Dr. Nepp József

Néhány gondolat a minősített adatokkal való visszaélésről

A modern társadalmak legösszetettebb kihívásai közé tartozik a minősített adatok védelme, amely a nemzetbiztonság, a jogállamiság és az egyéni alapjogok határmezsgyéjén helyezkedik el. A visszaélések megelőzése és a hozzáférés szabályozása ezért kiemelt jelentőséggel bír, mivel a titkos információk illetéktelen kezekbe kerülése súlyosan veszélyeztetheti a közbizalmat és az állam működésének stabilitását. A jelen tanulmány célja a minősített adatok kezelése jogi kereteinek bemutatását követően a visszaélések visszaszorításának lehetőségeit veszi számba, kitérve a kérdéskörben a mesterséges intelligencia jelenlegi és esetleges jövőbeni szerepére.

A – nemzeti és a külföldi – minősített adat fogalmát a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) 3. § 1. a) és 1.b) pontjaiban találjuk meg.

A hivatkozott rendelkezések szó szerinti beidézésétől most eltekintünk, azokat elemezve ugyanakkor megállapíthatjuk, hogy részletes és átfogó fogalommeghatározást adnak, lényegüket tömörebben összefoglalva minden olyan információ minősített adatnak tekinthető, amelynek illetéktelen megismerése vagy közzététele a nemzet biztonsági érdekeit, védelmi képességeit vagy nemzetközi kapcsolatait súlyosan sértené, melynek szükségszerű és ésszerű velejárója az ezen adatok megismerésének korlátozása. Minden ország birtokában van olyan adatoknak, amelyek megismerését nemzetgazdasági vagy politika érdekből nem kívánja sem saját állampolgárai, sem más államok számára megismerhetővé tenni, ugyanakkor az emberiséggel egyidősnek tekinthető az a szándék és akarat, mely ezen adatok – a már említett gazdasági vagy politikai érdekből való – megismerésére irányul, melynek célja valamely előny megszerzése. Hosszú fejlődési utat bejárva Magyarországon a minősített adatok „Szigorúan titkos”, „Titkos”, „Bizalmas” és „Korlátozott terjesztésű” kategóriákba sorolhatók. A minősítési szinteket a 2009. évi CLV. törvény, a Mavtv. 4. § (1) bekezdésében meghatározott minősítők, valamint az ezen szakasz (2) és (3) bekezdésében felsorolt személyek átruházott minősítői jogkörükben eljárva állapíthatják meg, figyelemmel a Mavtv. 5. § (4) bekezdésében meghatározottakra figyelemmel, melynek célja, hogy a kockázat mértékéhez igazodó védelemmel lássa el a minősítési szintbe sorolandó adatokat, az alábbiak szerint:

„(4) Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele

a) rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Szigorúan titkos!”,

b) súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Titkos!”,

c) károsítja a minősítéssel védhető közérdeket, akkor „Bizalmas!”,

d) hátrányosan érinti a minősítéssel védhető közérdeket, akkor „Korlátozott terjesztésű!” minősítési szintű.”

Az idézett jogszabályi rendelkezések már megelőlegezik azt, hogy a különböző minősítési szintekhez mérten az adatok biztonsági feltételeinek megteremtése is nélkülözhetetlen. A jogalkotó erre tekintettel a minősített adatkezelés alapfeltételének írja elő, hogy minősített adatot kezelni csak a Nemzeti Biztonsági Felügyelet által kiadott engedély alapján lehet, akkor, ha az állami vagy közfeladat ellátásához nélkülözhetetlen. (Mavtv. 10. § (1) bekezdése.).

A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet (a továbbiakban: Rendelet) határozza meg személyi, a fizikai, az adminisztratív és az elektronikus biztonság körébe tartozó feladatokat, melynek kivonata elérhető a Nemzeti Biztonsági Felügyelet honlapján. [1]

A legrészletekbe menőbb jogszabályi rendelkezések, valamint a helyi viszonyokhoz igazodó saját szabályozás kidolgozása, illetőleg az azok pontos betartására irányuló szigorú intézkedések ellenére a minősített adat védelme sérülhet.

A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 265. §-a rendelkezik a minősített adattal való visszaélésről. A szabályozás szerint a cselekmény egyik elkövetési módja a minősített adat jogosulatlanul történő megszerzése vagy felhasználása, a másik a jogosulatlan személy részére hozzáférhetővé, vagy jogosult személy részére hozzáférhetetlenné tétele.

„Btk. 265. § (1) Aki minősített adatot

a) jogosulatlanul megszerez vagy felhasznál,

b) jogosulatlan személy részére hozzáférhetővé, vagy jogosult személy részére hozzáférhetetlenné tesz,

minősített adattal visszaélést követ el.

A minősített adat minősítési szintjéhez igazodóan határozza meg a törvény az elkövetési magatartáshoz igazodó büntetési tételeket.”

A Btk. fent hivatkozott definíciója véleményem szerint egyértelművé teszi, hogy a visszaélések alapja az emberi tényező. A továbbiakban még említésre kerülő, a minősített adat védelme érdekében elengedhetetlen biztonsági feltételek megteremtése mellett is a minősített adat védelmének sérülése az esetek legnagyobb részében szándékos vagy gondatlan emberi magatartásra vezethetők vissza.

Egy nyilvánosságra jutott hír szerint 2019-ben a történelem

1 https://www.nbf.hu/hasznos-informaciok/biztonsagi-vezetok-figyelmebe/ (Letöltés időpontja: 2025. szeptember 1.)

írásbeli érettségi vizsga megkezdését követően az Oktatási Hivatalhoz (OH) bejelentés érkezett arról, hogy egy közösségi oldal zárt csoportjában a középszintű történelemérettségi feladatsor esszétémáit a vizsga kezdete előtt közzétehették. Az Oktatási Hivatal ismeretlen tettes ellen büntetőfeljelentést tett, […] az ügyben a Készenléti Rendőrség Nemzeti Nyomozó Iroda minősített adattal visszaélés gyanúja miatt folytat nyomozást ismeretlen tettes ellen. [2]

Konkrét jogeset megjelölése nélkül, számos alkalommal állami hivatali dolgozó belső dokumentumokat juttatott el egy külső félnek.

Az esetekből levonható az a következtetés, hogy a minősített adat jogosulatlan megismeréséhez és azok jogosulatlanok számára való megismerhetőségéhez valamely *személy* által az adatokhoz való belső hozzáférés vezethetett. A mögötte lévő motiváció többféle lehet, úgy, mint anyagi haszonszerzés, de anyagi problémák miatti kiszolgáltatottá válás, esetleg zsarolás is állhat a háttérben, első esetben a motiváció a mozgatórugó, míg a további két esetben a sebezhetőségen van a hangsúly.

A Rendelet 16–35. §-ai részletekbe menően szabályozzák a minősített iratok tárolására szolgáló helyiségekre vonatkozó szigorú követelményeket, melyek biztonsági osztályoknak megfelelően állapítanak meg előírásokat. A rendelkezések kiterjednek a technikai-fizikai feltételekre, a be- és kiléptetésre, az élőerős őrzésre, és a szükséges karbantartási feladatokra. A *fizikai* biztonságra vonatkozó rendelkezések előírásoknak megfelelő kiépítése, majd az ezt követő üzemeltetése álláspontom szerint az egyik legstabilabb védelmi alapot jelenti a személyi-fizikai-adminisztratív-elektronikus biztonság együttesében.

Az *elektronikus* biztonság feltételeinek megteremtése szoros összhangban van a fizikai és az adminisztratív követelményeknek való megfeleléssel, melynek lényege az információs rendszer illetéktelenek számára történő hozzáférésnek megakadályozása. Ez egy olyan komplex terület, amely a már említett fizikai és adminisztratív előírásokon túl részletesen szabályozza a hardverek és szoftverek biztonságára vonatkozó előírásokat. Erről a Nemzeti Biztonsági Felügyelet részletes iránymutatást adott ki. [3]

Megállapíthatjuk, hogy a jogalkotó részletekbe menő szabályokat hozott a minősített adatok védelme érdekében, így a személyi biztonság területén a biztonsági tanúsítványok rendszere, a rendszeres biztonsági ellenőrzések és a titoktartásra kötelezés, a fizikai biztonság területén minősített adatok tárolására és feldolgozására szolgáló speciális, ellenőrzött területek (zónák), valamint a belépés-ellenőrzési rendszerek kiépítésének előírása, az adminisztratív biztonság terén az adat nyomon követhetősége, míg az elektronikus biztonság szférájában a titkosított kommunikációs csatornák, a hálózatok szegmentálása (a számítógépes hálózatok kisebb, elkülönített részekre osztása részben a jobb teljesítmény, részben a fokozott biztonság érdekében), a hozzáférési jogosultságok pontos szabályozása és a rendszeres auditok, az internetről leválasztott számítógépeken történő adattárolás mind hozzájárulnak a célhoz.

Ezek gyakorlati megvalósításában személyi oldalról nagy szerepe lehet a dolgozók számára tartandó rendszeres és alapos biztonsági képzéseknek, amelyek a jogszabályi előírások és az azok megszegése esetén kilátásba helyezett szankciók megismertetésén túl a kiberfenyegetések felismerésére és a felelősségteljes adatkezelésre fókuszálnak, míg technikai oldalról a titkosítási technológiák továbbfejlesztése, a viselkedésalapú elemzőrendszerek bevezetése, amelyek képesek a szokatlan adathozzáférési mintákat azonosítani, és a valós idejű fenyegetés-felderítési rendszerek továbbfejlesztése játszhatnak jelentős szerepet.

Bár jelenleg a mesterséges intelligencia (MI) közvetlen szerepe a minősített adatok kezelésében marginális, ugyanakkor kutatások rámutatnak, hogy az MI hatékony lehet a hozzáférési szokások és minták elemzésében, az anomáliák valós időben történő észlelésében, az incidensek utáni digitális nyomozásban, esetlegesen a gyanús viselkedés előrejelzésében.

Az MI elsősorban a visszaélés megelőzésében és felderítésében játszik egyre növekvő szerepet. Az MI-alapú rendszerek képesek hatalmas adatmennyiséget elemezni, és anomáliákat, szokatlan mintákat azonosítani, amelyek emberi beavatkozás nélkül észrevétlenek maradnának. Példának említhetjük az adatforgalom monitorozását vagy a felhasználói viselkedés elemzését.

Az MI képes lehet segíteni a már megtörtént incidensek utólagos elemzésében, a károk mértékének felmérésében és az elkövető(k) nyomon követésében, és bár nem helyettesíti a nyomozati munkát, jelentősen felgyorsíthatja azt azáltal, hogy korrelációkat és kapcsolati hálókat derít fel.

A jövőben az MI szerepe tovább nőhet a prediktív elemzés területén, azaz a fenyegetések előrejelzésében, mielőtt azok bekövetkeznének. Emellett a természetes nyelvfeldolgozás (NLP) segítségével az MI automatikusan képes lehet a titkosított dokumentumok elemzésére, felderítve azokat, amelyekben kompromittáló információk lehetnek.

A minősített adatok védelme nem csupán jogi vagy technikai kérdés, e téren kiemelt jelentőségű az egyéni szemléletmód fejlesztésének szükségessége is, amely a megelőzésen, az állandó odafigyelésen és a technológiai fejlesztések nyomon követésén és alkalmazásán alapul. A magyar jogi szabályozás nemzetközi viszonylatban is modern és átfogó, ugyanakkor a technológia fejlődésével a jogi kereteket is folyamatosan adaptálni kell. A mesterséges intelligencia a jövőben kulcsfontosságú partnerré válhat a titokvédelem területén, de a végső felelősség továbbra is az emberé marad.

2 https://24.hu/belfold/2019/05/09/tortenelemerettsegi-szivarogtatas-minositett-adattal-visszaeles-buntetes/ (Letöltés ideje: 2025. szeptember 1.)

3 https://nbf.hu/docs/EBK_4.2_allami_vegleges_2023.pdf (Letöltés ideje: 2025. szeptember 1.)