

Juhász Zsolt¹ – Virányi Gergely² –
Hegedűs Tamás³ – Viztra Tímea⁴

A Nemzetbiztonsági Szakszolgálat hatósági feladatai

The Authority Functions of the Special Service for National Security

A Nemzetbiztonsági Szakszolgálat szervezettörténetét az elmúlt évtizedekben a hatósági feladatkörök megjelenése és kiszélesedése is jellemezte. Biztonsági okmányok védelme, elektronikus információbiztonság, minősített adat védelme. A cikk ezen címek alatt mutatja be a három, nemzetbiztonsági szempontból is kiemelt jelentőségű hatósági tevékenységet, amelyek jelenleg a Nemzetbiztonsági Szakszolgálat feladatrendszerébe tartoznak.

Biztonsági okmányok védelme: az okmánybiztonság nemzetbiztonsági jelentőségű kérdés, amelynek a történelem során mindig is kiemelt jelentősége volt. A cikkben az okmányvédelem történeti alakulását foglaljuk össze, amelyet napjaink szabályozásának bemutatása követ. Magyarországon a Nemzetbiztonsági Szakszolgálat Szakértői Intézete látja el a biztonsági okmányok védelmével összefüggő hatósági feladatokat. A 86/1996. (VI. 14.) Korm. rendelet határozza meg a biztonsági okmányok védelmével kapcsolatos szabályokat. A Szakértői Intézet közreműködik az értékpapírok előállításának, valamint a biztonsági papírok szállításának engedélyezési eljárásában is.

Elektronikus információbiztonság: társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmosságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibetér védelme.⁵ A feladatkörhöz tartozó hatósági tevékenységet a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete látja el.

¹ Dr. Juhász Zsolt, Nemzetbiztonsági Szakszolgálat Szakértői Intézet, Hatósági Osztály vezetője.

² Dr. Virányi Gergely: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, Nemzeti Elektronikus Információbiztonsági Hatóság munkatársa.

³ Hegedűs Tamás: Nemzetbiztonsági Szakszolgálat Nemzeti Biztonsági Felügyelet, Minősített Adatkezelési Hatósági Osztály vezetője.

⁴ Dr. Viztra Tímea: Nemzetbiztonsági Szakszolgálat Nemzeti Biztonsági Felügyelet, Nemzetközi Együttműködési és Koordinációs Osztály vezetője.

⁵ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztségéről preambulumban.

Minősített adat védelme: Az Országgyűlés a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvénnyel létrehozta a Nemzeti Biztonsági Felügyeletet. A Nemzeti Biztonsági Felügyelet önálló feladattal és hatósági jogkörrel a Nemzetbiztonsági Szakszolgálat szervezeti keretei között, főosztály jogállású szervezeti egységként működik. Feladata a nemzeti és a külföldi minősített adatok védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, az iparbiztonsági hatósági feladatok, valamint a minősített adatok védelmét érintő nemzetközi bizottságokban és munkacsoportokban történő nemzeti érdekérvényesítés ellátása.

Kulcsszavak: biztonsági papír, biztonsági okmány, engedélyezés, elektronikus információbiztonság, ellenőrzés, értékpapír, lbtv., incidenskezelés, incidenskoordináció, kockázatmenedzsment, biztonság tudatosság minősített adat, Nemzetbiztonsági Szakszolgálat, Nemzeti Biztonsági Felügyelet, okmánybiztonság, Nemzeti Kibervédelmi Intézet, Szakértői Intézet

The history of the Special Service for National Security has also been characterised in the past decades by the appearance and extension of authority functions: document security, security of information services, protection of classified information. The article describes the three authority activities which are also highlighted in national security terms and belong currently to the tasks of the Special Service for National Security.

Document security: Document security is a national security issue, which has always had an outstanding importance during history. The article presents a historical perspective of document security, then describes the present regulation. The Institute for Expert Services of the Special Service for National Security (SSNS IES) is the document security authority in Hungary. Government Decree 86/1996 contains the current regulation. The SSNS IES contributes to the authorisation procedure of stock production, and to the authorisation procedure of transportation of security papers.

Electronic information security: Society expects arrangements for the protection of the confidentiality, integrity and availability of data and information managed in electronic information systems that are indispensable for the state and its citizens, as well as the integrity and availability of the relevant system elements on a comprehensive and continuous basis, in a closed system, and commensurately with risks, and hence the protection of the cyberspace. The related tasks are performed by the National Cyber Security Centre of the Special Service for National Security as a responsible authority.

The protection of classified information: The Hungarian Parliament with Act No. 85/1998 on the National Security Authority established the body of the National Security Authority. The National Security Authority operates with independent task and magisterial status within the organisational structure of the Special Service for National Security as a Department. The tasks of the NSA are the protection, supervision and accreditation of handling classified information by law, industrial security tasks regarding classified information and promoting the national interests in connection with protection of classified information by an active participation at various international committees and working groups.

Keywords: security paper, security document, authorisation, accreditation, electronic information security, control, inspection, stock, Cybersecurity Act, incident management, incident coordination, IT risk management, security awareness, classified information, Special Service for National Security, National Security Authority of Hungary, document security, National Cyber Security Centre, Institute for Expert Services

Biztonsági okmányok védelme

Az okmánybiztonsággal kapcsolatos hazai feladatokat jelenleg a biztonsági okmányok védelmének rendjéről szóló 86/1996. (VI. 14.) Korm. rendelet szabályozza, amely alapján a kapcsolódó hatósági feladatokat Magyarország egyik nemzetbiztonsági szolgálata, a Nemzetbiztonsági Szakszolgálat (NBSZ) látja el. Az okmányvédelem állami feladata nagy múltra tekint vissza.

Az okmányvédelem mint (nemzet)biztonsági érdek

Az okmányok védelmének igénye az okmányokkal egyidős. Az írásbeliség terjedése a mindenkori közhatalom (állam) számára is lehetőséget biztosított a különböző kiváltságok, jogok megfelelő igazolására (például oklevelek kiadása stb.). A hatalom birtokosa által kiadott oklevelek és egyéb iratok kiállításával egyidős az azok hitelesítése iránti igény, azaz mai fogalmakat használva mindig is a hatalom mindenkori birtokosának alapvető biztonsági érdekei közé tartozott az általa kiadott (ok)iratok hamisítás ellen történő védelme.

A történelemben számos alkalommal lelhetünk fel példát a különböző csalók felbukkanására (például a személyiségüket valamilyen okból megváltoztató, nyomait eltüntetni akaró, nem valós jogokat birtokló személyekről szóló esetek). Egy másik ember személyazonosságának felvétele – az írott dokumentumok megjelenése óta – együtt jár a hamis okmányok megjelenésével. Az okmányok, dokumentumok hamisítása a legrégebb bűncselekmények közé tartozik.

A hamisítók mindig is számíthattak a méltó büntetésre. Magyarországon az első kodifikált büntető törvény az 1878. évi V. törvénycikk (az úgynevezett Csemegikódex) volt, amely a *Magyar büntetőtörvénykönyv a büntettekről és a vétségekről* címet viselte. Jól mutatja a hamisítás elleni küzdelem fontosságát, hogy már ebben a jogszabályban is – nagy részletességgel! – megjelenik az okiratokkal kapcsolatos bűncselekmények szabályozása. A Csemegi-kódex XXXII. fejezete az *Okirathamisítás* címet viselte, a 391. §-tól a 407. §-ig terjedt, és felölelte a hatályos Btk. (2012. évi. C. törvény) által szankcionált szinte valamennyi okirattal kapcsolatos bűncselekményt. A hazai büntetőjogi szabályozás változásait vizsgálva megállapítható, hogy az okiratok hamisításával kapcsolatos bűnös cselekmények folyamatosan, a kezdetektől napjainkig büntetendőnek minősültek.

A büntetőjogi következmények jellegükből fakadóan utólagosak, azaz csak a már elkövetett hamisítási cselekmények szankcionálása valósul meg általuk. Nyilvánvalóan

a szankcióknak is van visszatartó ereje, azonban kizárólag a szankcióktól megelőző szerep nem várható. Az állam alapvető biztonsági érdeke a hamisítások megelőzése, azaz nemcsak a hamisítások elkövetőinek megbüntetése a cél, hanem kívánatos a kiadott okiratokat olyan hitelesítéssel és védelemmel is ellátni, amely már eleve megnehezíti a hamisítások elkövetését (a lehetetlenné tétel nem reális elvárás). A különböző korok különböző okirat-kibocsátói ehhez a mindenkori, elérhető technikai vívmányokat hívták segítségül, és alkalmazták a különböző védelmi megoldásokat. Az írásbeliség fejlődése hívta életre a nyomdaipart, a nyomdaipar fejlődése pedig párhuzamos az okmánybiztonsági technikák, technológiák fejlődésével is. Az utóbbi évtizedekben ehhez a nyomdaipari fejlődéshez csatlakozott az informatika. Napjaink biztonsági okmányaiban a legújabb nyomdaipari technológiák mellett fejlett informatikai védelmi megoldásokat is alkalmaznak.

Az okmányvédelem hatósági felügyelete Magyarországon

Más országokhoz hasonlóan Magyarország is felismerte az okmányvédelem – megelőző funkciójából fakadó – fontosságát, és alkalmazta is a kor technikai színvonalához képest legfejlettebb okmánytechnikai megoldásokat a kiadott okmányaiban.

A magyar úti okmányok történetét feldolgozó szakirodalom az első magyar útlevélnek a Batthyány-kormány belügyminisztere, Szemere Bertalan által hitelesített úti okmányokat tekinti, amelyek első kiállítása 1848 áprilisában történt.⁶ Az akkoriban a leggyakoribb nyomdai eljárás a magasnyomtatás volt, ezzel szemben az első magyar úti okmányok már a nagy szakismeretet és gépi háttérrel igénylő könyomtatással készültek. Az előállítás nehézsége mellett az alkalmazott aprólékos mintázrendszer is nagyban hátráltatta ezen okmányok utánpótlását.⁷

A magyar biztonsági okmányokban alkalmazott okmányvédelem mindig az elérhető legmagasabb technológiai védelmet célozta, amely tudatos állami tevékenység eredménye. Az okmányvédelmi szempontok tudatos érvényesítése ezért jogi, szabályozási igényt is eredményezett.

Az okmányvédelem felügyelete hosszú múltra tekint vissza, és a kapcsolódó jogi szabályozás sem napjaink újdonsága.

A nemzetbiztonsági szolgálatok megalakulása idején az okmányvédelem felügyelete egy már kialakult, és jogilag szabályozott terület volt.

A Minisztertanács 3076/1973. számú határozata alapján a biztonsági okmányok védelmének szabályait a belügyminiszter utasításban szabályozta. Ez a Magyar Népköztársaság belügyminiszterének 1973. november 19-én kiadott, 024. számú, „Szigorúan titkos!” minősítésű utasítása volt.

Az utasítás meghatározta a biztonsági okmány fogalmát, és egy nem teljes körű felsorolással tartalmazta a biztonsági okmányok típusait is. Az utasítás hatálya kiterjedt valamennyi állami szervre, amely biztonsági okmányok kibocsátásával, illetőleg gyártásával foglalkozott.

⁶ SOM 2014, 47.

⁷ SOM 2014, 51.

A biztonsági okmányok védelme, gyártásának és kibocsátásának ellenőrzése a Belügyminisztérium Okmányvédelmi Szerve (OKSz) hatáskörébe tartozott. Ez a szerv volt okmányvédelmi szempontból az NBSZ Szakértői Intézetének szakmai elődszervezete.

Az utasításban foglaltak alapján a biztonsági okmányokat – az általuk biztosított jogoktól függően – védelem szempontjából az OKSz A, B és C osztályba sorolta. Az utasítás meghatározta a biztonsági okmányok rendszeresítésének szabályait is. A biztonsági okmányt gyártó szerv vagy vállalat az alap- és szövegnyomatról impri-matúrát volt köteles bemutatni, amelyet a kibocsátó szerv és az OKSz hagyott jóvá és engedélyezte a sorozatgyártást.

Az utasítás 1. számú melléklete tartalmazta a biztonsági okmányok nyomdatechnikai védelmi előírásait. Ebben a mellékletben szerepeltek az egyes védelmi osztályok alapelvei és a nyomdatechnikai kivitelezésük védelmi előírásai. A mellékletben rendkívül részletes technikai és technológiai előírások voltak megtalálhatók.

A demokratikus átalakulással 1990-ben megalakultak Magyarország nemzetbiztonsági szolgálatai. Az okmánybiztonsággal kapcsolatos feladatokat ekkortól kezdve a Nemzetbiztonsági Hivatal Szakszolgálati és Operatív Technikai Igazgatósága (SZOTI) látta el.

E tevékenységet 1990-ben a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról szóló 26/1990. (II. 14.) MT rendelet, és a módosításaként megjelent 90/1990. (V. 2.) MT rendelet a nemzetbiztonsági feladatok közé sorolták. A rendelet meghatározott feladatkörben hatósági jogkörrel ruházta fel a Nemzetbiztonsági Hivatalt, amely feladatokat az NBH SZOTI szervezeti egysége, az NBSZ Szakértői Intézet jogelődje végzett. Az 1990. évi rendeletek azonban nem tértek ki arra, hogy mely okmányok minősülnek biztonsági okmánynak, és melyek az okmányok védelmével összefüggő kibocsátói feladatok. A gazdasági átalakulással együtt járt a biztonsági okmányokat gyártók körének bővülése.

A rendszerváltozást követően a piacliberalizálás következtében a nyomdaipari vállalkozások száma is megnőtt, azonban a megrendelések száma ezt nem követte. Számos nyomdaipari vállalkozás a gazdasági problémái elől a hamisításban látta meg a kiutat. Jelentősen megnövekedett az útlevelel-hamisítások száma. A nagy tömegben megjelenő hamis okmányok a hitelességbe vetett közbizalmat rengették meg, így nemzetgazdasági, egyben nemzetbiztonsági problémát is generáltak. Általános tapasztalat továbbá, hogy a hamis okmányokkal elkövetett visszaélések már nemcsak nemzeti, hanem nemzetközi szinten is jelentkeztek, és akár ellenérdekű titkosszolgálati akciókhoz történő felhasználások is előfordultak (nem magyar okmányok esetében láttak napvilágot ilyen esetek).

A tájékoztatatlanság, a nem kellően részletes szabályozás eredményeként megnőtt az okmányhamisítások száma, és sürgetővé vált új szabályok kidolgozása.

A magyar okmánybiztonsági szabályozásban a nagy mérföldkő a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) megszületése volt. Az Nbtv. törvényi szinten rendelkezik a hazai biztonsági okmányok védelméhez kapcsolódó feladatokról, amelyeket a jogalkotó az Nbtv.-vel megalakított Nemzetbiztonsági Szakszolgálat-hoz telepített. Az okmányvédelemmel kapcsolatos hatósági feladatokat a Nemzetbiztonsági Szakszolgálat keretében működő Szakértői Intézet látja el. A szervezeti felállás az Nbtv. hatálybalépése óta nem változott.

A biztonsági okmányok előállításának engedélyezése hatósági eljárás keretében történik, ennek hátterét az Nbtv. megszületésekor az államigazgatási eljárás általános szabályairól szóló 1957. évi IV. törvény (Áe.), később pedig a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) tartalmazta. Az eljárási szabályokat jelenleg az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény határozza meg.

Az Nbtv. a biztonsági okmányok védelmével kapcsolatos részletszabályokat nem tartalmaz, hanem felhatalmazta a kormányt, hogy a biztonsági okmányok körét, a biztonsági okmányvédelemre jogosult szervezet feladat- és hatáskörét, valamint a biztonsági okmányvédelem eljárási szabályait rendeletben állapítsa meg.

Az Nbtv. 77. § (1) bekezdés b) pontjában kapott felhatalmazás alapján született meg a biztonsági okmányok védelmének rendjéről szóló 86/1996. (VI. 14.) Korm. rendelet (a továbbiakban: Korm. rendelet). A Korm. rendelet meghatározza a biztonsági okmányvédelem alapfogalmait, a biztonsági okmányok védelmének általános szabályait, a biztonsági okmány előállításának engedélyezési eljárását, az előállító és a kibocsátó kötelezettségeit és az okmányvédelem hatósági felügyeletét. A Korm. rendelet melléklete tartalmazza a biztonsági okmányok körének felsorolással történő meghatározását.

A Korm. rendeletben foglaltak alapján az NBSZ Szakértői Intézete hatósági feladatai keretében:

- ellátja a biztonsági okmány okmányvédelmi kategóriájához igazodó általános követelményrendszer meghatározásával kapcsolatos feladatokat (okmányvédelmi rendszerterv kidolgozása);
- engedélyezi a biztonsági okmányok előállítását, valamint az „A” okmányvédelmi kategóriába sorolt biztonsági okmány megszemélyesítéséhez alkalmazott eszköz és módszer alkalmazását.

Az NBSZ Szakértői Intézete az okmány-előállítás technológiai, technikai feltételeinek vizsgálatával működik közre a biztonsági okmány előállítójának kiválasztása során, valamint ellátja az okmányvédelmet érintő feltételek folyamatos fennállásának ellenőrzését.

A fentiekben túl tájékoztatással, tanácsadással segíti elő, hogy a biztonsági okmányok kibocsátói, előállítói, valamint az érintett egyéb szervezetek a biztonsági okmány védelmével kapcsolatos jogukat gyakorolhassák, kötelezettségeiket teljesíthessék.

A Korm. rendelet a hatálybalépése óta sok módosításon esett át, azonban a módosítások döntő többsége csak technikai jellegű volt, és a biztonsági okmányok körében történő változásokat szabályozta.

Hazánk csatlakozása az Európai Unióhoz az okmányvédelem területén is jelentős változásokat eredményezett. A korábban nemzeti hatáskörben lévő okmányfejlesztési feladatok és szabályozási tevékenység mára már megoszlik az Európai Unió és a tagállamok nemzeti hatóságai között. Az Európai Unió több biztonsági okmánynak minősülő okmány esetében is kötelező és közvetlenül alkalmazandó szabályozást alkotott, amely a Korm. rendelet megújulását is szükségessé tette.

Amikor hazánk az EU tagjává vált, a kormány az NBSZ Szakértői Intézetét jelölte ki Magyarország képviselőjére az okmánybiztonsággal foglalkozó EU szakbizottságban

(ügynevezett egységes vízumformátumért felelős bizottság vagy 6. cikk bizottság), amely feladatot azóta is az intézet lát el.

Az EU-csatlakozás miatti jogszabály-módosulás megváltoztatta a biztonsági okmányok körének meghatározását. A korábbi nem tételes felsorolás, taxatív és számított felsorolássá módosult. A felsorolás szerkezete az EU-szabályozást veszi alapul, és jelenleg is ez van hatályban.

A Korm. rendelet melléklete I. részében felsorolt biztonsági okmányok körébe az Európai Unió által a tagállamok részére egységesen, kötelezően és részleteiben meghatározott formai és biztonsági jellemzőkkel bíró, ügynevezett egységes formátumú okmányok tartoznak. Az okmányok megjelenését és védelmét részleteiben meghatározó technikai specifikációk kidolgozása az EU szakértői bizottságaiban folyó munka eredménye, és alkalmazásuk a tagállamok részére kötelező. Ez a csoport jelenleg három okmányból áll:

- vízumbélyeg,
- a vízum elhelyezésére szolgáló különlap,
- a tartózkodási engedély.

Ezen okmányok kiemelt védelmét az indokolja, hogy az Európai Unió tagállamain kívüli harmadik ország állampolgárai részére állítják ki ezeket, és az Európai Unió, illetve a schengeni térség tagállamaiba történő belépés, tartózkodás és szabad mozgás jogosultságát igazolják.

A Korm. rendelet melléklete II. részében felsorolt okmányok azon – egyébként nemzeti fejlesztési hatáskörbe tartozó – biztonsági okmányok, amelyekre vonatkozóan:

- az Európai Unió minimum okmánybiztonsági követelményeket fogalmaz meg, vagy
- az uniós vívmányok formai, tartalmi követelményeket, vagy
- egyéb biztonsági elvárásokat határoznak meg.

Ebbe a csoportba tartoznak többek között a személyazonosító igazolványok, az útlevelék és az 1 évnél hosszabb érvényességi idejű úti okmányok is.

A Korm. rendelet melléklete III. részében felsorolt okmányok azon – teljes mértékben nemzeti hatáskörbe tartozó – biztonsági okmányok, amelyek nem sorolhatók a fenti két csoportba. Ez a csoport két alcsoportra oszlik:

1. személyi és jogosultságot igazoló okmányok,
2. védelmet igénylő létesítmények, szervek, intézmények belépési engedélyei, belépésre jogosító igazolványai.

A biztonsági okmányokat tartalmuktól, az általuk keletkeztetett vagy igazolt jogosultságok, illetőleg kötelezettségek súlyától függően „A”, „B” vagy „C” okmányvédelmi kategóriába kell besorolni, a döntés miniszteri szinten történik.

A szabályozás következő mérföldköve 2015-ben jött el, amikor a Korm. rendelet módosításával megjelentek az elektronikus biztonsági okmányra vonatkozó speciális előírások. Elektronikus biztonsági okmánynak az informatikai adathordozót tartalmazó biztonsági okmány minősül.

Az elektronikus biztonsági okmányt – az irányadó okmányvédelmi kategórián túl – tartalmától, az általa keletkeztetett vagy igazolt jogosultságok, illetve kötelezettségek súlyától, és az informatikai adathordozón tárolt adat szenzitivitásától és felhasználásától függően „Kiemelt”, „Fokozott” vagy „Alap” okmányinformatikai védelmi kategóriába is be kell sorolni.

A Korm. rendeletben megjelenő felhatalmazás alapján az NBSZ Szakértői Intézete 2017-ben elvégezte valamennyi magyar biztonsági okmány átfogó, okmánybiztonsági szempontú felülvizsgálatát. Az okmánybiztonsági felülvizsgálat során a biztonsági okmányok legnagyobb része megfelelt az irányadó okmányvédelmi kategória követelményeinek. A felülvizsgálat megállapításairól a kibocsátók tájékoztatást kaptak, és megkezdték a szükséges intézkedések tervezését, majd azok végrehajtását.

A jogszabályban rögzítettek alapján a felülvizsgálatot az NBSZ Szakértői Intézete legalább öt évente ismételt elvégzi.

Az NBSZ Szakértői Intézete az elmúlt közel negyed évszázad során a magyar biztonsági okmányok védelmének erősítésére törekedett. Ez azt jelenti, hogy a hatósági felügyelet mellett okmányfejlesztési feladatokat is végez, amelyek keretében az elérhető legjobb védelemre törekszik a magyar biztonsági okmányok továbbfejlesztése során.

Jó példa erre az útlevífejlesztés. A magyar útleví fejlesztését – a gyártóval történő együttműködésben – mindig az okmánybiztonsági szerv végezte. Hazánk EU-csatlakozásával esett egy időbe a 2252/2004/EK rendelet megalkotása, a biometrikus útleví bevezetése az EU-tagállamaiban. A Korm. rendeletben biztosított felhatalmazás alapján a fejlesztési feladatokat az NBSZ Szakértői Intézete saját hatáskörébe vonta. A megújult útleví bevezetése határidőben megvalósult. Az arcképet elektronikusan is tartalmazó okmányok kiadása 2006. augusztus 29-től kezdődött meg, az adattartalom 2009-től az ujjenyomattal bővült.

Az NBSZ Szakértői Intézete az egységes EU-formátumú okmányok fejlesztésében is részt vesz. A 2012 és 2019 között valamennyi EU- és schengeni tagállam által kiadott vízumbélyeg UV-nyomata az intézet fejlesztése volt.

A személyazonosító igazolvány elektronikussá tételére vonatkozó kormányzati igény felmerülésekor az NBSZ Szakértői Intézet szintén saját hatáskörbe vonta a fejlesztést, amelynek eredményeképpen valósulhatott meg 2016. január 1-jétől az elektronikus személyazonosító igazolvány (a továbbiakban: eSZIG) kiadása. Az okmánybiztonsági szempontból teljesen megújult kártyaokmány informatikai tárolóelemet tartalmaz, amely alkalmassá teszi az okmányt az elektronikus személyazonosításra és lehetőséget biztosít az elektronikus ügyintézésre is. A nemzetközi követelményeknek megfelelő új okmány olyan multiapplikációs eszköz, amelynek használatához több elektronikus szolgáltatás is kapcsolódik. Az eSZIG kifejlesztését és bevezetését követően született meg az Európai Parlament és a Tanács (EU) 2019/1157 rendelete, amely az uniós polgárok személyazonosító igazolványai és a szabad mozgás jogával élő uniós polgárok és azok családtagjai részére kiállított tartózkodási okmányok biztonságának megerősítéséről szól, és amelyet 2021. augusztus 2-től kell alkalmazni. A 2016-ban bevezetett magyar eSZIG okmánybiztonsági szempontból megfelel az új követelményeknek is.

A forgalomban lévő biztonsági okmányok gyártásának felügyelete folyamatosan megvalósul. Az eredeti előállítóval történő változtatás nélküli utángyártás vizsgálata

(gyártásközi ellenőrzés) a gyártás helyszínén, illetve az előállító által megküldött minták alapján történik.

Szakhatósági feladatok

Az NBSZ Szakértői Intézeténél koncentrálnak okmány- és nyomdatechnikai szaktudás által más állami szervek, hatóságok eljárásainak támogatása is megvalósul.

Az intézet a 45/2016. (XI. 29.) NGM rendeletben kapott felhatalmazás alapján részt vesz a különböző zárjegyek okmánytechnikai védelmének kialakításában, továbbá szakhatóságként működik közre az alábbi két hatósági engedélyezési eljárásban.

1. A biztonsági papírok országhatárt átlépő kereskedelmének engedélyezése

A biztonsági papír a hamisítók számára nagyon értékes alapanyag, mert nem tartalmaz nyomatot, amelynek eltávolítása, módosítása egy jól megtervezett védelmi rendszer esetében jelzi a hamisítást, „szabadon” nyomtatható és így könnyebb a megtévesztésre alkalmas hamisítványok létrehozása.

Emlékeztető bűnügy volt Magyarországon az 5000 forintos bankjegy hamisítása a kilencvenes évek közepén. A biztonsági papírok szállítása az elkövetéskor még nem volt engedélyköteles Magyarországon, és egy vállalkozás mintegy 15 tonnányi mennyiséget importált egy német cégtől. A dán papírgyár miatt silkeborgi néven elhíresült papírszállítványnak Magyarországon nyoma veszett, és később kiderült, hogy az alappapírt az ötezsresek hamisításához is felhasználták. Az azonosított jelentős mennyiségű hamisítvány miatt a Magyar Nemzeti Bank előbbre hozta az 5000 forintos bankjegy tervezett kivonását. A silkeborgi papírokból még 2007-ben is volt lefoglalás.

Részben a silkeborgi papírok esete miatt Magyarország úgy döntött, hogy a biztonsági papírok országhatárt átlépő szállítását engedélykötelessé teszi. Tekintettel arra, hogy a kereskedelmi engedélyező hatóság (ezt a feladatot jelenleg Budapest Főváros Kormányhivatala látja el) nem rendelkezik szakismerettel a biztonsági papírok tekintetében, ezért az NBSZ Szakértői Intézete szakhatóságként működik közre az eljárásában. A szakhatósági vizsgálatok során az intézet azt vizsgálja, hogy a kérdéses papír biztonsági papírnak minősül-e, illetve hogy a mintaként rendelkezésre bocsátott papírból készül-e

- forgalomban lévő magyar bankjegy,
- a 86/1996. (VI. 14.) Korm. rendelet hatálya alá tartozó biztonsági okmány, vagy
- a 98/1995. (VII. 24.) Korm. rendelet hatálya alá tartozó értékpapír.

A megvalósult szállítások ellenőrzését a vámhatóság végzi.

2. Értékpapírok fizikai előállítása

Értékpapír fizikai előállítását Magyarországon csak a Magyar Nemzeti Bank által kiadott engedéllyel rendelkező nyomda végezheti 1995 óta. Az értékpapírpiacon dematerializálódása mellett kisebb számban, de továbbra is mutatkozik igény a fizikai értékpapírokra, így azok kiadása a jövőben is várható lesz.

Az engedélyező hatóságot az NBSZ Szakértői Intézete szakhatósági közreműködéssel segíti.

Az értékpapírok előállítása során kötelezően alkalmazandó minimum védelmi megoldásokat tartalmazó szabályzatot a Magyar Nemzeti Bank (korábban Pénzügyi Szervezetek Állami Felügyelete) adja ki. Az NBSZ Szakértői Intézete vizsgálja az engedélyezésre benyújtott értékpapírminták szabályzatnak történő megfelelését.

Az új értékpapírok mellett az értékpapírok utánnomása is ellenőrzés alá kerül. Utánnomásnak az adott kibocsátó konkrét értékpapírjának – ismételt megrendelés alapján – az eredeti értékpapírnyomdánál történő előállítása minősül. Az előállító a korábbival azonos megjelenéssel köteles az értékpapírok utánnomására, ennek ellenőrzésével működik közre az intézet az MNB eljárásában.

Az elmúlt közel negyed évszázad tapasztalatai alapján megállapítható, hogy a fenti két területen tevékenykedő cégek jogkövető magatartást tanúsítanak, és az engedélyezési eljárások alapvetően jól működnek. A kialakított szabályozás beváltotta a hozzá fűzött reményeket, a biztonsági szempontok érvényesülését.

Az elektronikus információbiztonság felügyelete

A kibertér fenyegetései

A kiberfenyegetések komplexitása és volumene folyamatosan növekszik, a kiberbűnözésből származó károk világszinten megközelítik az államok GDP-jének 1%-át, különféle (például iszlamista) szervezetek egyre intenzívebb módon használják fel a kibertér ideológiák terjesztésére és – akár magyar – állampolgárok befolyásolására, és egyre erőteljesebben jelennek meg az állami szereplők, és a vélhetően államilag támogatott kiberkémkedési műveletek.

A kiberbűnözés fő célja a pénzügyi adatok és a személyes adatok tömeges megszerzése, pénzügyi rendszerek befolyásolása. A személyes, pénzügyi adatok kibertámadások révén történő megszerzése nem új jelenség, de a módszerek összetétele változó trendet mutat. Korábban a potenciális áldozatokat közvetlenül megcélózva (például becsapós vagy fertőzött e-mail, hamis weboldal) kis tételben gyűjtöttek leginkább érzékeny adatokat, úgy az elmúlt években egyre több nagy horderejű, központi nyilvántartás elleni sikeres támadás látott napvilágot. Az adatlopáson túl elterjedt az elektronikus szolgáltatások károkozási célú megbénítása (úgynevezett elosztott szolgáltatás-megtagadásos támadásokkal), illetve kéretlen levelek és kártékony kódok terjesztése, robothálózatok (fertőzött gépekből álló, kártékony célra felhasználható hálózatok) kialakítása. A kiberbűnözés mellett jelentős fenyegetés a hacktivizmus, amely jellemzően ideológiai motivációjú támadásokat takar, valamilyen ideológiai cél elérése, vagy valamilyen ideológia közvetítése érdekében, (például az Anonymous csoport meghirdetett „kampányai”; a hazai migrációs válsággal kapcsolatos iszlamista háttérű weboldalrongálások).

Jelentős és egyre növekvő veszélyt jelentenek azok a – jellemzően kiberkémkedés célú – kifinomult, rejtett támadások, amelyek mögött feltételezhetően állami

„szponzoráció”, támogatás áll. A fő veszélyt a rendkívül szofisztikált támadások jelentik, amelynek keretében hosszú időn át elrejtve tudják végezni a tevékenységüket, ezáltal rendkívül hatásosan hajtják végre a megbízók által kijelölt célokat (információszivárogtatás, rombolás, kémkedés stb.). Az ilyen támadásokra jellemző a nagyfokú rejtőzködés, a hosszú ideig tartó lappangási időszak.

Nemzeti Kibervédelmi Intézet Hatósági Főosztály

Az Országgyűlés 2013-ban – figyelembe véve Magyarország Nemzeti Biztonsági Stratégiáját [1035/2012. (II. 21.) Korm. határozat], Magyarország Nemzeti Kiberbiztonsági Stratégiáját [1139/2013. (III. 21.) Korm. határozat], valamint ez utóbbit is megalapozó Európai Unió kiberbiztonsági stratégiáját – megalkotta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.), amely 2013. július 1-jén lépett hatályba.

Az Ibtv. célként fogalmazta meg a nemzeti elektronikus adatvagyon, valamint az állami- és önkormányzati szervek elektronikus információs rendszereinek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonságának erősítését; deklarálja, hogy az elektronikus információs rendszerek biztonságáért az üzemeltető, működtető állami szerv a felelős.

A törvény továbbá létrehozta a hazai kibervédelmi szervezetrendszer, amelynek alapvető rendeltetése, hogy az állami szervek információbiztonsági feladatainak végrehajtását biztonsági szolgáltatásokkal támogassa, ellenőrizze, az állami szervezetrendszer egésze tekintetében a biztonsgáttudatosságot fejlessze.⁸

Az újonnan hatályba lépő Ibtv. új szervezeti struktúrát hozott létre, amelynek egyik pillére az akkor, frissen megalakult, a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó Nemzeti Elektronikus Információbiztonsági Hatóság volt. A hatóság az első időszakban a Nemzeti Fejlesztési Minisztérium szervezetén belül működött. A hatóság akkori munkáját szinte kizárólag az Ibtv. és végrehajtási rendeletei határozták meg.

A hatóság legfőbb feladatai közé tartozott az Ibtv. alanyi hatálya alá tartozó állami és önkormányzati szervek elektronikus információs rendszereik biztonságának felügyelete. Az Ibtv. jogalanyait a törvény 2. §-a határozza meg. Ezek:

- a) a központi államigazgatási szervek, a kormány és a kormánybizottságok kivételével,
- b) a Köztársasági Elnöki Hivatal,
- c) az Országgyűlés Hivatala,
- d) az Alkotmánybíróság Hivatala,
- e) az Országos Bírósági Hivatal és a bíróságok,
- f) az ügyészségek,
- g) az Alapvető Jogok Biztosának Hivatala,
- h) az Állami Számvevőszék,
- i) a Magyar Nemzeti Bank,

⁸ <https://nki.gov.hu/intezet/tartalom/magunkrol/> (A letöltés dátuma: 2019. 12. 01.)

- j) a fővárosi és megyei kormányhivatalok,
- k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai, a hatósági igazgatási társulások,
- l) a Magyar Honvédség.

Ezen túl a fentiek számára adatkezelést végzők, valamint a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, illetve az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek védelmére is kiterjed az lbtv. hatálya.⁹

Feladatai körében a hatóság az első időszakban a több ezres ügyfélkör azonosításához szükséges adatokat, az elektronikus információs rendszerek adatait, biztonsági osztályát, és a kötelezően kinevezendő elektronikus információs rendszer biztonságáért felelős személyek adatait vette nyilvántartásba.

A jogalkotó eredeti szándéka szerint, két év elteltével az lbtv.-t felülvizsgálták, majd módosították, ezért 2015. január 1-jén a hatóság előbb a Belügyminisztérium, majd július 16-án a Nemzetbiztonsági Szakszolgálat szervezetébe került. Az NBSZ-en belül korábban, 2013-tól a Kormányzati Eseménykezelő Központ működött előbb a Szakértői Intézet főosztályaként, majd önálló főosztályként. A hatóság NBSZ-hez kerülésével a szervezeti egység igazgatóságként működött tovább 2015 októberétől Nemzeti Kibervédelmi Intézetként (NKI).

Az NKI megalakulásától a Hatóság Főosztályi státuszban, két fő szakterületen végzi feladatait: nyilvántartás és ellenőrzés. A Nyilvántartási Osztály hatósági aktus keretében regisztrálja az ügyfelektől beérkezett, az lbtv. előírásainak megfelelő adatokat. Ennek keretében a hatóság nyilvántartja és kezeli:

- a) a szervezet azonosításához szükséges adatokat,
- b) a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,
- c) a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefonszámát, e-mail-címét, a 13. § (8) bekezdésében meghatározott végzettségét,
- d) a szervezet informatikai biztonsági szabályzatát,
- e) a biztonsági eseményekkel kapcsolatos, az eseménykezelő központtól kapott értesítéseket.¹⁰

A hatóság felügyeleti jogkörében eljárva, az ellenőrzési osztály révén, a tárgyévvel megelőző év november 30-áig összeállított éves ellenőrzési terv alapján látja el auditjellegű

⁹ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

¹⁰ lbtv. 15. § (1) bekezdés.

feladatait.¹¹ Az éves ellenőrzési terv összeállításakor az lbtv. 14. §. (2) bekezdésének d) pontjában meghatározott és a belső normában szabályozott kockázatelemzés alapján kerülnek kiválasztásra az ellenőrzésre, valamint az utóellenőrzésre kiválasztott szervezetek. A Hatósági Főosztály kockázatértékelési tevékenységének ellátásáról Igazgatói Intézkedés került kiadásra. A hatóság a 2013. július 1-jétől a hatósági nyilvántartásában rendelkezésre álló és hatósági ellenőrzések során megállapított információk felhasználásával kockázatértékelést végez annak érdekében, hogy a hatósági felügyeleti hatáskörébe tartozó elektronikus információs rendszerekre hatással lévő biztonsági kockázatok feltárása és értékelése megtörténjen. A kockázatok értékelése alapján a főosztály a megállapított, elektronikus információs rendszerekre és jogalany szervezetekre hatással lévő kockázatok csökkentését, mérséklését támogató éves ellenőrzési tervet készíti.

A hatósági ellenőrzés alapvető eszköz a magyar állami és önkormányzati szervezetek kiberbiztonsági felkészültségének értékeléséhez. Az ellenőrzés tapasztalatai rávilágítanak arra, hogy a biztonságtudatos viselkedés szintje jelenleg még elmarad a kívánatostól, az alkalmazott biztonsági intézkedések tartalma az esetek többségében nem maradéktalan.

A hatósági ellenőrzések olyan tipikusnak számító hibákra képesek rávilágítani, minthogy a magas biztonsági osztályba sorolt szakrendszereket futtató számítógépeken az internetet, magán levelezési fiókokat, közösségi oldalakat a felhasználók korlátozások nélkül, szabadon használják, a számítógépekhez korlátozás nélkül csatlakoztathatók külső eszközök. Az lbtv. hatálya alá tartozó intézmények a felhasználókkal szemben az informatikai eszközökön sok esetben korlátozó, felügyeleti intézkedéseket nem alkalmaznak, így a rendszerek fokozottan kitetteké válhatnak az informatikai támadásoknak.

Az ellenőrzések adatai alapján megvalósul egy értékelő-elemző munka is, amely képes összefüggésekre rávilágítani, mint például az intézmény által a felhasználóknak nyújtott biztonságtudatosítási képzések tartalma, minősége és száma, valamint a felhasználók biztonsági felkészültsége, a felhasználói interakció következtében bekövetkező biztonsági események száma és kockázati szintje közötti relációk.

Azokban az esetekben, ahol magas biztonsági kockázatot tárnak fel – például a munkahelyi informatikai eszközök magáncélú használata esetén az eszközöket nem védik megfelelően, vagy a felhasználók jogosultságait nem korlátozzák – a kockázatok csökkentése érdekében a hatóság ezen szolgáltatásokhoz való hozzáférések azonnali megszüntetését, szabályozását írja elő, ismételt tudatosító előadások megtartását rendeli el.

A hatóság az ellenőrzések során nagy hangsúlyt fektet a hatályos információ-biztonsági szabályozás lényegi és központi elemeként jelentkező, az elektronikus információbiztonságért felelős személy feladatainak végrehajtására, hatáskörének gyakorlására. Az állami és önkormányzati szervek elektronikus információbiztonságért felelős személyt kijelölő megbízások, munkaköri leírások vizsgálatának általános

¹¹ 187/2015. (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 12. §.

tapasztalata, hogy a szervezetben elfoglalt helye alapján szakmai szempontból ezen személyek befolyástól mentes munkavégzése nem minden esetben biztosított (például a fejlesztésekért felelős informatikai vezető közvetlen beosztottjaként gyakorolja a hatáskörét). Ezen esetekben a hatóság javaslatot tesz a szervezeten belüli változtatásokra is.

Az elektronikus információbiztonságért felelős személy alapvető kötelezettsége az lbtv. 13 § (1) f) bekezdésben meghatározott együttműködés a hatósággal, eseménykezelő központtal. A hatóság külön vizsgálja az intézmény reagálóképességét és gyorsaságát többek között az intézmény részéről a biztonsági eseményekkel kapcsolatos bejelentések megtételének ideje, illetve az eseménykezelő központ részéről érkező, az incidensek hatását mérsékelni hivatott riasztások, tájékoztatók fogadása, feldolgozási ideje vonatkozásában is.

A hatósági ellenőrzések eredményeként kijelenthető, hogy az intézmények elektronikus információbiztonságának színvonala folyamatosan emelkedik, a szervezetek erre irányuló tevékenységének tervezettsége és szervezettsége emelkedő színvonalú. Ugyanakkor az információbiztonsági összehatás és költséghatékonyság növelése érdekében fejlesztésre szorul az intézmények együttműködési hajlandósága a központi fejlesztések megtervezése és implementálása, továbbá az ezek támogatásához kapcsolódó projektek hatókörének meghatározása és ennek felügyelete során.

A hatóság az intézmények információbiztonsági tevékenysége tervezésének és megvalósításának szakmai támogatása céljából, ellenőrzési tapasztalatait felhasználva több formában, rendszeresen megjelenő oktatási tevékenységet folytat. Ez az aktivitás az információbiztonsági tájékoztató eseti és rendszeres figyelmeztetések, tanácsok, sajtószemlék, szemléletformáló előadások, szórólapok elkészítésében és az érintettek részére történő eljuttatásában is tetten érhető. Emellett a közelmúltban került publikálásra a Közigazgatási Kibervédelmi Eszköztár, amely „fehér könyv” célja, hogy segítséget nyújtson a felhasználóknak, az informatikai üzemeltetőknek és vezetőknek, annak érdekében, miként növelhetik a meglévő biztonsági szintet, csökkenthetik a kockázatoknak való kitettséget, illetve milyen elvárt magatartásformát javasolt követniük, ezzel összefüggésben BM utasítást is kiadtak.¹²

A hatóság ellenőrzi továbbá a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában, az információbiztonsági követelmények megtartását.¹³ Ez praktikusán azt jelenti, hogy a projektnak, az új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesítenie kell.¹⁴

Fentiekén túl a hatósági főosztály látja el a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló az Európai Parlament és a Tanács (EU) 2016/1148 irányelvének (NIS direktíva) (31) pontjában meghatározott egyedüli nemzeti kapcsolattartó pont (*single point of contact – SPOC*) feladatát is. Az irányelv szerint a SPOC a hálózati

¹² 17/2019. (VIII. 15.) BM utasítás a Belügyminisztérium és a belügyminiszter által irányított szervek elektronikus információbiztonsággal összefüggő biztonság tudatos viselkedési kódexe kiadásáról.

¹³ lbtv. 16. § (1) bekezdés d) pontja.

¹⁴ lbtv. 8. § (7) bekezdés.

és információsrendszerek biztonságával kapcsolatos kérdések koordinálásáért és az uniós szinten folytatott határokon átnyúló együttműködésért felel, tekintettel arra, hogy az irányelv célja az, hogy bizalomteremtés révén javítsa a belső piac működését, a tagállami szervezeteknek képesnek kell lenniük eredményesen együttműködni a gazdasági szereplőkkel, és struktúrájukat ennek megfelelően kell kialakítani.¹⁵

A hatóság kiemelt feladatként tekint a biztonságtudatos magatartás kialakulásának elősegítésére, tudatosító előadások megtartásával, kiadványok készítésével végzi tudatosító tevékenységét. Az európai kiberbiztonsági hónap keretében minden évben konferenciát, illetve kiberversenyt szerveznek meg az érintett állami, valamint piaci szektor, illetve a releváns tudással rendelkező magánszemélyek találkozásának, együttműködésének elősegítése céljából.

A klasszikus állami és önkormányzati szerveken kívül a hatóság időközben több új feladatot is kapott. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény szerinti bejelentésköteles elektronikus kereskedelmi szolgáltatásokat (online piactér, kereső szolgáltatás, felhőszolgáltatás) nyújtók adatait szintén a hatóság tartja nyilván.

Az alapvető szolgáltatást nyújtók kijelölésében szintén jogszabályi változás várható a közeljövőben.

A jövő kihívásait jelenthetik az elektronikus ügyintézés kiterjedt használatának általánossá válása, továbbá érdekes aspektusa lehet a NIS-irányelv előírásai minőségi szempontú pontosításának hatása az NKI ügyfélkörére és eljárásaira (a várakozások szerint a hatósági eljárás szakmai minőségében gazdagodni fog a bővítésre kerülő ügyfélkör által már jelenleg is alkalmazott információbiztonsági irányítási rendszerek alapján megalkotott folyamatok integrálásának igénye miatt).

Nem szabad megfeledkeznünk a feltörekvő technológiák (5G; fintech megoldások; mesterséges intelligencia stb.) révén megjelenített információbiztonsági kihívások kezelésével összefüggő a jövőben előálló új típusú hatósági felügyeleti és tudatosítási feladatokról sem.

A minősített adat védelme

A Nemzeti Biztonsági Felügyelet létrehozása, feladatkörének bővülése

A Magyar Köztársaság Kormánya és az Észak-atlanti Szerződés Szervezete (NATO) által 1994. július 5-én aláírt Biztonsági Megállapodás, valamint a Magyar Köztársaság és a Nyugat-európai Unió (NYEU) között 1996. október 1-jén aláírt Biztonsági Megállapodás szerint Magyarország kötelezettséget vállalt arra, hogy az együttműködés

¹⁵ <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from> (A letöltés dátuma: 2019. 12. 01.)

során átvett minősített információkat a tagállamokban érvényes biztonsági normák szerint kezeli és őrzi.

Az előzőekben említett biztonsági megállapodások alapján létre kellett hozni egy nemzeti biztonsági hatóságot, amely felelős a NATO minősített információkra vonatkozó személyi, fizikai, adminisztratív és elektronikus biztonsági követelmények magyarországi érvényesítéséért.

Ezen előzményekre figyelemmel fogadta el az Országgyűlés a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvényt, amely 1999. január 18-i hatállyal létrehozta a Nemzeti Biztonsági Felügyeletet, és hatáskörébe utalta a NATO minősített információk komplex védelmének feladatát. A Nemzeti Biztonsági Felügyelet a polgári nemzetbiztonsági szolgálatokat irányító tárca nélküli miniszter irányítása alatt működő, országos hatáskörű közigazgatási szervként jött létre. A Nemzeti Biztonsági Felügyelet feladata lett, hogy felügyeleti funkciója gyakorlásán keresztül elősegítse és biztosítsa nemzeti szinten a NATO és a NYEU biztonsági szabályzataiban meghatározott azon biztonsági alapelveket és minimális követelmények betartását, amelyeket minden NATO-tagállamnak alkalmaznia és érvényesítenie kell annak érdekében, hogy a NATO és a NYEU minősített információk megfelelő védelmet kapjanak az engedély nélküli hozzáférés ellen.¹⁶

Hasonlóan a NATO-hoz, az Európai Unió (EU) is elvárta a csatlakozni készülő új tagállamaitól, hogy maradéktalanul megfeleljenek az EU biztonsági szabályzataiban, vagyis az Európai Unió Tanácsa, az Európai Bizottság, valamint az Európai Atomenergia Közösség biztonsági szabályzataiban foglalt előírásoknak, és kijelöljenek egy nemzeti biztonsági hatóságot, amely az EU felé szavatolja az EU minősített adatokkal kapcsolatos biztonsági követelmények betartását.¹⁷ Az EU biztonsági szabályzatai a NATO biztonsági szabályzatának rendszerét követik, gyakorlatilag azonos intézményi struktúra (Központi Nyilvántartó, Nyilvántartók, Ellenőrző pontok) létrehozását teszik kötelezővé, továbbá szövegezésük is hasonló. Figyelembe véve tehát, hogy az EU minősített adatok védelme terén hasonló jellegű és hasonló volumenű feladatok jelentkeztek, mint a NATO esetében, a 2003. évi LIII. törvény a Nemzeti Biztonsági Felügyeletet jelölte ki a feladatkör ellátására.

A nemzeti minősített adatok védelmének rendszere 2007 augusztusáig szervezetileg is elkülönült a külföldi (NATO, NYEU, EU) minősített adatok védelmének rendszerétől, amelynek egységes felügyeletét és szakmai irányítását a Nemzeti Biztonsági Felügyelet látta el. A nemzeti titokvédelmi rendszer megosztott volt, egyes részterületei eltérő irányítás alatt, elkülönítetten működtek, s így hatékonysága, szabályozottsága esetenként nem érte el a NATO-, EU-követelmények minimumát sem. A nemzeti minősített adatok védelmének szakmai felügyeletét a belügyminiszter látta el, a honvédségnél, valamint a polgári nemzetbiztonsági szolgálatoknál e jogkörét a hatáskörrel rendelkező miniszterrel együttesen gyakorolta. A Belügyminisztérium 2006. évi megszüntetését követően ez a feladatkör a Miniszterelnöki Hivatalhoz került.

A Nemzeti Biztonsági Felügyelet hatáskörének bővülése során újabb mérföldkövet jelentett a polgári nemzetbiztonsági szolgálatokat irányító tárca nélküli miniszter

¹⁶ HEGEDŰS 2018, 344.

¹⁷ HEGEDŰS 2018, 345.

feladat- és hatásköréről szóló 177/2007. (VII. 1.) Korm. rendelet, amely a miniszter hatáskörébe utalta a nemzeti minősített adatok szakmai felügyeletét, amellyel kapcsolatos feladatok ellátását a Nemzeti Biztonsági Felügyelet végezte.

Az Országgyűlés 2009. december 14-én tartott ülésén fogadta el a minősített adat védelméről szóló 2009. évi CLV. törvényt (a továbbiakban: Mavtv.), amely 2010. április 1-jén lépett hatályba.

A Mavtv. felhatalmazása alapján, a törvény végrehajtása érdekében 2010 tavaszán a kormány az alábbi három rendeletet alkotta meg:

- a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendeletet;
- az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendeletet;
- a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendeletet.

A Mavtv., illetve az annak végrehajtásáról rendelkező három kormányrendelet alapján változtatta meg a minősített adatok védelmének magyarországi rendszerét. E jogszabályok elfogadása különösen az alábbiak miatt bírt jelentőséggel:

- egységes védelmi követelményeket állapítanak meg a nemzeti és a külföldi minősített adatokra;
- a Mavtv. bevezette a négy szintű minősítési rendszert, ezért „Szigorúan titkos!”, „Titkos!”, „Bizalmas!” és „Korlátozott terjesztésű!” minősítési szinteket különböztetünk meg;
- az EU-telephely biztonsági tanúsítvány intézményének bevezetésével lehetővé vált a magyarországi gazdálkodó szervezetek részvétele az EU minősített beszerzésekben;
- Magyarországon első ízben született érdemi szabályozás az elektronikusan kezelt minősített adat védelmére;
- eddig hiányzó jogintézmények (például nemzeti személyi biztonsági tanúsítvány, nemzeti telephely biztonsági tanúsítvány) létrehozásával lehetőség nyílt arra, hogy Magyarország kétoldalú titokvédelmi megállapodásokat kössön.

A Nemzeti Biztonsági Felügyelet szervezete, jelenlegi feladatai

A Nemzeti Biztonsági Felügyelet önálló feladattal és hatósági jogkörrel a Nemzetbiztonsági Szakszolgálat szervezeti keretei között, főosztály jogállású szervezeti egységként működik.

A Nemzeti Biztonsági Felügyelet három osztályát – a Minősített Adatkezelési Hatósági Osztály, az Iparbiztonsági Osztály, az E-biztonsági Osztály – a minősített adatvédelem alrendszerének megfelelően alakították ki. A negyedik osztály a Nemzetközi Együttműködési és Koordinációs Osztály a Nemzeti Biztonsági Felügyelet nemzetközi szerepvállalásának és együttműködésének elősegítését, valamint a hazai jogszabályalkotással kapcsolatos feladatokat végzi.

Általánosságban szólva, a Nemzeti Biztonsági Felügyelet feladata a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint az iparbiztonsági hatósági feladatok ellátása.

A NATO és az EU tagországaiban a minősített adat védelméért felelős nemzeti hatóságoknak a kormányzati szervezetrendszerben elfoglalt helye, struktúrája eltérő képet mutat. Lényeges közös jellemzőként állapítható azonban meg annak a követelménynek az érvényesítése, hogy a nemzeti minősített adatok védelme a NATO-ban, illetve az EU-ban elfogadott biztonsági elveknek megfelelő legyen, ebből következően egy hatóság lássa el a külföldi (NATO, EU), illetve a nemzeti minősített adat védelmének felügyeletét.

A Nemzeti Biztonsági Felügyelet kodifikációs feladataival összefüggésben szakmailag előkészíti a minősített adat védelemről szóló jogszabályokat és a közjogi szervezetszabályozó eszközöket.

A Nemzeti Biztonsági Felügyelet egyedi közhatalmi aktusokkal kapcsolatos feladataival összefüggésben:

- a minősített adatot kezelő szervnél engedélyezi a minősített adatok kezelését, jogosult a kiadott adatkezelési engedély módosítására vagy visszavonására,
- engedélyezi a minősített adatok kezelésére szolgáló elektronikus rendszerek használatbavételét, jogosult a kiadott rendszerengedély módosítására vagy visszavonására,
- nyilvántartja az adatkezelési és rendszerengedéllyel rendelkező minősített adatot kezelő szervezet nevük és székhelyük feltüntetésével,
- ellátja a rejtjeltevékenység hatósági engedélyezését és felügyeletét [Mavtv. 20. § (2) a)-e) pont].

A Nemzeti Biztonsági Felügyelet az engedélyezési eljárást a minősített adatot kezelő szervek kérelmére az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény rendelkezéseire figyelemmel folytatja le és annak eredményeként határozat formájában adatkezelési, valamint rendszerengedélyt ad ki.

A Nemzeti Biztonsági Felügyelet európai uniós és nemzetközi feladatai körében:

- ellátja az Európai Unió Tanácsa, az Európai Bizottság, az EURATOM, az EUROPOL, az EUROJUST (a továbbiakban együtt: EU), a NATO és az ESA vonatkozó szabályzataiban, valamint a minősített adatok védelme tárgyában kötött nemzetközi szerződésekben a nemzeti biztonsági hatóságok számára előírt feladatokat,
- kapcsolatot tart a NATO, az EU, az ESA és a tagállamok illetékes szervezeteivel, és tevékenységéről – a szükséges mértékben – tájékoztatja azokat,
- ellátja a nemzeti érdekérvényesítést a minősített adatok védelmét érintő nemzetközi bizottságokban és munkacsoportokban,
- részt vesz a minősített adatok cseréjével járó két- vagy többoldalú biztonsági megállapodások, továbbá valamennyi olyan nemzetközi szerződés előkészítésében, amely minősített adatokat is érint [Mavtv. 20. § (2) m)–p) pont].

A Nemzeti Biztonsági Felügyelet egyéb feladataival összefüggésben:

- egyetértési jogot gyakorol a minősített adatot kezelő szervek biztonsági vezetőinek kinevezésével kapcsolatban [Mavtv. 20. § (2) f) pont];
- végzi az elektronikus adatkezelő rendszerek vagy azok elemeinek elektromágneses kompromittáló kisugárzásának méréseit, és ezek alapján meghatározza azok zónabesorolását [Mavtv. 20. § (2) s) pont];
- a minősített adatot kezelő szervnél vizsgálja a minősített adatok elvesztésével, illetéktelen személy tudomására jutásával, valamint a biztonság megsértésével kapcsolatos eseményeket [Mavtv. 20. § (2) k) pont];
- ellenőrzi a minősítők minősítési gyakorlatát, ennek eredményeként egyedi vagy általános ajánlást bocsáthat ki az egységes minősítési gyakorlat kialakítása érdekében, illetve kezdeményezheti a minősítés felülvizsgálatát [Mavtv. 20. § (2) g) pont];
- ellátja a minősített adatot kezelő szervnél a minősített adat kezelésének hatósági felügyeletét, ellenőrzi a minősített adat védelmére vonatkozó jogszabályok, valamint a személyi, fizikai, adminisztratív és elektronikus biztonsági szabályok betartását [Mavtv. 20. § (2) h) pont];
- kiadja a külföldi minősített adat felhasználói, továbbá a minősített adatot kezelő gazdálkodó szervezetek felhasználói részére a személyi biztonsági tanúsítványt [Mavtv. 17. § (1) bekezdés], továbbá a 90/2010. (III. 26.) Korm. rendelet alapján a különböző külföldi (NATO/EU) szervezeteknél történő munkavállalás, tanácskozás, gyakorlat, szövetségi szintű hadműveletek, békefenntartó műveletek esetén igazolja az adott szervezethez hivatalos célból kiutazó magyar állampolgárok személyi biztonsági tanúsítványainak meglétét és érvényességét;
- az arra jogosult gazdálkodó szervezetek részére telephely biztonsági tanúsítványt vagy egyszerűsített telephely biztonsági tanúsítványt ad ki, jogosult a telephely biztonsági tanúsítvány és az egyszerűsített telephely biztonsági tanúsítvány módosítására vagy a már kiadott tanúsítvány visszavonására [Mavtv. 20. § (2) i) pont];
- gondoskodik a jogutód nélkül megszűnt szervek által keletkeztetett minősített adatok felülvizsgálatának elvégzéséről [Mavtv. 20. § (2) l) pont];
- gondoskodik a biztonsági vezetők részére tartandó képzésről és továbbképzésről [Mavtv. 20. § (2) q) pont];
- együttműködik a Nemzeti Adatvédelmi és Információszabadság Hatósággal a közérdekű adatok megismeréséhez fűződő alkotmányos jog tiszteletben tartása és az információszabadság érvényesülése érdekében [Mavtv. 20. § (2) r) pont].

A Nemzeti Biztonsági Felügyeletnek a közigazgatási hatósági eljárásban hozott döntése ellen a döntés közlését követő 15 napon belül lehet közigazgatási pert kezdeményezni [Mavtv. 21. § (1) bekezdés].

A Nemzeti Biztonsági Felügyelet adatkezelése

A Mavtv. rendelkezik a Nemzeti Biztonsági Felügyelet által kezelt adatokról is. A jogszabály taxatívén felsorolja, hogy a Nemzeti Biztonsági Felügyelet milyen adatokat kezelhet a személyi biztonsági tanúsítvány kiadásához. Ezek az adatok a következők:

- az érintett személy természetes személyazonosító adatai, állampolgársága, úti okmányának okmányazonosítója, a minősített adat felhasználásához kötődő munkahelye, beosztása és feladatköre, a nemzetbiztonsági ellenőrzése során kitöltött biztonsági kérdőívben és a biztonsági szakvéleményben foglalt adatai,
- a kiadott személyi biztonsági tanúsítvány száma, kelte, érvényességi ideje és szintje [Mavtv. 22. § (1) bekezdés].

A fentiekben felsorolt adatokat a Nemzeti Biztonsági Felügyelet az érintett személy részére kiadott utolsó személyi biztonsági tanúsítvány érvényességi idejének lejártát vagy visszavonását követően a minősített adattal visszaélés bűncselekményére a Büntető törvénykönyvben meghatározott büntetési tétel felső határának megfelelő ideig kezeli [Mavtv. 22. § (2) bekezdés]. Amennyiben az érintett személy részére személyi biztonsági tanúsítvány kiadására nem kerül sor, a Nemzeti Biztonsági Felügyelet a célhoz kötöttség elvének megfelelően az eljárás befejezését követően köteles törölni az általa kezelt személyes adatokat [Mavtv. 22. § (3) bekezdés].

A Nemzeti Biztonsági Felügyelet ellenőrzései

A 90/2010. (III. 26.) Korm. rendelet szerint éves ellenőrzési terv alapján alkalmanként 2 fő részvételével, az állami szervek és a gazdálkodó szervezetek esetében komplex ellenőrzéseket hajt végre, amelynek keretében a személyi, fizikai, adminisztratív és elektronikus biztonsági szabályok érvényesülését, valamint a minősített adat védelmére vonatkozó jogszabályok alkalmazását vizsgálja. Az ellenőrzés megállapításairól minden esetben jegyzőkönyv készül, valamint a feltárt hiányosságok pótlására a Nemzeti Biztonsági Felügyelet végzésben kötelezi az ellenőrzött szervezetet. A végzésben meghatározott feladatok végrehajtásának nyomon követése érdekében utóellenőrzés elrendelésére is sor kerülhet.

A NATO a NATO Biztonsági Szabályzata [C-M(2002)49] alapján periodikusan – háromévenként – az EU és az EU intézményei az EU minősített adatok védelmére szolgáló biztonsági szabályokról szóló, 2013. szeptember 23-i 2013/488/EU tanácsi határozata szerint rendszeresen országellenőrzést hajtanak végre.

A 90/2010. (III. 26.) Korm. rendelet alapján a Nemzeti Biztonsági Felügyelet koordinálja a NATO, az EU és az EU intézményei által Magyarország területén végrehajtott, a NATO minősített adatai, valamint az EU és az EU intézményei minősített adatai védelmére irányuló ellenőrzéseket. Az országellenőrzések előkészítése, koordinálása, valamint az ahhoz kapcsolódó szakmai és protokoll tevékenységek szervezése és végrehajtása a Nemzeti Biztonsági Felügyelet feladata.

Az országellenőrzések a NATO, az EU és Magyarország jogrendszere összhangjának, a Nemzeti Biztonsági Felügyelet NATO, illetve EU minősített adatok védelmével

összefüggő hatósági tevékenységének, valamint a NATO és EU minősített adatok személyi, fizikai, adminisztratív és elektronikus biztonsági védelmével kapcsolatos jogszabályok érvényesülésének vizsgálatára terjednek ki.

Felhasznált irodalom

HEGEDŰS Tamás (2018): A Nemzeti Biztonsági Felügyelet mint a titkos információgyűjtést támogató szervezet. In RESPERGER István szerk.: *A nemzetbiztonság elmélete a közszolgálatban*. Budapest, Dialóg Campus Kiadó. 344–355.

SOM Krisztián (2014): *A magyar úti okmányok 1848–2012*. Nemzetbiztonsági Szakszolgálat – Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság.

Internetes forrás

<https://nki.gov.hu/intezet/tartalom/magunkrol/> (A letöltés dátuma: 2019. 12. 01.)

Jogforrások

161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól
177/2007. (VII. 1.) Korm. rendelet a polgári nemzetbiztonsági szolgálatokat irányító tárca nélküli miniszter feladat- és hatásköréről

17/2019. (VIII. 15.) BM utasítás a Belügyminisztérium és a belügyminiszter által irányított szervek elektronikus információbiztonsággal összefüggő biztonságtudatos viselkedési kódexe kiadásáról

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

1878. évi V. törvénycikk a magyar büntető törvénykönyv a büntettekről és a vétségekről
1957. évi IV. törvény az államigazgatási eljárás általános szabályairól

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

1998. évi LXXXV. törvény a Nemzeti Biztonsági Felügyeletről

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

2009. évi CLV. törvény a minősített adat védelméről

2012. évi C. törvény a Büntető Törvénykönyvről

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

2016. évi CL. törvény az általános közigazgatási rendtartásról

- 86/1996. (VI. 14.) Korm. rendelet a biztonsági okmányok védelmének rendjéről
- 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről
- 92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól
- A Magyar Népköztársaság belügyminiszterének 1973. évi 024. számú utasítása a biztonsági okmányok védelmének szabályairól
- A Tanács 2252/2004/EK rendelete a tagállamok által kiállított útlevelék és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról
- Az Európai Parlament és a Tanács (EU) 2019/1157 rendelete az uniós polgárok személyazonosító igazolványai és a szabad mozgás jogával élő uniós polgárok és azok családtagjai részére kiállított tartózkodási okmányok biztonságának megerősítéséről
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (2016. július 6.). Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=HU> (A letöltés dátuma: 2019. 12. 01.)