A Nemzeti Adatvédelmi és Információszabadság Hatóság 2018. évi beszámolója*

2018 report of the Hungarian National Authority for Data Protection and Freedom of Information

A NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) számára a 2018. év a GDPR (General Data Protection Regulation – az Európai Unió Általános Adatvédelmi Rendelete) jegyében telt el. A 2016-ban elfogadott uniós norma alkalmazása 2018 májusa óta hazánkban is kötelező, valamint ugyanebben az évben megtörtént az adatvédelmi csomag részét képező bűnügyi adatvédelmi irányelvek átültetése a magyar jogba, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) teljes körű módosítása is befejeződött. Számos egyéb (szektorális) adatvédelemmel kapcsolatos jogszabály GDPR-hez „igazítása" jelenleg is folyik, illetve a jövőben jelent jogalkotó munkát. „A nemzeti felügyeleti hatóságok elkezdték működtetni adatvédelmi incidens-bejelentő rendszerüket, lezárultak az első GDPR alapján lefolytatott vizsgálatok, és korrekciós hatáskörüket gyakorolva a tagállami adatvédelmi hatóságok kiszabták első, a megújult előírások alapján megállapított adatvédelmi bírságaikat…" – *Péterfalvi Attila*, a NAIH elnöke az éves beszámoló bevezetőjében így adott számot a 2018. évről (https://www.naih.hu/files/Beszamolo-2018-MR.PDF). A beszámoló a Hatóság működésének statisztikai adataival összefüggésben megállapítja, hogy „A Hatósághoz érkezett adatvédelmi tárgyú konzultációs beadványok száma megközelítőleg a duplájára emelkedett a korábbi évek számadataihoz viszonyítva, mely jelentős munkatöbbletet jelentett a Hatóság számára. A konzultációs beadványok közül 2409 adatvédelmi tárgyú, 88 pedig a közérdekű vagy közérdekből nyilvános adatok megismerhetőségére vonatkozott. Az adatvédelmi tárgyú konzultációs beadványok nagy száma – melyekben valamely polgár, adatkezelő vagy közfeladatot ellátó szerv tanácsot, tájékoztatást kér egy általa leírt adatkezelést érintően – azt mutatta, hogy a jogalkalmazók számára nagy volt a bizonytalanság a GDPR-ral kapcsolatban."

A vizsgálati eljárások tekintetében is hasonló tendenciát lehet megfigyelni, ugyanis „az 1205 vizsgálati eljárásból 827 adatvédelmi és 375 információszabadság tárgyú volt". Ez azt jelenti, hogy 2017-hez képest az adatvédelmi tárgyú vizsgálati eljárások száma közel duplájára emelkedett, ami szintén a GDPR bevezetésével hozható kapcsolatba.

A beszámoló szerkezete is igazodott a GDPR által generált új helyzethez, a személyes adatok védelmével kapcsolatos résznél például külön alfejezet szól arról, hogy a gyakorlat hogyan igazodott az adatvédelmi kö-

* A beszámolót összeállította *Lakatos Miklós*, a Központi Statisztikai Hivatal ny. szakmai főtanácsadója.

vetelményrendszer változásaihoz. Az adatvédelemmel kapcsolatban elsősorban azt kell megállapítani, hogy a vizsgált ügy a GDPR tárgyi hatálya alá tartozik-e vagy sem. Mellőzve a részleteket, itt csak egy kérdésre hívjuk fel a figyelmet, mégpedig arra, hogy ha az adatkezelést a természetes személyek kizárólag személyes vagy otthoni tevékenységek keretében végzik-e. Amennyiben igen, akkor ez a tevékenység nem tartozik a GDPR tárgyi hatálya alá. Ez az ún. „háztartási kivétel", ami azt feltételezi, hogy a személyes adatok kezelését nem lehet összefüggésbe hozni semmilyen szakmai vagy üzleti tevékenységgel.

„A »háztartási kivételek« közé tartozik többek között a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek. […]

Több megkeresés is érkezett a Hatósághoz a Facebook közösségi oldalon létrehozott csoportokkal kapcsolatban, amely csoportokat óvodai csoportok…, iskolai osztályok… hoztak létre a szülők és a pedagógusok közötti kommunikáció megkönnyítése érdekében. A Hatóság e megkeresésekre adott válaszban úgy foglalt állást, hogy az elhatárolás szempontjából a csoport összetételének van jelentősége: amennyiben e csoportok tagjai kizárólag a gyermekek és szülők, úgy az e csoportokban megosztott tartalom nem tartozik a GDPR tárgyi hatálya alá, azonban, amennyiben egy pedagógus is tagja a csoportnak, úgy nem mondható el, hogy a tevékenységnek ne lenne szakmai jellege, így az nem minősülhet háztartási kivételnek.

A Hatóság nem sorolta a háztartási kivételek közé a közösségi médiafelületeken nyilvánosan megosztott tartalmakat – például egy személy társkereső oldalon használt, képmást is tartalmazó profiljának egy nyilvános Facebook-csoportban történő megosztását … –, annak ellenére, hogy e tevékenységeknek sincs szakmai vagy üzleti vonzata, tekintettel arra, hogy ha a személyes adatot meghatározhatatlan számú ember ismeri meg, vagy ha az nyilvánosságra hozatalra kerül, akkor a kivétel nem alkalmazható.

A Hatóság a beadványok megválaszolása során a háztartási célú kivételek közé sorolta a turisták utazáson készült felvételeit, illetve a családi és baráti összejöveteleken történő képfelvétel-készítést is…, továbbá az iskolai rendezvényeken a szülők által gyermekükről készített felvételeket is, akkor is, ha azokon más gyermekek is szerepelnek…. Hangsúlyozandó, hogy a Hatóság kizárólag e felvételek elkészítését értékelte háztartási célú adatkezelésnek, amennyiben e képeket a készítő feltöltötte volna az internetre, az adatkezelés a GDPR hatálya alá tartozna."

A GDPR tartalmazza az adatvédelemmel kapcsolatos alapelveket, melyek között van olyan, ami eddig nem szerepelt sem a korábbi uniós adatvédelmi irányelvben, sem a magyar Infotv.-ben. Ezek közül „Kiemelkedő jelentőséget kap a GDPR 5. cikk (2) bekezdésében meghatározott elszámoltathatóság elve, amely alapján az adatkezelő felelős a GDPR 5. cikk (1) bekezdésben rögzített alapelvek érvényesülésének biztosításáért, továbbá képesnek kell lennie arra, hogy az adatkezelés ezen alapelveknek történő megfelelését igazolja. Az elszámoltathatóság elve az adatkezelő által tett adatvédelmi intézkedésekért való felelősségvállalást jelenti, valamint tartalmazza az adatkezelés megtervezésétől kezdődően annak végzésén keresztül az adatkezelési cél megvalósítása érdekében tett valamennyi intézkedést, a személyes adatokhoz való hozzáférést, adattovábbítást és azok adminisztrálását, igazolását."

A beszámoló külön alfejezetben sorolja fel azokat a jogeseteket, amelyek az alapelvekhez

kapcsolódnak. A személyes adatok kezelésének célhoz kötöttsége, az adattakarékosság elve az egyik legfontosabb alapelv. Az adatvédelmi biztosoknak, a NAIH-nak állandóan figyelmeztetni kellett az adatkezelőket arra, hogy csak a célnak megfelelő személyes adatokat kezeljék. „A Hatóság megállapította, hogy egy sportegyesület jogszerű cél nélkül kezel személyes adatokat, megsértve ezzel a GDPR 5. cikk (1) bekezdés b) pontjában szabályozott célhoz kötöttség elvét, amikor a bárki által használható futópályára történő belépéshez a sportolni szándékozó személy nevét és telefonszámát rögzíti. Az adatkezelés célját, illetve a mögötte húzódó érdeket adatkezelés nélkül is meg lehet valósítani.

A kitiltott vagy eltiltott személyek belépésének megtagadása és ezzel összefüggésben a jogsértés miatt eltiltott személyek azonosítása mint adatkezelési cél jogszerű lehet, ehhez azonban nem alkalmas eszköz valamennyi sportolni kívánó személy adatának a felírása, elegendő csupán a jogsértést elkövető személyek adatainak a rögzítése. Ez következik a GDPR 5. cikk (1) bekezdés c) pontja szerinti adattakarékosság elvéből is, mely szerint a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek, és a szükségesre kell korlátozódniuk.

A sportolók aktuális létszámának nyilvántartásával kapcsolatban a Hatóság álláspontja az volt, hogy ahhoz nem szükséges személyes adatok kezelése. Amennyiben a pályát használók számát szeretné nyilvántartani a sportegyesület, az megvalósítható bármilyen, az érintett azonosításra nem alkalmas jelzés alapján is."

A beszámoló külön alfejezetben foglalkozik a honlapok adatkezelésével. Mivel ez a tevékenység egyre több személyt, vállalkozást és intézményt érint, ezért érdemes e tárgyban a NAIH álláspontját részletesen idézni. „A NAIH 2018. évi gyakorlatában számos alkalommal felmerült a honlapok adatkezelésének kérdésköre. Az általános adatvédelmi rendelet 2. cikke alapján az általános adatvédelmi rendelet tárgyi hatálya az ott felsoroltakon kívül minden személyes adat kezelésére kiterjed függetlenül attól, hogy a honlap üzemeltetője nagyvállalat, kkv vagy magánszemély. Amennyiben egy honlap érintettek személyes adatát kezeli, akkor alkalmazni kell rá az általános adatvédelmi rendelet szabályait. […]

Az általános adatvédelmi rendelet 4. cikk 1. alpontja szerint személyes adat bármely olyan információ, amely akár közvetve akár közvetetten egy adott természetes személyhez köthető. Ebbe az úgynevezett »pszeudonim« vagy álnevesített személyes adatok is beletartoznak, mint a becenév vagy az e-mail cím akkor is, ha nem tartalmazza a természetes személy valódi nevét. A vissza nem fejthető hash-ek adott esetben lehet, hogy nem személyes adatok, de ezt csak az eset és az adatkezelés technikai megvalósításának összes körülménye alapján lehet megállapítani, hogy bárki által összeköthetőek-e egy természetes személlyel. Az adatkezelés az általános adatvédelmi rendelet 5. cikke alapján nem terjedhet ki az adott adatkezelési cél elérésére alkalmatlan, ahhoz nem feltétlenül szükséges, aránytalanul sok személyes adatra, és csak a célhoz feltétlenül szükséges ideig tarthat.

Az olyan sütik, szerver naplók (pl. IP címek naplózása), vagy egyéb személyes adatok kezelését, amelyek az adott honlap alapvető működéséhez és az informatikai rendszer biztonságához szükségesek, általában az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja szerinti jogos érdekre célszerű alapozni, mivel ha a honlap alapvető működéséhez és az informatikai rendszer biztonságához szükséges az adatkezelés, akkor enélkül a honlap objektíven nem lehet elérhető, ezért nem lehet érvényes hozzájárulás tárgya.

Az általános adatvédelmi rendelet 6. cikk (1) bekezdésének f) pontjára történő hivatkozás esetén fontos annak előzetes dokumentálása, hogy az adott konkrét jogos érdek(ek) érvényesítése előnyt élvez az adott helyzetben a honlapot használó érintettek személyes adataihoz fűződő rendelkezési jogához képest, és milyen technikai, szervezeti, eljárási intézkedések biztosítják azt, hogy az érintettek személyes adatai biztonságban legyenek (érdekmérlegelési teszt).

Az olyan sütik, szerver naplók, vagy egyéb személyes adatok kezelésére, amelyek az adott honlap alapvető működéséhez és az informatikai rendszer biztonságához nem szükségesek (pl. csak statisztikai, kényelmi, marketing, stb. célokat szolgálnak) általában az általános adatvédelmi rendelet 6. cikk (1) bekezdés a) pontja szerinti hozzájárulás szolgálhat jogalapként.

Az általános adatvédelmi rendeletnek megfelelő hozzájárulás alapvető…" feltétele szerint „…minimum követelmény, hogy a hozzájárulás megfelelő tájékoztatáson alapuló, önkéntes (negatív következmény nélkül megtagadható vagy visszavonható), egyértelműen kifejezett, és konkrét legyen, és az adott érintett általi hozzájárulás megtörténtét az adatkezelő az általános adatvédelmi rendelet 5. cikk (2) bekezdése alapján bármikor igazolni tudja. Az egyértelműen kifejezettség feltételét nem teljesíti a hozzájárulás, ha azt »előre kitöltött jelölőnégyzetes« módszerrel gyűjtik, a passzív magatartás nem minősül megfelelőnek. A konkrétság feltételét nem teljesíti a hozzájárulás, ha az egyes egymástól független adatkezelési célokhoz, illetve egyes egymástól független, különböző adatkezelők által végzett adatkezelésekhez nem lehet külön is hozzájárulni, kizárólag mindenhez egy »csomagban«."

A GDPR a felügyeleti hatóságok feladatául határozza meg, hogy összeállítsák és (a NAIH honlapján) nyilvánosságra hozzák azoknak az adatkezelési műveleteknek a listáját, amelyek esetén az adatkezelőnek kötelező hatásvizsgálatot készíteni. A 24 tételből álló hatásvizsgálati listából a következőket emeltük ki:

„1. Ha egy természetes személy egyedi azonosítását célzó biometrikus adatának kezelése módszeres megfigyelésre irányul. […]

6. Hitelképesség értékelése. Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagyszámú, illetve módszeres értékelése útján. […]

8. Harmadik személytől gyűjtött adatok további felhasználása. Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalakor.

9. Diákok, hallgatók személyes adatainak értékelésre való felhasználása. Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú. […]

14. Módszeres megfigyelés. Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera). […]

16. Munkavállalók munkájának megfigyelése. Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagyszámú és módszeres feldolgozása, illetve értékelése. Például GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából. […]

21. Új technológiai megoldások használata az adatkezelés során. Ideértve az érzékelővel

ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik."

A GDPR nagy súlyt helyez az adatvédelmi „incidensek" témájára. Az adatvédelmi incidens „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését (rendelkezésre állás sérülése), megváltoztatását (integritás sérülése), jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést (bizalmas jelleg sérülése) eredményezi."

A NAIH-hoz 2018-ban 244 incidenst jelentettek be: „a) A bejelentések legjelentősebb részét a téves címzés miatti félrepostázások, illetve téves címzett részére küldött elektronikus levelek adták. Az adatkezelőnek ilyenkor mindent meg kell tennie, hogy a téves címzett a birtokába jutott, személyes adatokat, tartalmazó dokumentumot, üzenetet megsemmisítse/törölje. Postai küldemény esetén az adatkezelő válaszborítékkal együtt küldött újabb levélben is kérheti a téves címzettet a nem neki szóló küldemény visszaküldésére. Gondoskodnia kell továbbá az adatkezelőnek arról, hogy a tényleges címzett is megkapja az üzenetet, valamint, amennyiben például az érintett személyes adatok jellege alapján az incidens kockázatát valószínűsíthetően magasnak, értékeli, tájékoztatnia kell az incidensről az érintettet. Az ilyen tájékoztatás másolatát is célszerű megküldeni a Hatóságnak. Hasonló magatartás várható el az adatkezelőtől akkor is, ha a címzettnek az egyébként neki szóló üzenettel együtt téves, személyes adatokat tartalmazó csatolmány is kiküldésre került, akár postán, akár elektronikus üzenetben."

A GDPR hatályba lépése csak a személyes adatok védelmével kapcsolatos szabályozási rendszert érinti, és a magyar Infotv.-nek is ez a része módosult. Mivel a magyar Infotv. az információszabadsággal kapcsolatos szabályrendszert is tartalmazza, ezért bizonyos szempontból a GDPR-nek is van szerepe az információszabadsággal kapcsolatos kérdések kezelésében. A beszámoló kiemeli, hogy „Amennyiben ugyanis a személyes adatok védelméhez való jog mellett valamely más, az adatok nyilvánosságával összefüggő alapvető jog – általában a közérdekű vagy közérdekből nyilvános adatok nyilvánosságához vagy a sajtó és véleménynyilvánítás szabadságához fűződő alapvető jogok – együttes vagy egymásra figyelemmel történő érvényesüléséről van szó, akkor az alkotmányos jogok esetleges kollízióját valamilyen módon fel kell oldani. Döntést kell hozni arról, hogy melyik érdek védelme szolgálja jobban a közérdeket, és ez a döntés milyen konkrét jogi rendelkezésekre, illetve jogelvekre vezethető vissza. Előfordulhat, hogy a jogaikban sértett személyek közszereplők (akik pozíciójuk, a helyi vagy országos életben betöltött funkciójuk vagy önkéntes szerepvállalásuk okán közvéleményformáló szereplővé lépnek elő, ugyanakkor személyes adataikat, magánszférájukat mások által veszélyeztetve érzik). Egyes esetekben azonban éppen a közszereplőnek minősülő közfeladatot betöltő személyek (például polgármesterek) választanak helytelen eszközt a jogsértések – jellemző módon az internet nyilvánossága előtt történő – »leleplezésére«, mások pellengérre állítására."

Nagyon fontos és a statisztikai adatok nyilvánosságát is érintő téma a közszféra információihoz történő hozzáférés: „2018-ban megkezdődött a közszféra információinak további felhasználásáról szóló 2003/98/EK

európai parlamenti és tanácsi irányelv (a továbbiakban: PSI irányelv) felülvizsgálata. A közszféra hatalmas adatmennyiséget állít elő (pl.: meteorológiai adatok, digitális térképek, jogszabályok stb.), ezek az adatok értékes forrásai a digitális gazdaságnak. Az Európai Bizottság értékelő jelentésében megállapította, hogy számos területen további intézkedés szükséges: ezek közé tartozik a dinamikus adatokhoz történő valós idejű hozzáférés biztosítása megfelelő technikai eszközök révén, a nagy értékű nyilvános adatok további felhasználás céljából való rendelkezésre bocsátásának növelése, a kizárólagosságot biztosító megállapodások új formáinak visszaszorítása, a határköltség szerinti díjszámítás elve alóli kivételek korlátozása. A NAIH is részt vesz a PSI irányelv módosításával kapcsolatos magyar álláspont kialakításában. A Hatóság tapasztalatai szerint Magyarország felkészültsége a nyílt hozzáférésű adatok („open data") tekintetében a múltban nem minősült sikeresnek; annak ellenére, hogy az irányelv átültetése a hazai jogrendbe megtörtént, annak végrehajtása tekintetében számos hiányosság merül fel."

A beszámoló sorra veszi az információszabadsággal kapcsolatos – korábbi években is felmerült –, gyakran előforduló témákat.

– Köztisztviselők adatainak a nyilvánossága: „A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény (a továbbiakban: Kttv.) 179. §-a alapján közérdekből nyilvános adat a név, állampolgárság, a foglalkoztató államigazgatási szerv neve, a szolgálati jogviszony kezdete, a besorolási adatok, a munkakör, a vezetői kinevezés időpontjai, a címadományozás és az illetmény. Fontos, hogy az Infotv. a közérdekből nyilvános személyes adatok esetében különbséget tesz az adatok megismerhetősége és az adatok terjesztése, illetve nyilvánosságra hozatala között, így például legfeljebb egy évig lehet az elektronikus közzétételi felületként szolgáló internetes honlapon közzé tenni a közérdekből nyilvános személyes adatokat tartalmazó nyilvános testületi ülésre benyújtott képviselőtestületi előterjesztéseket."

– A közpénzek, költségvetési támogatások átláthatósága: „A közpénzből finanszírozott megbízási szerződések, költségvetési támogatások, átláthatóságát szolgálja az Infotv. 27. § (3) bekezdése, nevesítve a helyi önkormányzatokat is és ex lege közérdekből nyilvános adatnak minősítve a költségvetési, illetve az európai uniós támogatás felhasználásával, az önkormányzati vagyon kezelésével kapcsolatos adatokat. Az ilyen jogviszonyba belépő másik (nem állami) szerződő felet pedig a törvény alapján – erre irányuló igény esetén – bárki felé tájékoztatási kötelezettség terheli. Így a költségvetési támogatások kedvezményezettjeinek a nevére, a támogatási program megvalósítási helyére vonatkozó adatok, illetve az államháztartás pénzeszközei felhasználásával, az államháztartáshoz tartozó vagyonnal, történő gazdálkodással összefüggő, ötmillió forintot elérő vagy azt meghaladó értékű árubeszerzésre, építési beruházásra, szolgáltatás megrendelésre, stb. vonatkozó szerződések megnevezése (típusa), tárgya, a szerződést kötő felek neve és az ott felsorolt további adatok közérdekből nyilvánosak és kötelezően közzéteendőek. A természetes személyek neve a fenti jogviszonyok tekintetében közérdekből nyilvános adatnak minősül. A költségvetési támogatásnak nem minősülő adatok esetében a természetes személyre vonatkozó adatok védelmet élveznek."

Az informatika robbanásszerű fejlődése előrevetíti annak lehetőségét, hogy a személyes adatok kezelése egyre hatékonyabb és központilag irányított lesz. Az adatkezelések rendszerét érintő nagy állami informatikai fejlesztési tervek ebbe az irányba mutatnak. A 2018. évi beszámoló külön alfejezetben foglalkozik ezzel a témával. A minisztériumi

anyagokban használt „Szitakötő” megnevezésű projekt „egy az ország valamennyi településén jelen lévő, egységes központosított rendszerbe szervezett, a közterületeken tartózkodók, a közlekedők és a tömegközlekedési eszközökön utazók intenzív és tömeges megfigyelést lehetővé tevő képi megfigyelő rendszer létrehozására vonatkozik. A következő adatok érzékeltetik a tervezett megfigyelőrendszer nagyságrendjét: 35 000 kamera képfolyamainak folyamatos gyűjtése a Kormányzati Adatközpontban, 25 000 TByte megfigyelési adat folyamatos kezelése és (a településeknél megjelenő további költségeket leszámítva) központi szinten legalább 50 milliárd forint közpénz elköltése mindennek megvalósítása érdekében. […]

A Hatóság kifogásolta, hogy a normaszöveg a lehető legáltalánosabb módon a gyűjtött adatok »felhasználására« ad lehetőséget, amibe a mindenkori technikai lehetőségek függvényében bármely felhasználási mód beleérthető a képfolyam egyidejű, ember általi megfigyelésétől kezdve a képállományok lementésén vagy más rendszerbe való áttöltésén keresztül akár a megfigyelt személyek automatikus biometrikus azonosításáig, mozgásának követéséig, továbbá viselkedési, valamint kapcsolati profiljának feltérképezéséig.”

A NAIH a rendszer bevezetését biztosító törvénytervezet egyeztetése során számos adatvédelmi garanciát javasolt annak normaszövegébe beépíteni. A kormányzati anyagokból az is kiderült, hogy a képi mellett a hangmegfigyelés felülvizsgálatát is szorgalmazta: „A Hatóság véleménye szerint azért lenne szükséges a szabályozás differenciálása, mert amíg a képi megfigyelés elsősorban egy adott helyszínen történtek megfigyelésére alkalmas – beleértve a helyszínen tartózkodók magatartását is –, az akusztikus megfigyelés és a hanginformációk rögzítése révén további érzékeny adatok, így különösen a helyszínen jelen lévők beszélgetése és egyéb magánjellegű közlései is megismerhetővé válnak. Ezek olyan többletinformációk, amelyek jellemzően semmiféle kapcsolatban nincsenek azzal az adatkezelési céllal, amely miatt a képi megfigyelőeszközt az adott helyszínen elhelyezték.” A „hallgatózás” jogához tehát szintén igen erős adatvédelmi garanciákat kell rendelni.

A NAIH aggodalmát fejezte ki a biometrikus arcfelismerő rendszerrel kapcsolatban is: „A Hatóság véleménye szerint rendkívül problematikusak a biometrikus arcképadatok kezelésére vonatkozó tervek, ugyanis a biometrikus személyazonosítás és ellenőrzés azon technológiák, közé tartozik, amelyek jellegüknél fogva különösképp veszélyesek az állampolgárok alapvető jogaira. Az automatikus arcfelismerésen alapuló azonosítás és személyazonosság ellenőrzés nem igényli az érintett közreműködését, ezért rejtett megfigyelést tesz lehetővé. Az arcfelismerési és hasonló jellegű biometrikus technológiák kiterjedt, tömeges alkalmazása ahhoz vezethet, hogy a települési közterületek, a nyilvánosság számára nyitva álló egyéb közterületek és a tömegközlekedési eszközök megszűnnek a magánélet színterei lenni. A biometrikus azonosításra épülő szolgáltatások alkalmazásának kiterjesztése ellentétbe kerülhet a magyar alkotmányos jogfejlődés már elért eredményeivel, így különösen azzal, hogy az Alaptörvény a magán- és családi élet, az otthon és kapcsolattartás tiszteletben tartását egyaránt alapvető jogokként ismeri el, továbbá a magánélet védelméről szóló 2018. évi LIII. törvényben a magánélet fokozottabb védelme érdekében deklarált elvekkel és szabályokkal.”

Az említett azonosítási módok – egy központi szolgáltatási platform létrehozása révén – a leendő magyarországi „okos városokat” fogják kiszolgálni: „4. A tervezett szabályok a Kormányzati Adatközpont (KAK) kizárólagos feladatkörébe kívánják utalni az okos városok

számára nyújtandó platform-szolgáltatások egy részének nyújtását és ezzel összefüggésben megtiltják a települési önkormányzatok számára, hogy ezekkel párhuzamos vagy alternatív szolgáltatásokat tartsanak fenn. A platformszolgáltatások kötelező igénybevétele az adatkezelés kormányzati centralizációjával járna, hiszen elvonná a polgárok helyi közösségeitől azt az önkormányzati autonómiából levezethető jogot, hogy eldöntsék, vállalják-e a központi platformszolgáltatásoktól való függőséget, valamint az adataik KAK-ban történő kezelését, vagy inkább maguk kívánnak gondoskodni a település működésével és a helyi ügyekkel összefüggő adataikról. […]

5. Ha az okos városok adatainak kezelése bekerül a KAK-ba, úgy egy országosan uniformizált és centralizált informatikai infrastruktúra fog létrejönni, illetve tovább épülni. Az egységesítésnek és a centralizációnak számos előnye mellett vannak árnyoldalai is, így például az, hogy a központtal való kapcsolat megszűnése esetén, illetve a központ bármilyen módon történő kiiktatásával (pl. üzemzavar, természeti katasztrófa, szabotázs stb.) megbénítható a rendszer működése. A Hatóság ezzel összefüggésben javasolta a monolitikus, centralizált architektúra alternatíváit, így különösen a decentralizált, heterogén és osztott információs rendszermodelleket is számításba venni az okos városok informatikai infrastruktúrájának koncepcionális tervezése során."

Az „okos város" projekt megvalósításáról intenzív egyeztetések kezdődtek meg a NAIH és a minisztériumi szakértők között annak érdekében, hogy e nagy ívű fejlesztés során az adatvédelmi szempontok maximálisan érvényesüljenek.

A beszámoló mindezeken túl tájékoztatást nyújt a titokfelügyelettel kapcsolatos adatvédelmet érintő ügyekről, beszámol a NAIH nemzetközi tevékenységéről és társadalmi kapcsolatairól. A 2018. évi beszámoló kapcsán is megállapítható, hogy a Hatóság éves beszámolói továbbra is fontos dokumentumai a hazai információszabadság és adatvédelem témakörének.