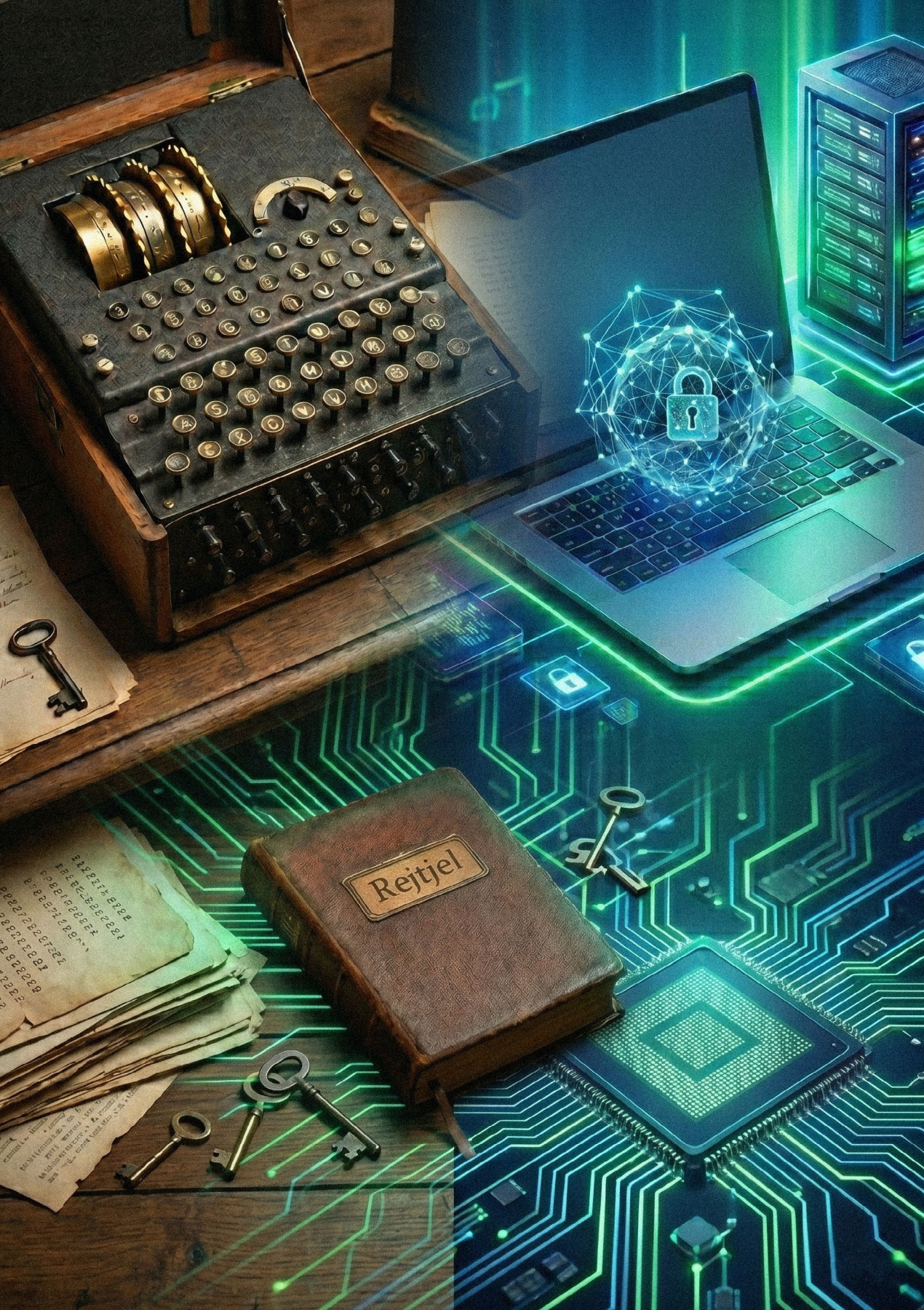
Rejtjel

https://doi.org/10.66102/BSZ.2026.2.1

Barna Balázs

Rejtjelezés és minősített iratkezelés a büntetés-végrehajtásban – Jogi, szervezeti és technikai összefüggések

Encryption and classified document management in the Prison Service – Legal, organizational, and technical aspects

A digitális információs környezet alapvetően átalakította a büntetés-végrehajtási szervezet működését. Az elektronikus adatkezelés, a hálózati kommunikáció és az integrált informatikai rendszerek megjelenésével a minősített adatok védelme már nem biztosítható kizárólag fizikai és adminisztratív eszközökkel. A modern büntetés-végrehajtási szervezetben a rejtjelezés és az elektronikus biztonsági megoldások a szervezeti működés strukturális elemévé váltak.

A minősített adatvédelem jogi szabályozása Magyarországon részletes, többszintű normarendszerre épül. Ennek ellenére hiányoznak azok az átfogó elemzések, amelyek a jogi, szervezeti és technikai dimenziók együttes működését a büntetés-végrehajtás sajátos kontextusában vizsgálják. Különösen hiányzik annak rendszerszintű bemutatása, miként kapcsolódik össze a minősítési döntéshozatal és a rejtjeltevékenység az elektronikus rendszerek engedélyezési és felügyeleti mechanizmusaival.

Kulcsszavak: minősített adat, rejtjelezés, elektronikus biztonság, adatvédelem, szervezeti felelősség

The digital information environment has fundamentally transformed the operations of the prison service. With the advent of electronic data management, networked communication, and integrated IT systems, the protection of classified data can no longer be ensured solely through physical and administrative measures. In modern correctional institutions, encryption and electronic security solutions have become structural elements of organizational operations.

The legal regulation of classified data protection in Hungary is based on a detailed, multi-tiered system of norms. Nevertheless, there is a lack of comprehensive analyses that examine the combined functioning of the legal, organizational, and technical dimensions within the specific context of the prison system. In particular, there is a lack of a systematic presentation of how classification decision-making and encryption activities are linked to the licensing and oversight mechanisms of electronic systems.

Keywords: *classified information, encryption, electronic security, data protection, organizational responsibility*

Bevezetés

A büntetés-végrehajtási szervezet (a továbbiakban: bv. szervezet) az állami intézményrendszeren belül egy zárt, és az információbiztonságra érzékeny alrendszer, amely működéséből fakadóan rendszeresen kezel olyan adatokat, amelyeknek nyilvánosságra kerülése, jogosulatlan megismerése vagy módosítása közvetlenül veszélyeztetheti a közrendet, a közbiztonságot, valamint a büntetés-végrehajtási intézetek (a továbbiakban: bv. intézetek) működését. A szabadságelvonással járó büntetések végrehajtása, a bv. intézetek rendje, a fogvatartottak mozgatása, illetve a rendkívüli események kezelése mind olyan területek, ahol az információk védelme kiemelt jelentőséggel bír.

A minősített adatkezelés jogi és szervezeti kereteit Magyarországon *a minősített adat védelméről* szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.), és a *Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről* szóló 90/2010. (III. 26.) Korm. rendelet határozza meg. A szabályozási környezet nem elszigetelt normák összessége, hanem egymásra épülő rendszer, amely meghatározza a minősítés feltételeit, az adatkezelés rendjét, valamint a védelem személyi, fizikai, adminisztratív és elektronikus eszközeit. A bv. szervezet belső szabályzatai e jogszabályi keretekre épülve konkretizálják az egyes feladatokat, hatásköröket és felelősségi szinteket.

A digitalizáció és az elektronikus adatkezelés térnyerése alapvetően átalakította a minősített adatok kezelésének módját. Az elektronikus rendszerek megjelenésével párhuzamosan növekedett az adatok sérülékenysége, valamint az illetéktelen hozzáférés és az adatkompromittálódás kockázata. A kihívásokra adott válaszként vált nélkülözhetetlenné a rejtjelezés, mint technikai védelmi eszköz, amely biztosítja, hogy az elektronikus úton kezelt vagy továbbított minősített adatok tartalma jogosulatlan személyek számára hozzáférhetetlen maradjon. A rejtjelezés alkalmazása ugyanakkor nem választható el a jogi megfeleléstől és a szervezeti felelősségi rendszertől.

A tanulmány célja a rejtjelezés és a minősített iratkezelés rendszerének átfogó bemutatása a büntetés-végrehajtásban, különös tekintettel a jogi szabályozásra, a szervezeti struktúrára és a technikai megoldásokra. A vizsgálat nem a jogszabályok szó szerinti ismertetésére törekszik, hanem azok értelmezésén keresztül mutatja be a minősített adatvédelem és a rejtjeltevékenység logikai felépítését, valamint gyakorlati jelentőségét.

A minősítési szintek rendszere és jelentőségük

A minősített adatok védelme nem egységes szintű korlátozást jelent, az differenciált rendszerben valósul meg. A jogalkotó abból indult ki, hogy nem minden adat sérülése jár azonos következményekkel, ezért a védelem mértékét ahhoz a kárhoz kell igazítani,

amely az adat jogosulatlan megismerése esetén bekövetkezhet. Ennek megfelelően a magyar szabályozás négy minősítési szintet határoz meg: „Korlátozott terjesztésű!", „Bizalmas!", „Titkos!" és „Szigorúan titkos!". A minősítési szintek nem pusztán elnevezések, hanem eltérő védelmi követelményeket és eljárásokat aktiválnak.

A „Korlátozott terjesztésű!" minősítési szint a minősített adatvédelem legalacsonyabb foka. Az ide sorolt információk esetében a jogalkotó abból indul ki, hogy az adat nyilvánosságra hozatala nem okozna súlyos állami vagy szervezeti kárt, ugyanakkor indokolt megakadályozni annak széles körű terjesztését. A „Korlátozott terjesztésű!" minősítési szintű irat kezeléséhez titoktartási nyilatkozat elegendő. A hétköznapi olvasó számára ez úgy érthető meg, hogy az adat „nem való mindenkinek", de kezelése még nem igényli a legszigorúbb biztonsági intézkedéseket. A büntetés-végrehajtásban ilyen lehet például egyes belső működési rendek vagy intézkedési tervek részlete, amelyek nyilvánossága zavart okozhatna, de nem vezetne súlyos biztonsági következményekhez.

A „Bizalmas!" minősítési szint már olyan adatokat véd, amelyek jogosulatlan megismerése érzékelhetően befolyásolhatja az állami szerv működését, a rend fenntartását vagy egyes eljárások eredményességét. Ebben a kategóriában az adat kompromittálódása tényleges működési vagy biztonsági problémát okozhat. A büntetés-végrehajtásban ide sorolhatók például olyan információk, amelyek intézetbiztonsági intézkedésekhez, kockázatelemzésekhez vagy speciális eljárások előkészítéséhez kapcsolódnak. A „Bizalmas!" szint már szigorúbb hozzáférési és kezelési szabályokat követel meg, beleértve a személyi és adminisztratív kontroll erősítését is.

A „Titkos!" minősítési szint esetében a jogalkotó már súlyos következményekkel számol. Az ide sorolt adatok jogosulatlan megismerése az állam alapvető működését, a közbiztonságot vagy a bv. szervezet kulcsfontosságú feladatait veszélyeztetheti. Ez azt jelenti, hogy az ilyen információk kiszivárgása nemcsak egy-egy eljárást érinthet, hanem rendszerszintű kockázatot hordoz. A „Titkos!" minősítéshez már kiemelten szigorú személyi biztonsági feltételek, elkülönített kezelési rend, valamint engedélyezett informatikai rendszerek és rejtjelező megoldások alkalmazása kapcsolódik.

A „Szigorúan titkos!" minősítési szint a legmagasabb fokú védelem alá eső adatokat jelöli. Ezek jogosulatlan megismerése rendkívül súlyos, akár helyrehozhatatlan következményekkel járhat az állam biztonsága vagy alapvető érdekei szempontjából. A büntetés-végrehajtásban ez a szint ritkán jelenik meg, de nem kizárt: különösen akkor, ha az információ nemzetbiztonsági dimenzióval is rendelkezik. A kezelés rendkívül szigorú: a hozzáférés rendje, az iratkezelés, az elektronikus feldolgozás és a rejtjelezés minden elemét külön ellenőrzési és engedélyezési rendszer övezi.[1]

1 Mavtv. 3. §

A minősítési szintek gyakorlati jelentősége abban áll, hogy nem maga a címke védi az adatot, hanem az ahhoz kapcsolódó intézkedések rendszere. A minősítési szint határozza meg, ki férhet hozzá az adathoz, hol és hogyan tárolható, milyen módon továbbítható, milyen elektronikus rendszerekben kezelhető, valamint milyen ellenőrzési mechanizmusok vonatkoznak rá. A bv. szervezet működésében ez biztosítja, hogy a védelem ne legyen sem indokolatlanul túlzó, sem veszélyesen gyenge, hanem a tényleges kockázatokhoz igazodjon.

Ki és hogyan minősíthet?

A minősítésre jogosult személyek köre

A minősített adat létrejötte minden esetben tudatos és felelős döntés eredménye. A jogalkotó abból az alapvetésből indul ki, hogy a minősítés az információhoz való hozzáférés korlátozását jelenti, amely alapjogokat érint, ezért alkalmazása nem bízható tetszőleges szervezeti szereplőre. A minősítésre jogosult személyek körét a Mavtv. kifejezetten és zárt felsorolásban határozza meg, kizárva a minősítési jogkör általános vagy automatikus alkalmazását.

A Mavtv. alapján minősítésre jogosult többek között a köztársasági elnök, az Országgyűlés elnöke, a Kormány, valamint a Kormány tagjai saját feladat- és hatáskörükben. A minősítési jogkör kiterjed továbbá az önálló szabályozó szervek vezetőire, az Alkotmánybíróság elnökére, az alapvető jogok biztosára, valamint egyes állami vagy közfeladatot ellátó szervek vezetőire az általuk irányított szervezet működéséhez kapcsolódó adatok tekintetében.[2]

A felsorolás mögött világos jogpolitikai logika húzódik meg. A minősítés nem technikai vagy adminisztratív aktus, hanem olyan döntés, amelyhez szükséges a szervezet működésének átfogó ismerete, a biztonsági kockázatok értelmezése, valamint annak mérlegelése, hogy az információ nyilvánosságra kerülése milyen következményekkel járhat. A jogalkotó ezért kizárólag olyan személyeket ruház fel minősítési jogkörrel, akik a döntésükért politikai, jogi vagy szervezeti értelemben is felelősséggel tartoznak.

Leegyszerűsítve úgy fogalmazható meg, hogy nem az minősít, aki az iratot írja, és nem is az, aki technikailag kezeli, hanem az, aki felelősséggel képes mérlegelni az információ súlyát és kockázatait. A minősítés tehát vezetői döntés, amelynek következményei túlmutatnak az adott dokumentumon, és a szervezet egészének működésére lehetnek hatással. A minősítési döntések jellemzően azoknál a vezetőknél jelennek meg, akik az intézet biztonságáért, a rendkívüli események kezeléséért, a szervezeti működésért

2 Mavtv. 4. §

vagy az együttműködések irányításáért felelnek. Ez biztosítja, hogy a minősítés összhangban álljon a valós biztonsági kockázatokkal, és ne váljon indokolatlanul széles körű vagy rutinszerű gyakorlattá.

A bv. szervezetben az adatok minősítésére – a Mavtv. alapján – kizárólag az országos parancsnok jogosult, azonban ezen jogosultságát átruházhatja a törvényben meghatározott feltételek teljesülése esetén.

„Szigorúan titkos!" minősítési szintig minősítésre jogosultak az országos parancsnok helyettesei.

„Titkos!" minősítési szintig minősítésre jogosult:

- a BVOP Hivatal hivatalvezetője,
- a BVOP Jogi és Adatkezelési Főosztály főosztályvezetője,
- a BVOP Humán Szolgálat szolgálatvezetője,
- a BVOP Ellenőrzési Szolgálat szolgálatvezetője,
- a BVOP Biztonsági Szolgálat szolgálatvezetője,
- a BVOP Fogvatartási Ügyek Szolgálata szolgálatvezetője,
- a BVOP Nyilvántartási és Logisztikai Főosztály főosztályvezetője,
- a BVOP Felderítési Főosztály főosztályvezetője,
- a BVOP Felderítési Főosztály főosztályvezető-helyettese,
- valamennyi bv. intézet/intézmény vezetője.[3]

A minősítési eljárás rendje és a minősítő felelőssége

A minősítési eljárás rendje szigorúan meghatározott feltételekhez és lépésekhez kötött. Minősítésre kizárólag akkor kerülhet sor, ha az adat olyan közérdeket érint – például nemzetbiztonsági, honvédelmi, bűnüldözési vagy állami működési érdeket –, amelynek sérelme az adat jogosulatlan megismerése esetén valós kockázatot jelent. A minősítési eljárást az adat keletkezésekor az kezdeményezi, akinél az adat létrejön, és indokolással ellátott minősítési javaslatot készít, amelyben megjelöli a védendő közérdeket, a javasolt minősítési szintet és az érvényességi időt. A döntést a minősítő hozza meg, főszabály szerint 30 napon belül, ennek hiányában a minősített adat nem jön létre. A minősítés során alapelv, hogy az adat megismerhetősége csak a szükséges mértékben és ideig korlátozható, a minősítési szintet pedig az okozható kár súlyossága határozza meg. Az adat minősített jellegét egyértelműen jelölni kell, és a minősítés időtartama törvényben meghatározott, amely indokolt esetben meghosszabbítható, azonban a minősítés megszűnését követően az adat ismételt minősítésére nincs

3 A Büntetés-végrehajtás Országos Parancsnoksága minősített adatainak Biztonsági Szabályzatáról szóló 3/2020. (VII. 14.) BVOP utasítás 78-80. pontja

lehetőség. Az eljárás teljes folyamata során kiemelt jelentőséggel bír az indokoltság, az arányosság és az ellenőrizhetőség követelménye, amely a minősítő döntésének szakmai és jogi megalapozottságát biztosítja.[4]

A minősítői jogkör gyakorlása nem pusztán formális felhatalmazás, hanem olyan döntés, amely jelentős jogi és szervezeti felelősséggel jár. A minősítő személy döntése közvetlen hatással van arra, hogy egy információ milyen körben válik hozzáférhetővé, milyen védelmi intézkedések kapcsolódnak hozzá, valamint milyen ellenőrzési és iratkezelési eljárásrend alá esik. A minősítési eljárást ezért nem adminisztratív rutinfeladatnak, hanem minden esetben mérlegelést igénylő, dokumentált döntési folyamatnak kell tekinteni. A minősítési eljárás első lépése annak vizsgálata, hogy az adott adat jogosulatlan megismerése milyen közérdeket sérthet vagy veszélyeztethet. A jogszabály nem engedi meg az absztrakt vagy általános indokolást, a minősítés alapját minden esetben konkrét kockázatoknak kell képezniük. A bv. szervezet gyakorlatában ez azt jelenti, hogy a minősítőnek értékelnie kell például az adat bv. intézet biztonságára, a rend fenntartására, a személyi állomány vagy a fogvatartottak biztonságára, illetve a folyamatban lévő eljárások eredményességére gyakorolt hatásait. A döntés során nem az információ „kényessége", hanem annak lehetséges következményei képezik a mérlegelés tárgyát.

A minősítés során a minősítő személynek meg kell határoznia a megfelelő minősítési szintet is. A minősítési szint kiválasztása nem önkényes, hanem a várható kár súlyosságához igazodik. A túl alacsony minősítési szint a védelem elégtelenségéhez, míg a túl magas minősítés indokolatlan korlátozásokhoz és szervezeti, működési nehézségekhez vezethet. A minősítő felelőssége abban áll, hogy a védelem mértéke arányban álljon a tényleges kockázattal, és ne váljon sem alul-, sem túlminősítetté.

A minősítési eljárás elválaszthatatlan eleme az időbeli korlátozás meghatározása. A jogszabály abból indul ki, hogy a minősítés nem örök érvényű állapot, hanem a védett érdek fennállásához kötődik. A minősítőnek ezért döntést kell hoznia arról is, hogy a minősítés meddig indokolt. A határozott időre szóló minősítés biztosítja, hogy az információ védelme ne maradjon fenn akkor is, amikor a kockázatok már nem állnak fenn. A büntetés-végrehajtási gyakorlatban ez különösen fontos olyan adatok esetében, amelyek egy konkrét intézkedéshez, eljáráshoz vagy eseményhez kapcsolódnak.

A Mavtv. módosítása alapján megváltozott a minősített adat felülvizsgálatára vonatkozó szabályozás, melynek értelmében megszűnt a minősített adatokra korábban előírt 5 évente történő felülvizsgálati kötelezettség, feltéve, ha törvény nem határozza meg a felülvizsgálat lefolytatásának határidejét. Ugyanakkor fontos annak megállapítása, hogy a minősítés alapjául szolgáló körülmények változtak-e, és a minősítés fenntartása

4 Mavtv. 5-6. §

továbbra is indokolt-e. A felülvizsgálati kötelezettség a minősítő felelősségi körébe tartozik, és nem ruházható át automatikusan más szervezeti szereplőre. A rendszer ezzel biztosítja, hogy a minősítés dinamikusan kövesse a valós kockázati környezetet.[5]

A minősítő felelőssége nem ér véget a döntés meghozatalával. A minősítési döntés végrehajtása – az iratkezelési rend, a hozzáférési jogosultságok, az elektronikus kezelés és a rejtjelezés alkalmazása – a szervezeti szabályzatok alapján történik, azonban a döntés jogszerűségéért továbbra is a minősítő tartozik felelősséggel. A bv. szervezet belső ellenőrzési rendszere lehetőséget teremt arra, hogy a minősítési gyakorlatot utólag is vizsgálják.

A minősítési eljárás és a minősítő felelősségének rendszere összességében azt a célt szolgálja, hogy a minősítés a büntetés-végrehajtásban ne rutinszerű korlátozásként, hanem tudatos, ellenőrizhető és elszámoltatható döntésként jelenjen meg. A jogi és szervezeti garanciák együttesen biztosítják, hogy a minősítés valóban a közérdek és a biztonság védelmét szolgálja, miközben tiszteletben tartja az információszabadság alkotmányos kereteit.

A minősített adatkezelés rendszere a bv. szervezetben

Irányítási és felügyeleti szintek

A minősített adatkezelés biztonsága a bv. szervezetben nem kizárólag jogszabályi előírásokon múlik, hanem azon is, hogy a szervezet miként építi fel és működteti az irányítási és felügyeleti rendszerét. A jogalkotó abból indul ki, hogy a minősített adatok védelme csak akkor lehet hatékony, ha a döntési, végrehajtási és ellenőrzési hatáskörök világosan elkülönülnek, ugyanakkor egymással összehangoltan működnek. A szervezeti struktúra ezért a minősített adatvédelem egyik alapvető garanciális eleme.

A büntetés-végrehajtás tekintetében a minősített adatkezelés irányításának központi szereplője a BVOP, melynek feladata, hogy meghatározza azokat az egységes elveket, szabályokat és eljárásokat, amelyek a minősített adatok kezelésére, a rejtjeltevékenységre és az információbiztonságra vonatkoznak. A központi irányítás jelentősége abban áll, hogy biztosítja a szervezet egészében az egységes jogértelmezést és gyakorlatot, megelőzve azt, hogy az egyes intézetek vagy szervezeti egységek eltérő, esetleg egymással ellentétes megoldásokat hozzanak.

A központi irányításhoz szorosan kapcsolódik a biztonsági vezető szerepe, aki a minősített adatvédelem rendszerének szakmai koordinációjáért felel. A biztonsági vezető

5 Mavtv. 8. §

feladata nem egyetlen részterület irányítása, hanem a személyi, fizikai, adminisztratív és elektronikus biztonsági intézkedések összehangolása, a megfelelő személyi biztonsági tanúsítványok, valamint a titoktartási nyilatkozatok kiállítása a minősített adatot jogosultan felhasználók részére. A hétköznapi értelemben a biztonsági vezető tekinthető annak a szereplőnek, aki „összefogja" a minősített adatvédelem különböző elemeit, és biztosítja, hogy azok egyetlen egységes rendszerként működjenek. A szerepkör kiemelt jelentőségét az adja, hogy a biztonsági vezető tevékenysége közvetlen kapcsolatot teremt a jogszabályi követelmények és a napi gyakorlat között.

A felügyeleti rendszer következő fokozatát a helyi szinten megjelenő biztonsági felügyelet jelenti. A BVOP Helyi Biztonsági Felügyelete (a továbbiakban: HBF) az egyes intézetek és szervezeti egységek működésében lát el ellenőrzési és koordinációs feladatot. A felügyelet célja annak vizsgálata, hogy a minősített adatok kezelésére vonatkozó jogszabályi és belső előírások a gyakorlatban is érvényesülnek-e. A helyi szintű ellenőrzés különösen fontos a büntetés-végrehajtásban, mivel a napi működés során itt jelennek meg leggyakrabban azok a kockázatok, amelyek közvetlen hatással lehetnek az információbiztonságra.

A felügyeleti tevékenység nem kizárólag hibakeresést jelent. A HBF szerepe kiterjed a megelőzésre, a szabályok egységes értelmezésének elősegítésére és a jó gyakorlatok kialakítására is. Összefoglalva a felügyelet nem „ellenőrként", hanem „biztosítékként" van jelen a szervezet működésében. A cél nem a szankcionálás, hanem annak elősegítése, hogy a minősített adatkezelés megfeleljen a jogi és szervezeti elvárásoknak.

Az irányítási és felügyeleti szintek elkülönítése egyben a felelősségi körök tisztázását is szolgálja. A központi irányítás a szabályalkotásért és az egységes végrehajtás feltételeinek biztosításáért felel, a biztonsági vezető a rendszer működésének szakmai felügyeletéért, míg a helyi biztonsági felügyelet a napi gyakorlat ellenőrzéséért. Ez a többszintű felépítés teszi lehetővé, hogy a minősített adatvédelem a büntetés-végrehajtásban ne formális előírások halmaza legyen, hanem ténylegesen működő, ellenőrizhető és fejleszthető rendszerként jelenjen meg.[6]

Végrehajtási és szakmai szerepkörök a minősített adatkezelésben

A minősített adatkezelés irányítási és felügyeleti szintjei önmagukban nem elegendőek a biztonság garantálásához. A rendszer tényleges működése azon múlik, hogy a végrehajtási és szakmai szerepkörök hogyan valósítják meg a jogszabályi és belső

6 A Büntetés-végrehajtás Országos Parancsnoksága minősített adatainak Biztonsági Szabályzatáról szóló 33/2020. (VII. 14.) BVOP utasítás

előírásokat a napi gyakorlatban. Ezek a szerepkörök alkotják azt az operatív réteget, ahol a minősített adatokkal való tényleges munka zajlik, legyen szó elektronikus adatkezelésről, iratkezelésről vagy rejtjeltevékenységről.

A bv. szervezetben a végrehajtási szerepkörök egyik meghatározó eleme a rejtjeltevékenység szakmai rendszere. A rejtjeltevékenység nem önálló informatikai feladatként jelenik meg, hanem a minősített adatvédelem integráns részeként. A rendszer szakmai irányítását a rejtjelfelügyelő látja el, aki a biztonsági vezető felügyelete mellett felel a rejtjeltevékenység jogszerű és szakszerű végrehajtásáért. A rejtjelfelügyelő feladatkörébe tartozik a rejtjelező eszközök alkalmazásának felügyelete, a rejtjelanyagok nyilvántartása, valamint annak biztosítása, hogy a rejtjeltevékenység megfeleljen az engedélyezési és biztonsági követelményeknek.

A rejtjelfelügyelő szerepe köztes pozíciót foglal el a stratégiai irányítás és a technikai végrehajtás között, azaz olyan szakmai felelősként írható le, aki biztosítja, hogy a rejtjelezés ne pusztán technikailag működjön, hanem jogilag és szervezetileg is megfeleljen az előírásoknak. A szerepkör jelentősége abban áll, hogy a rejtjeltevékenység során bekövetkező hibák vagy szabálytalanságok közvetlenül veszélyeztethetik a minősített adatok védelmét. Elkészíti a rejtjeltevékenységre vonatkozó biztonsági dokumentációt, érvényesíti az üzemeltetés-biztonsági szabályzat előírásait, valamint megismerteti azt a felhasználókkal.

A rejtjelezők végzik a rejtjeltevékenység közvetlen végrehajtását. Feladatuk a rejtjelező eszközök rendeltetésszerű használata, a kulcskezelési eljárások betartása, valamint az adatátvitel és adattárolás során alkalmazott rejtjelezési megoldások szakszerű használata. A tevékenység kizárólag megfelelő jogosultság és engedély birtokában végezhető, és szigorúan dokumentált eljárásokhoz kötött. A rejtjelezők nem hoznak döntéseket a minősítésről vagy a hozzáférési körökről, feladatuk a már meghozott döntések technikai végrehajtása.

A végrehajtási szerepkörök közé tartozik az informatikai rendszerek üzemeltetéséért felelős rendszeradminisztrátor is. A rendszeradminisztrátor feladata az informatikai környezet működtetése oly módon, hogy az megfeleljen a minősített adatok kezelésére vonatkozó elektronikus biztonsági követelményeknek. A szerepkör technikai jellegű, és nem terjed ki a minősített adatok tartalmának megismerésére vagy értékelésére. A rendszeradminisztrátor a hozzáférési jogosultságok technikai beállításáért, a felhasználói fiókok kezeléséért, az eseménynaplók működtetéséért, valamint a mentési és helyreállítási eljárások végrehajtásáért felel.[7]

7 A büntetés-végrehajtási szervezet rejtjelszabályzatáról szóló 29/2020. (VII. 10.) BVOP utasítás

Szükséges hangsúlyozni, hogy a rendszeradminisztrátor nem „dönt" a minősített adatokról, hanem biztosítja azt a technikai környezetet, amelyben a jogszerűen meghozott döntések végrehajthatók. A szerepkör jelentősége abból fakad, hogy egy technikai hiba vagy nem megfelelő jogosultságkezelés ugyanúgy a biztonság sérüléséhez vezethet, mint egy tudatos jogsértés. A jogszabályok ezért a rendszeradminisztrátori tevékenységet is szigorú ellenőrzési és dokumentációs követelményekhez kötik.

A rendszerbiztonsági felügyelő a rendszer személyi, fizikai, adminisztratív, valamint rendszerbiztonsági feltételeinek biztosításáért felelős személy. Érvényesíti az elektronikus biztonsági követelményeket a rendszer teljes életciklusában, gondoskodik az engedélyezett rejtjelező eszközök telepítéséről, rendeltetésszerű és biztonságos működtetéséről, szükség szerinti karbantartásáról és javíttatásáról.

A végrehajtási és szakmai szerepkörök rendszerét az különbözteti meg az irányítási szintektől, hogy ezek a szereplők nem a szabályokat határozzák meg, hanem azok alkalmazásáért felelnek. A világos hatáskör-megosztás biztosítja, hogy a döntési jogkörök és a végrehajtási feladatok ne keveredjenek, ami a minősített adatkezelés egyik alapvető garanciája. A bv. szervezet működésében ez a megkülönböztetés hozzájárul ahhoz, hogy a minősített adatvédelem átlátható, ellenőrizhető és elszámoltatható módon valósuljon meg.

Iratkezelési és ellenőrzési szerepkörök a minősített adatvédelemben

A minősített adatkezelés biztonságos működésének egyik legfontosabb eleme az iratkezelési és ellenőrzési funkciók megfelelő kialakítása. A jogszabályi követelmények abból indulnak ki, hogy a minősített adat védelme nem ér véget a minősítési döntés meghozatalával vagy a technikai védelem alkalmazásával. A védelem hatékonysága azon is múlik, hogy az iratok és adatok mozgása, kezelése és ellenőrzése mennyire átlátható és visszakövethető a szervezeten belül.

A minősített iratkezelés operatív végrehajtásáért a titkos ügykezelő felel. A titkos ügykezelő szerepe sajátos helyet foglal el a minősített adatvédelem rendszerében, mivel tevékenysége közvetlenül kapcsolódik az iratok fizikai és adminisztratív kezeléséhez. Feladatkörébe tartozik a minősített iratok nyilvántartása, iktatása, őrzése, továbbítása, valamint a kiadás és visszavétel dokumentálása. Ennek alapján a titkos ügykezelő biztosítja azt, hogy a minősített iratok útja a szervezeten belül minden esetben nyomon követhető legyen.

A titkos ügykezelő tevékenysége szigorú személyi és jogosultsági feltételekhez kötött. A feladat ellátásához megfelelő személyi biztonsági tanúsítvány, valamint titoktartási nyilatkozat szükséges. A szerepkör nem terjed ki a minősített adatok tartalmi

értékelésére vagy a minősítési döntések meghozatalára. A titkos ügykezelő nem dönt az adat sorsáról, hanem a már meghozott döntések szabályszerű végrehajtásáért felel.

A minősített iratok kezelése során különös jelentőséggel bír az adminisztratív fegyelem. Az iratok nyilvántartása, mozgatása és tárolása kizárólag meghatározott rend szerint történhet, amelyet a belső szabályzatok részletesen rögzítenek. A dokumentáltság biztosítja, hogy egy esetleges biztonsági esemény vagy hiányosság esetén pontosan megállapítható legyen, mikor, hol és milyen körülmények között történt az eltérés. A rendszer ezzel nemcsak a megelőzést, hanem az utólagos felelősség megállapítását is szolgálja.[8]

Az ellenőrzési funkciók ellátásában kiemelt szerepet tölt be a HBF. A HBF az egyes bv. intézetek, szervezeti egységek szintjén vizsgálja, hogy a minősített adatkezelés jogszabályi és belső szabályzati követelményei ténylegesen érvényesülnek-e. Az ellenőrzés kiterjed az iratkezelési folyamatokra, a hozzáférési jogosultságok meglétére, a rejtjeltevékenység szabályszerűségére, valamint az elektronikus rendszerek biztonsági működésére.

A HBF szerepe nem merül ki az ellenőrzésben. A felügyeleti tevékenység célja a megelőzés és a támogatás, amely a szabályok helyes értelmezésének segítésén és a kockázatok korai felismerésén keresztül valósul meg. A hétköznapi olvasó számára ez úgy fogalmazható meg, hogy a felügyelet nem kizárólag „ellenőriz", hanem hozzájárul ahhoz is, hogy a minősített adatkezelés a mindennapi gyakorlatban jogszerűen és biztonságosan működjön.

Az iratkezelési és ellenőrzési szerepkörök együttes működése biztosítja a minősített adatkezelés egyik legfontosabb alapelvét: a visszakövethetőséget. A dokumentált iratkezelés és a rendszeres ellenőrzések révén a szervezet képes azonosítani a hiányosságokat, kezelni a biztonsági eseményeket, valamint folyamatosan fejleszteni a védelmi rendszert. A büntetés-végrehajtás működésében ez különösen fontos, mivel a szervezet sajátos feladatai fokozott biztonsági elvárásokat támasztanak az információkezeléssel szemben.

Rejtjelezés és elektronikus biztonság a bv. szervezetben

A rejtjelezés fogalma és szerepe a minősített adatvédelemben

A rejtjelezés a minősített adatok védelmének egyik legfontosabb technikai eszköze, amely elsősorban az elektronikus adatkezeléshez és adatátvitelhez kapcsolódik. Lényege abban

8 A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet

áll, hogy az információ tartalmát olyan módon alakítja át, amely az arra nem jogosult személyek számára értelmezhetetlenné válik, miközben az arra jogosult felhasználók megfelelő kulcs vagy jogosultság birtokában az adatot változatlan tartalommal vissza tudják állítani. A rejtjelezés így nem az adat elrejtését, hanem annak védett formában történő kezelését jelenti.

A témában kevésbé jártas olvasó számára a rejtjelezés ahhoz hasonlítható, mintha egy üzenetet olyan nyelven írnánk meg, amelyet kizárólag a címzett ért. Az információ fizikailag jelen van, de tartalma csak az arra jogosult számára válik hozzáférhetővé. A bv. szervezetben ez különösen fontos, mivel a minősített adatok egyre nagyobb arányban elektronikus formában keletkeznek, kerülnek tárolásra vagy továbbításra, és így ki vannak téve az elektronikus rendszereket érintő kockázatoknak.

A rejtjelezés szerepe túlmutat az adatátvitel védelmén. A minősített adatvédelem rendszerében a rejtjelezés a bizalmasság egyik alapvető garanciája, amely biztosítja, hogy az adat tartalma akkor sem válik megismerhetővé, ha az adathordozóhoz vagy az adatfolyamhoz illetéktelen személy fér hozzá. A bv. szervezet elektronikus rendszereiben kezelt információk esetében ez különösen jelentős, mivel így egy technikai vagy szervezeti hiba önmagában nem vezethet az adatok tartalmi kompromittálódásához.

Fontos hangsúlyozni, hogy a rejtjelezés nem önálló védelmi megoldásként értelmezendő. A jogszabályi és szakmai megközelítés abból indul ki, hogy a rejtjelezés kizárólag a személyi, fizikai és adminisztratív biztonsági intézkedésekkel együtt képes betölteni rendeltetését. A rejtjelezés nem helyettesíti a jogosultságkezelést, az elkülönített rendszerek alkalmazását vagy az ellenőrzési mechanizmusokat, hanem azok technikai megerősítését szolgálja. A büntetés-végrehajtásban ez a szemlélet biztosítja, hogy a technológiai védelem ne váljon öncélúvá, hanem szervezeti és jogi keretek között kerüljön rögzítésre.

A rejtjelezés alkalmazása a minősített adatkezelés során szoros összefüggésben áll a minősítési szintekkel. A magasabb minősítési szintű adatok kezelése szigorúbb rejtjelbiztonsági követelményeket von maga után, beleértve az alkalmazható algoritmusokat, eszközöket és kulcskezelési eljárásokat. A jogszabályi környezet ezzel biztosítja, hogy a technikai védelem mértéke igazodjon az adat kompromittálódása esetén várható kár nagyságához.

A kriptográfiai rendszerek gyakorlati biztonsága nem kizárólag az alkalmazott algoritmus matematikai tulajdonságaitól függ, hanem a kulcskezelési eljárások, rendszerüzemeltetés és szervezeti biztonsági intézkedések megfelelő működésétől is (László, 2009).

A bv. szervezet szempontjából a rejtjelezés jelentősége abban is megmutatkozik, hogy hozzájárul az elektronikus adatkezelésbe vetett szervezeti bizalom fenntartásához. A megfelelően alkalmazott rejtjelezési megoldások lehetővé teszik az elektronikus rendszerek biztonságos használatát olyan területeken is, ahol korábban kizárólag papíralapú iratkezelés volt elfogadott. A rejtjelezés ily módon nem csupán védelmi eszköz, hanem a modern, hatékony és jogszerű működés egyik előfeltétele a bv. szervezetben.

A rejtjelezés alkalmazása a bv. szervezet elektronikus rendszereiben

A bv. szervezet elektronikus rendszereiben kezelt minősített adatok védelme olyan összetett követelményrendszerhez kapcsolódik, amely túlmutat az általános informatikai biztonsági megoldásokon. A jogalkotó abból indult ki, hogy a minősített adatok elektronikus kezelése önmagában fokozott kockázatot jelent, ezért az ilyen rendszerek kialakítása és működtetése kizárólag szigorúan szabályozott feltételek mellett megengedett. A rejtjelezés ebben a környezetben a technikai védelem egyik alapvető eszközeként jelenik meg, amely az adatkezelés teljes életciklusát végigkíséri.

A minősített adatot kezelő elektronikus rendszerek egyik legfontosabb alapelve az elkülönítés elve. A gyakorlatban ez azt jelenti, hogy az ilyen rendszerek nem kapcsolódhatnak közvetlenül nyílt vagy nem ellenőrzött hálózatokhoz, működésüknek zárt, ellenőrzött informatikai környezetben kell megvalósulnia. A büntetés-végrehajtásban ez az elkülönítés nem csupán technikai feltételek tekintetében, hanem szervezeti és eljárási szinten is érvényesül, mivel a minősített adatkezeléshez kapcsolódó feladatokat elkülönített munkafolyamatok és jogosultsági rend támogatja.[9]

A rejtjelezés ebben az összefüggésben nem helyettesíti az elkülönítést, hanem annak technikai megerősítését szolgálja. A zárt rendszer önmagában nem zárja ki teljes mértékben a jogosulatlan hozzáférés vagy adatvesztés kockázatát, különösen akkor, ha az adat elektronikus formában kerül tárolásra vagy továbbításra. A rejtjelezés biztosítja, hogy egy esetleges hozzáférési hiba vagy fizikai kompromittálódás ne eredményezze automatikusan az adat tartalmának megismerhetőségét, így a rendszer nemcsak „zárva van", hanem az abban kezelt információk is „lezárt" állapotban maradnak.

A bv. szervezet elektronikus rendszereiben a rejtjelezés alkalmazása kiterjed az adattárolásra és az adatátvitelre egyaránt. Az adattárolás során alkalmazott rejtjelezési megoldások célja annak biztosítása, hogy az adathordozókhoz vagy a tárolórendszerhez való fizikai hozzáférés önmagában ne tegye lehetővé az adatok megismerését. Ez különösen

9 A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet

fontos olyan helyzetekben, amikor az adatok hordozható eszközökön, mentési adathordozókon vagy archivált formában kerülnek megőrzésre. A rejtjelezett adattárolás ily módon a fizikai biztonság kiegészítő, technikai garanciájaként jelenik meg.

Az adatátvitel rejtjelezése ezzel szemben az információk továbbítása során fellépő kockázatokat kezeli. A bv. szervezetben ez elsősorban az elkülönített rendszerek közötti adatcserét, valamint a belső hálózati kommunikációt érinti. A rejtjelezett adatátvitel biztosítja, hogy az információk tartalma a továbbítás teljes időtartama alatt védett maradjon, és ne legyen hozzáférhető sem illetéktelen felhasználók, sem technikai közvetítők számára. A jogszabályi követelmények e területen is a minősítési szinthez igazodó védelmet írnak elő.

A rejtjelezés alkalmazásának egyik központi eleme a kulcskezelés. A rejtjelezési megoldások biztonsága nem kizárólag az alkalmazott algoritmusokon múlik, hanem azon is, hogy a rejtjelkulcsok létrehozása, tárolása, felhasználása és cseréje milyen szabályok szerint történik. A bv. szervezetben a kulcskezelési eljárások szigorúan szabályozottak, és kizárólag arra jogosult személyek végezhetik. Ez azt jelenti, hogy a „kulcs" kezelése legalább olyan fontos, mint maga a „zár".

A rejtjelezés alkalmazása az elektronikus rendszerekben szorosan kapcsolódik a dokumentáltság és az ellenőrizhetőség követelményéhez. A rejtjelezési eljárásoknak, konfigurációknak és jogosultságoknak minden esetben nyomon követhetőnek kell lenniük, hogy egy esetleges biztonsági esemény során megállapítható legyen a kiváltó ok, a felelősségi kör és a szükséges intézkedések. A dokumentált működés nem csupán ellenőrzési eszköz, hanem a jogszerű adatkezelés egyik alapfeltétele is.

Összességében a rejtjelezés alkalmazása a büntetés-végrehajtás elektronikus rendszereiben nem önálló technikai megoldásként értelmezendő, hanem a minősített adatvédelem komplex rendszerének részeként. A zárt környezet, a jogosultságkezelés, a szervezeti ellenőrzés és a rejtjelezés együttese biztosítja, hogy az elektronikus adatkezelés megfeleljen a jogszabályi követelményeknek és a szervezet sajátos biztonsági elvárásainak.

Elektronikus biztonsági követelmények és az engedélyezési rendszer

A minősített adatok elektronikus kezelése a bv. szervezetben nem pusztán informatikai kérdés, hanem szigorúan szabályozott jogi és szervezeti folyamat. A jogalkotó abból indul ki, hogy egy elektronikus rendszer önmagában kockázatot hordoz, mivel az adatok sérülékenysége a technológiai környezetből fakadóan magasabb, mint a kizárólag papíralapú iratkezelés esetében. Az elektronikus biztonsági követelmények célja ezért annak biztosítása, hogy a minősített adatokat kezelő rendszerek kialakítása,

működtetése és ellenőrzése minden körülmények között megfeleljen a védendő információk súlyának.

Az elektronikus biztonsági követelményrendszer egyik alapelve, hogy minősített adatot kezelő informatikai rendszer nem helyezhető üzembe automatikusan, vagy kizárólag szervezeti döntés alapján. A rendszer használatához a Nemzeti Biztonsági Felügyelet által lefolytatott előzetes engedélyeztetési eljárás szükséges, amelynek során vizsgálatra kerül, hogy az adott technikai megoldás alkalmas-e a meghatározott minősítési szintű adatok kezelésére. Az engedélyezés célja nem az informatikai fejlesztések akadályozása, hanem annak biztosítása, hogy a technológiai megoldások ne gyengítsék a minősített adatvédelem egészét.[10]

A rendszer engedélyezése során több szempont együttes értékelése történik. Vizsgálni kell a rendszer architektúráját, az elkülönítés gyakorlati megvalósulását, a jogosultságkezelés módját, valamint az alkalmazott rejtjelezési megoldások megfelelőségét. A rendszer csak akkor kaphat engedélyt, ha bizonyítható, hogy a minősített adatok bizalmassága, sértetlensége és rendelkezésre állása a teljes üzemeltetési idő alatt biztosított. Ez azt jelenti, hogy a rendszernek jól működőnek, valamint biztonságosnak és ellenőrizhetőnek is kell lennie.

Az elektronikus biztonsági követelmények nem kizárólag technikai paramétereket határoznak meg. A szabályozás hangsúlyt fektet az adminisztratív és szervezeti feltételekre is, ideértve a dokumentációs kötelezettségeket, az üzemeltetési rendet, valamint a felelősségi és jogosultsági körök egyértelmű rögzítését. A dokumentált működés biztosítja, hogy egy adott rendszer használata nem személyhez kötötten, hanem ellenőrizhető szabályok mentén történik.

Az engedélyezési rendszer szerves részét képezi a folyamatos felügyelet és ellenőrzés. Az engedély nem végleges és nem korlátlan időre szóló felhatalmazás, hanem feltételekhez kötött jogosultság. A rendszer működésében bekövetkező változások – például technológiai frissítések, konfigurációs módosítások vagy szervezeti átalakulások – újabb vizsgálatot tehetnek szükségessé. A szabályozás ezzel biztosítja, hogy az egyszer megfelelőnek minősített rendszer a későbbiekben se váljon biztonsági kockázattá.

A bv. szervezetben az elektronikus biztonsági követelmények gyakorlati alkalmazását a belső szabályozás konkretizálja. *A Büntetés-végrehajtás Országos Parancsnoksága minősített adatainak Biztonsági Szabályzatáról* szóló 33/2020. (VII. 14.) BVOP utasítás és a rejtjeltevékenységre vonatkozó helyi intézkedések jogszabályi előírásokra épülve

10 A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet

határozzák meg az egyes rendszerek használatának részletszabályait, az engedélyezési és ellenőrzési eljárások rendjét, valamint az érintett szereplők felelősségi körét. A belső normák jelentősége abban áll, hogy a jogszabályi kereteket a bv. szervezet sajátos működési környezetéhez igazítják.

Az elektronikus biztonsági követelmények és az engedélyezési rendszer összességében azt szolgálják, hogy a minősített adatok elektronikus kezelése ne elszigetelt informatikai feladatként jelenjen meg, hanem a minősített adatvédelem integrált, jogilag szabályozott és szervezetileg ellenőrzött részeként. A rendszer biztosítja, hogy a technológiai fejlődés előnyei a bv. szervezetben úgy hasznosuljanak, hogy közben a biztonsági kockázatok kezelhető szinten maradjanak.

Ellenőrzés, felelősség és jogkövetkezmények a minősített adatkezelésben

Ellenőrzési mechanizmusok és felügyeleti rend

A minősített adatkezelés jogszerű és biztonságos működése nem tekinthető statikus állapotnak, hanem folyamatos ellenőrzést igénylő folyamat. A jogalkotó abból indul ki, hogy még a legszigorúbb szabályozás és a legkörültekintőbb szervezeti kialakítás sem képes önmagában kizárni a hibák, mulasztások vagy szabályszegések lehetőségét. Az ellenőrzési mechanizmusok célja ezért nem kizárólag a jogsértések feltárása, hanem a kockázatok időben történő felismerése és kezelése.

A bv. szervezetben az ellenőrzési rendszer több szinten működik. A központi irányítás által meghatározott szabályok végrehajtását helyi szinten ellenőrzik, biztosítva, hogy a minősített adatkezelés ne csak formálisan, hanem a napi gyakorlatban is megfeleljen az előírásoknak. A BVOP HBF kulcsszerepet tölt be ebben a rendszerben, mivel közvetlen rálátással rendelkezik az intézetek működésére, és az ott zajló adatkezelési folyamatokra.

A szakirányítói ellenőrzések kiterjednek a minősített iratkezelés adminisztratív rendjére, a hozzáférési jogosultságok meglétére és megfelelőségére, a rejtjeltevékenység szabályszerűségére, valamint az elektronikus rendszerek biztonsági működésére. A dokumentáció vizsgálata kiemelt jelentőségű, mivel a minősített adatkezelés egyik alapelve a visszakövethetőség. A megfelelően vezetett nyilvántartások és naplók lehetővé teszik annak megállapítását, hogy egy adott adat mikor, hol és milyen körülmények között került kezelésre.

Az ellenőrzési tevékenység nem kizárólag eseti vizsgálatokból áll. A rendszeres, tervszerű ellenőrzések célja a folyamatos megfelelés biztosítása, míg az eseti ellenőrzések jellemzően konkrét eseményekhez, változásokhoz vagy bejelentésekhez kapcsolódnak. A két

forma együttes alkalmazása teszi lehetővé, hogy a bv. szervezet rugalmasan reagáljon a változó biztonsági környezetre, miközben fenntartja a jogszerű működés kereteit.

Felelősségi rendszer és kötelezettségek

A minősített adatkezeléshez kapcsolódó felelősségi rendszer világosan elkülöníti az irányítási, felügyeleti és végrehajtási szinteket. A felelősség megállapítása minden esetben ahhoz a szerepkörhöz és hatáskörhöz igazodik, amelyben az adott személy vagy szervezeti egység eljár. Ez az elv biztosítja, hogy a felelősség ne váljon elmosódottá, és egy esetleges jogsértés vagy biztonsági esemény bekövetkezésekor egyértelműen megállapítható legyen az érintettek köre.

A minősítési döntésekért elsődlegesen a minősítésre jogosult személyek tartoznak felelősséggel. A felelősség nem csupán a minősítés meghozatalára, hanem annak indokoltságára, arányosságára és időbeli korlátozására is kiterjed. A minősítő köteles gondoskodni arról, hogy a minősítés fennmaradása kizárólag addig tartson, ameddig a védett érdek ezt ténylegesen indokolja.

A biztonsági vezető felelőssége a minősített adatvédelem rendszerének egészére terjed ki. Ide tartozik a belső szabályozás alkalmazásának felügyelete, az ellenőrzési mechanizmusok működtetése, valamint a feltárt hiányosságok kezelése. A rejtjelfelügyelő és a rejtjelezők felelőssége a rejtjeltevékenység szakszerű és előírásszerű végrehajtásához kapcsolódik, míg a rendszeradminisztrátor, a rendszerbiztonsági felügyelő és a titkos ügykezelő felelőssége végrehajtó jellegű, a technikai és adminisztratív szabályok betartására irányul.

A felhasználók és közreműködők felelőssége a minősített adatok rendeltetésszerű kezelésében jelenik meg. A jogosultság megléte nem mentesít a szabályok betartása alól; minden érintett köteles az adatokat kizárólag a feladatellátás céljából, a meghatározott keretek között felhasználni. A Mavtv. változásai kapcsán fontos hangsúlyozni, hogy a felhasználói jogosultság önmagában nem biztosít elegendő felhatalmazást egy adott feladat végrehajtásához. Egy konkrét ügyben történő eljárás csak akkor válik jogszerűvé és végrehajthatóvá, ha azt vezetői szignálás is megerősíti. Ez a szabályozás biztosítja, hogy az egyedi döntések mögött egyértelműen azonosítható felelősségi rend és ellenőrizhetőség álljon.

Jogkövetkezmények és intézkedések

A minősített adatkezelés szabályainak megsértése jogkövetkezményekkel jár, amelyek súlya az elkövetett cselekmény jellegéhez és következményeihez igazodik. A jogkövetkezmények célja nem kizárólag a szankcionálás, hanem a jogszerű állapot helyreállítása,

és a hasonló esetek megelőzése. A büntetés-végrehajtásban ez különösen fontos, mivel egyetlen adatkezelési hiba is súlyos következményekkel járhat.

A jogsértések kezelése során elsődleges szempont a biztonsági események haladéktalan feltárása és dokumentálása. Az intézkedések köre kiterjedhet fegyelmi eljárás megindítására, jogosultságok korlátozására vagy visszavonására, valamint szükség esetén hatósági eljárások kezdeményezésére. A szervezeti intézkedések mellett indokolt lehet a belső szabályozás felülvizsgálata is, amennyiben a jogsértés rendszerszintű hiányosságokra mutat rá.

A jogkövetkezmények alkalmazása szorosan kapcsolódik az ellenőrzési és felelősségi rendszerhez. A következetes kontroll nemcsak a jogsértő magatartás visszaszorítását szolgálja, hanem hozzájárul a minősített adatkezelés biztonsági kultúrájának erősítéséhez is. A bv. szervezet működésében ez a kultúra alapvető feltétele annak, hogy a minősített adatvédelem hosszú távon is hatékony maradjon.

Összegzés és következtetések

A tanulmány a rejtjelezés és a minősített iratkezelés rendszerét a bv. szervezet sajátos működési környezetében vizsgálta jogi, szervezeti és technikai megközelítésben. Az elemzés rávilágított arra, hogy a minősített adatvédelem nem elkülönült részfeladat, hanem olyan összetett rendszer, amelyben a jogi szabályozás, a szervezeti struktúra és a technikai védelem egymást feltételezve és erősítve működik.

A minősített adat fogalmának és alapelveinek bemutatása egyértelművé tette, hogy a minősítés nem az információk indokolatlan elzárását szolgálja, hanem a közérdek védelmét. A szükségesség és arányosság elvének érvényesítése, valamint a „szükséges ismeret” elve olyan garanciális elemek, amelyek biztosítják, hogy a minősítés alkalmazása összhangban maradjon a demokratikus jogállami működés követelményeivel. A bv. szervezetben ez különösen nagy jelentőséggel bír, mivel a szervezet feladatai eleve fokozott alapjog-korlátozással járnak.

A minősítésre jogosult személyek körének és a minősítési eljárás rendjének elemzése rámutatott arra, hogy a minősítés minden esetben vezetői felelősséget hordozó döntés. A minősítői felelősség nem merül ki a döntés meghozatalában, hanem kiterjed annak indokoltságára, időbeli korlátozására és felülvizsgálatára is. A szabályozás ezzel biztosítja, hogy a minősítés dinamikusan kövesse a tényleges kockázati környezetet, és ne váljon rutinszerű gyakorlattá.

A szervezeti rendszer bemutatása igazolta, hogy a minősített adatkezelés biztonsága kizárólag világosan elkülönített felelősségi és hatáskörök mellett valósítható meg.

A központi iránymutatás, a rejtjeltevékenység szakmai irányítása, valamint az iratkezelési és ellenőrzési funkciók egymásra épülő struktúrát alkotnak. A titkos ügykezelő, a rendszeradminisztrátor és a helyi biztonsági felügyelet szerepe jól példázza, hogy a minősített adatvédelem nem kizárólag vezetői vagy technikai kérdés, hanem a szervezet teljes működését átható feladat.

A rejtjelezés és az elektronikus biztonsági követelmények elemzése rámutatott arra, hogy a technikai védelem önmagában nem elegendő a minősített adatok biztonságának garantálásához. A rejtjelezés kizárólag a személyi, fizikai és adminisztratív biztonsági intézkedésekkel együtt képes betölteni rendeltetését. Az engedélyezési és ellenőrzési rendszer szerepe abban áll, hogy a technológiai megoldások alkalmazása ellenőrzött, dokumentált és jogilag megalapozott keretek között maradjon.

Az ellenőrzési, felelősségi és jogkövetkezményi mechanizmusok vizsgálata igazolta, hogy a minősített adatkezelés megsértése nem csupán egyéni mulasztásként, hanem szervezeti kockázatként is értelmezendő. A következetes ellenőrzés és a jogkövetkezmények alkalmazása hozzájárul a biztonsági kultúra fenntartásához és fejlesztéséhez, amely a bv. szervezet működésének elengedhetetlen feltétele.

Összességében megállapítható, hogy a bv. szervezetben alkalmazott minősített adatkezelési és rejtjelezési rendszer olyan komplex, több szinten működő struktúrát alkot, amelyben a jogi szabályozás, a szervezeti felépítés és a technikai védelem elválaszthatatlan egységet képez. A rendszer hatékonysága nem kizárólag a technológiai fejlettségtől függ, hanem attól is, hogy a szervezet mennyire képes következetesen alkalmazni a szabályokat, kezelni az emberi tényezőt, valamint működtetni az ellenőrzési mechanizmusokat. A bemutatott keretek együttesen alkalmasak arra, hogy a büntetés-végrehajtás működése során keletkező minősített adatok védelme hosszú távon is biztosított maradjon.

Felhasznált irodalom

29/2020. (VII. 10.) BVOP utasítás a rejtjeltevékenység rendjéről

33/2020. (VII. 14.) BVOP utasítás a Büntetés-végrehajtás Országos Parancsnoksága minősített adatainak Biztonsági Szabályzatáról

90/2010. (III. 26.) Korm. rendelet a minősített adat kezelésének rendjéről

161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és felügyeletének szabályairól

2009. évi CLV. törvény a minősített adat védelméről

László Zsuzsanna (2009): Rejtjelbiztonság. Hadmérnök, 4(2), 375-384. Online: http://www.hadmernok.hu/2009_2_laszlo.php (Letöltés ideje: 2026. február 24.)