó közegek és szervek munkaterhét, holott megfelelő szervezéssel nem csupán a régi munka anyagát lehetne célszerűen csökkenteni, hanem az újabb munkajárulékot is többnyire minden nehézség nélkül lehetne ahhoz hozzákapcsolni, esetleg bele is olvasztani." – írta Fluck András 1938-ban.[32]

Megállapítása ma is helytálló; az információvédelem és az adatbiztonság két olyan terület, amelyeket – közös pontjaikra tekintettel – a végrehajtandó feladatok racionalizálása érdekében szükséges harmonizálni. Azt se felejtsük el, hogy a szabályozás nem pusztán adminisztráció: célja a jogszerű és szakszerű működés kereteinek meghatározása. Egy szervezet szabályozási rendszere pedig magáról a szervezetről nyújt a vezetést és irányítást is támogató, valós képet.

30 314/2018. Korm. rendelet.

31 Az Ibtv. által besorolandó rendszerek és az Állami Alkalmazás-katalógusban nyilvántartandó szoftverrendszerek köre azonban nem esik egybe. Ennek oka egyrészt az, hogy az Ibtv. komplex rendszerfogalmat használ, amibe nem csak a szoftver értendő bele, másrészt az, hogy az Állami Alkalmazás-katalógusban nem minden szoftvernek kell szerepelnie (pl. nem kell nyilvántartani az intézményeknél meglevő operációs rendszereket vagy irodai alkalmazáscsomagokat).

32 Fluck A. (1938) p. 142.

Felhasznált irodalom

Fluck András (1938): A közigazgatási ügyintézés racionalizálása. 2. átdolgozott kiadás. Közzéteszi dr. vitéz Keresztes-Fischer Ferenc m. kir. t. t., belügyminiszter, Budapest.

Jóri András (2009): Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése. PhD dolgozat. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola. Pécs.

Jogszabályok, dokumentumok

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (E-ügyintézési tv.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)

314/2018. (XII. 27.) Korm. rendelet az egységes Állami Alkalmazás-fejlesztési Környezetről és az Állami Alkalmazás-katalógusról, valamint az egyes kapcsolódó kormányrendeletek módosításáról

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

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, GDPR)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (bűnügyi adatvédelmi irányelv)

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK – Úton a prosperáló adatközpontú gazdaság felé COM(2014) 442

Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Rev.4 National Institute of Standards and Technology U.S. Department of Commerce. April 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Letöltve: 2019. december 4.)

https://nki.gov.hu/hatosag/hirek/ovi-urlap-4-50/ (Letöltve: 2019. december 4.)