ADATVÉDELEM „ÚJRATÖLTVE”

A GDPR alkalmazása a hazai gyakorlatban

Ilosvai András

1. Bevezető

Talán kevesen gondolták, hogy eljut odáig a technológia fejlődése, hogy egy pénzintézet mesterséges intelligencia alapú rendszere – jogtalanul – elemezni fogja ügyfeleivel történő beszélgetését az alapján, hogy az ügyfél milyen hangulatban kereste meg a bankot. A GDPR ma már megkerülhetetlen bármilyen személyiségi jogi kérdés esetén, tekintettel a személyes adatok védelmére. A rendelet 2018-as kötelező alkalmazása óta egyre kiforrottabbá kezd válni a joggyakorlata, amit jól mutat elsősorban a Nemzeti Adatvédelmi és Információszabadság Hatóság munkássága is. Az átállás – bármennyire is jól működő törvényi szabályozás állt előzményként mögötte – Magyarországon sem volt zökkenőmentes, mára azonban egyre biztosabb a működése. Az egész GDPR áttekintésére jelen tanulmányban nincs lehetőség, azonban szeretnék kiemelni néhány fontos pontot, ami viszont elengedhetetlen a rendelet megértéséhez, továbbá néhány jogeseten, iránymutatáson keresztül röviden bemutatni a nemzetközi gyakorlatot és a NAIH hazai gyakorlatát.

2. Mi is az a GDPR?

Először mindenképp néhány alapfogalmat érdemes ismertetni. Ezek a fogalmak már a GDPR megjelenése előtt is alapvetőek voltak, a rendelet azt kívánta elérni a fogalmak meghatározásával, hogy csiszolja, egységesítse azokat a tagállami jogrendszerek között. A GDPR, azaz az Általános Adatvédelmi Rendelet

(General Data Protection Regulation) legfontosabb fogalma, amelynek elsődlegesen pontos definíciót kell adjunk: a személyes adat fogalma.[1]

Személyes adatnak tekintünk minden olyan adatot, amely kötődik az egyénhez és helyzetét valamilyen módon befolyásolja. Három fogalmi elem különböztethető meg benne: (1) a „bármely információ", mely alatt az adat formai és tartalmi kritériumai értendők, (2) az „érintett", aki az azonosított vagy azonosítható személy, és (3) a „vonatkozó", amely az adat és az érintett közötti kapcsolatot teremti meg.[2] Ezek pontos behatárolása elengedhetetlen a jogszerű adatkezeléshez. A személyes adatnak a fogalma azonban közel sem meríti ki azt, ami mögötte van: folyamatosan bővül, hogy mit értünk személyes adat alatt. Az adatoknak két csoportját különböztetjük meg: egyrészt az érintettre vonatkozó adatokat, másrészt az érintett kontextusából vonatkozó következtetéseket. A személyes adatoknál foglalkozik a GDPR a magánszféra és a nyilvánosság közötti határról, ami eszerint sem mindig egyértelmű, olykor még össze is ér. Erre egy olyan példát hoz a szerző, hogy a vállalkozó címénél, ami a saját lakcíme is, mennyire jogszerű ennek a kezelése. A jogalkotó a tagállami törvényekre bízza, hogy mi számít közérdeknek: mint láttuk, ezt hazánkban a Ptk. szabályozza.[3] A fogalmi elemek között említett „vonatkozó" az, amely a legkevésbé könnyen feloldható. Ez azt takarja, hogy az adat és érintett közötti kapcsolat három pilléren áll: a tartalom – cél – elem hármasságán, amelynek minden adatkezelés során meg kell felelni. Fontos kikötésként jelenik meg a rendeletben, hogy az információ addig őrzi meg jellegét, míg kapcsolata helyreállítható az érintettel. A személyes adat fogalmánál érdemes kitérni az adatkezelő egyik legfontosabb kötelezettségére, az érintett hozzájárulására.[4] Négy konjunktív elem alkotja a hozzájárulást: (1) az önkéntesség, (2) a konkrétság, azaz, hogy célhoz kötött, (3) megfelelően tájékoztatva legyen az érintett, és mindez (4) beleegyező nyilatkozat hozatalával történjen meg. A hozzájárulás elvén tovább haladva át is térhetünk az adatkezelés fogalmára.

---

1 Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer Hungary, 2018. 63–77.

2 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 4. cikk:
1. „személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

3 Ptk. 2:44. §.

4 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 7. cikk.

Adatkezelésnek minősül bármely olyan művelet, amely a személyes adatokon történik, tehát pld. a tárolás, gyűjtés, de a statisztika, a kutatás és a kérdőív készítése is.[5] Az adatkezelés fogalma mögött jogalkotói szándék áll: a jogalkotó szeretné az összes személyes adattal összefüggő tevékenységet a rendelet hatálya alá helyezni. Ennek a típusainak meghatározása nem taxatív, hanem kazuisztikus. Ezt azért is találom fontosnak, mert lehetetlenség lenne minden egyes esetet pontosan a törvény alá vonni, elég egy generálklauzula, amely lefedi a felmerülő esetek egészét általánosan. Az adatkezelés jogszerű eljárása – a „vonatkozó” elvéhez hasonlóan – három pilléren áll: egyrészt az alapelveket, másrészt a jogalapokat, harmadrészt a körülményeket kell szemügyre venni és ha mindennek megfelel az adatkezelés, akkor állíthatjuk róla biztosan, hogy jogszerűen történik. Ebből fakad, hogy ha a három pillér közül bármelyik is kiesik, akkor az adatkezelés nem jogszerű, így korlátozható. Ezen kívül még három esetet említ a rendelet:[6] amikor a személyes adatok pontossága vitatott, amikor a személyes adatok jogi igények előterjesztéséhez volnának szükségesek, illetve amikor a tiltakozási jogának gyakorlása ellenére próbálnak adatkezelést végrehajtani. Amellett, hogy korlátozzák az adatkezelést, még megvalósulhat az adatvédelmi incidens tényállása is. Alapvetően öt típusát különböztetjük meg, köztük a személyes adatok megsemmisítését, elvesztését, megváltoztatását, továbbítását vagy közlését, illetve a jogosulatlan hozzáférését. A GDPR értelmezések is hangsúlyozzák azt, hogy elsősorban az adatbiztonságot kell megteremteni ahhoz, hogy adatvédelmi incidens ne is fordulhasson elő. A tény pedig, hogy az adatvédelmi incidens nem szándékosan, hanem vétlenül történt, nem változtat a megítélésén, és mint enyhítő körülmény sem releváns.

Mindenképp fontos fogalmak az anonimizálás és a pszeudonimizálás. Anonimizálás alatt azt értjük, amikor az érintett személyes adatait oly módon változtatják meg (képletesen), hogy ne lehessen azonosítani.[7] Pszeudonimizálás pedig álnevesítést jelent, nem teljesen anonimizálják a személyt, viszont ezen adatok kezelése is adatkezelésnek minősül.

Az adatkezelés elveken nyugszik, olyan elveken, amelyek korlátozzák az adatkezelő működését és biztosítják az érintettek adatainak védelmét. Ebben a hét főelvben visszaköszönnek a polgári jogi alapelvek, generálklauzulák is, pld. a jogszerűség, tisztességes eljárás és átláthatóság elvénél.[8]

---

5 Péterfalvi–Révész–Buzás i. m. 77–79.

6 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 18. cikk.

7 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete (26) bekezdés.

8 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (1) *a)* pont.

Jogszerűség alatt a jogalkotó a megfelelő jogalapot érti, amelyet a GDPR 6. cikke határoz meg.[9] Ez a felsorolás azonban nem rangsorolás, mindegyik jogalap ugyanolyan súllyal bír, illetve – általánosságba véve – ugyanolyan joghátrányokat von maga után. Tisztességes eljárás alatt a jogszabályok irányába mutatott erkölcsi és morális hozzáállást kell érteni. Átláthatóságra pedig azért van szükség, hogy az adatkezelésnek a folyamata és dokumentációja nyilvános legyen a külvilág felé. Ennek része a tájékoztatás, melyet a GDPR írásban kér az adatkezelőktől. Ezeknek a tájékoztatóknak lényegi elemei, hogy érdemi, egyszerű és világos nyelvezetű, könnyen hozzáférhető és közérthető legyen.

A célhoz kötöttség elve[10] az adatvédelem legfontosabb elve. A korábbi magyar adatvédelmi törvényekben sem volt idegen ez a fogalom, ez nagyrészt az Alkotmánybíróság munkájának köszönhető, hogy alaposan kimunkálta ezt az elvet a hazai jogrendben.[11] A célnak egyértelműnek, nyilvánvalónak és érthetőnek kell lennie. Fogalmi elemei, hogy az adatkezelés céljának egyértelműnek és jogszerűnek kell lennie, valamint a személyes adatok kezelésének összeegyeztethetőnek kell lennie a céllal és ezen kikötés mentén is kell ezt alkalmazni. A kettős fogalmi elem mellett négy elvárást is állít az alkalmazó elé, amelyek nagyban-egészében összefüggenek az eddigi elvekkel: konkrét cél meghatározása, még az adatkezelés előtt, legitim cél, érthető kommunikáció és összeegyeztethetőség. A célhoz kötöttség elve alá tartozik a nyilvánosságra hozható adatok köre. A jogalkotó három „forrást" ad meg, amely esetekben az adatkezelés eredménye nyilvánosságra hozható: ha egy nyilvános adatbázis kötelező adatkezeléséről van szó, ha a jogalkotó konkrét szándékával történik az adatkezelés, illetve, ha polgárok önkéntesen járultak hozzá ehhez.

A következő elv az adattakarékosság elve.[12] Adattakarékosság alatt a szükségességet és az adatminimalizálást kell érteni, tehát azt a megvalósítandó célt, hogy az adatkezelő minél kevesebb adatot minél kevesebb ideig tároljon és kezeljen. Először is azt kell megvizsgálnia az adatkezelőnek, hogy egyáltalán szükség van-e az adat kezelésére. Csak olyan személyes adat kezelhető, ami szükséges és arányos az adatkezelés céljának eléréséhez.[13] Ha ez a cél megvalósult, utána az adatkezelő köteles az adatokat vagy törölni, vagy anonimizálni. Ahhoz, hogy ez fenntartható és megismerhető legyen az érintett számára, az

9 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 6. cikk (1) bek.

10 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (1) *b).*

11 Péterfalvi–Révész–Buzás i. m. 96–101.

12 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (1) *c).*

13 Péterfalvi–Révész–Buzás i. m. 101–102.

egyes adatvédelmi tájékoztatókban pontos, taxatív meghatározások szükségesek arról, hogy milyen célra lesz felhasználva az adat.

A pontosság elve[14] kétoldalú felelősség. Az adatok frissítése az adatkezelő feladata, viszont adatalany nélkül nehéz ezt végrehajtani. A nagy állami nyilvántartások esetén az állam az, aki ezt végzi. A hazai jogrendben a pontosság a személyes adatok teljességében jelenik meg: ennek célja, hogy a tárolt és forgó adatok ne legyenek töredékesek.[15]

A korlátozott tárolhatóság elve[16] annyiban egészíti ki az adattakarékosság elvét, hogy a cél megvalósulásához szükséges ideig lehessen tárolni az érintett adatait, valamint, hogy az érintett azonosíthatóságának megszüntetését kell főszabályként alkalmazni, ha viszont ez nem lehetséges, akkor az anonimizálás lép be.[17]

Az integritás és a bizalmas jelleg elve[18] korábban nem szerepelt elvként és önmagába véve a hozzájáruláshoz kapcsolódóan köti azt meg, hogy az eltérő célú adatbázisokat külön kell kezelni. Erre példa a felhőszolgáltatások *(cloud computing)* esete.[19]

Az elvek között végül, de nem utolsósorban az elszámoltathatóság elve szerepel.[20] Ez nem is az elveket taglaló bekezdésben kerül tárgyalásra és egy nem is hosszú meghatározást ad neki a jogalkotó. Mégis az elszámoltathatóság fogja össze az alapelveket, rendezi egy rendszerbe és biztosítja az adatvédelmi megfelelőséget, amolyan „szuperelvként”.[21] Feladatkörébe sok minden besorolható: adminisztráció, központi irányítás, monitoring, PR, hatékony végrehajtás, szabályzatok felülvizsgálata, panaszkezelés és még lehetne folytatni. Míg a célhoz kötöttség elvénél hangsúlyoztam azt, hogy a legfontosabb elv elméleti szempontból, ugyanez elmondható az elszámoltathatóság elvéről is, gyakorlati szempontból.

Az adatkezelés központi kérdése – az alapelveket követően – a jogalapok vizsgálata.[22] A GDPR 6. cikkében felsorolt jogalapok között nincsen hierarchia. A leggyakrabban használt jogalap a hozzájárulás, ugyanakkor látni kell azt,

---

14 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (1) *d).*

15 Péterfalvi–Révész–Buzás i. m. 102–105.

16 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (1) *e).*

17 Péterfalvi–Révész–Buzás i. m. 105–106.

18 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (1) *f).*

19 Péterfalvi–Révész–Buzás i. m. 106–108.

20 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 5. cikk (2).

21 Péterfalvi–Révész–Buzás i. m. 106–108.

22 Péterfalvi–Révész–Buzás i. m. 111–113.

hogy sok esetben a hozzájárulás vagy nem megfelelő, vagy szükségtelen. A hozzájárulás abban az esetben biztosítja legjobban az érintettet, ha ténylegesen ő dönthet az adatkezelésről. A hozzájárulás szükségtelensége pedig olyan esetekben látható, amikor az adatkezelő tudatában van annak, hogy az érintett adatainak kezelésére a beleegyezéstől függetlenül is szüksége van, viszont, ha ennek ellenére is hozzájárulást kér az adatkezelő, azzal megtéveszti az érintettet. Vannak olyan helyzetek is, ahol nem a hozzájárulás a megfelelő jogalap, pld. egy szerződéskötés esetén. Egy adatkezelésnek egy jogalapja lehet. Több adatkezelésnél mindegyikhez külön hozzájárulás szükséges, nem lehet egy hozzájárulás keretében többet is igényelni, érdekmérlegelésnél ez főleg előjön. Az adatkezelőnek nem a konkrét személyes adat kezelésére kell jogalapot találnia, hanem a tevékenységre kell megtalálnia a megfelelő jogalapot. Több adatkezelés esetén, ha az érintett visszavonja az egyiket (pld. hírlevélről történő leiratkozás), attól még a többi jogalapi kezelés nem szűnik meg. Az adatkezelőnek fontos feladata, hogy a konkrét tevékenységhez a lehető legjobb megoldást válassza, viszont kivételesen van arra lehetőség, hogy egyik jogalapról a másikra váltsanak, de ezt kellőképpen meg kell tudni indokolni. A jogszerűségi alapelvnek itt is érvényesülnie kell: attól, hogy az adatkezelés rendelkezik jogalappal, még nem vonja maga után azt a tényt, hogy az adatkezelés jogszerű is.

A GDRP 2016-os elfogadása után a tagállamok két évet kaptak arra, hogy a saját jogrendszerükbe tudják illeszteni a rendeletben foglaltakat. Azt az Európai Parlament is látta, hogy egy ilyen nagy volumenű átalakításhoz bő időkeretet kell megadni, hogy minden tagállam a lehető legpontosabban tudja beleilleszteni a jogrendjébe, ugyanakkor azt is szem előtt kell tartani, hogy a rendelkezések átültetése és egységesítése nem tud maradéktalanul megvalósulni. Az Európai Parlament jogalkotói azért választották a GDPR-nak a rendelet formát, mert a tagállamok között eddig is abban volt a jelentős különbség, hogy milyen a jogforrás jellege.[23] Ezelőtt irányelv, a 95/46/EK irányelv szabályozta. A rendelet megad egy szabályozási rendszert, amitől negatív irányba eltérni, tehát enyhíteni azokat nem lehet, szigorúbb szabályozásokat viszont be lehet vezetni. Ezt hívjuk minimumharmonizációs szabályozásnak. Nemzetközi jogi szempontból a GDPR nemzetközi szerződésnek minősül, így tud érvényesülni az Alaptörvény E) cikk szerinti szuverenitás-transzfer is.[24] A tagállami jogalkotásnál figyelembe kell azt is venni, hogy az Európai Unió Bíróságának joggyakorlatával összeegyeztethetőnek kell lennie. Már a normaszöveg alkotá-

[23] Uo.

[24] Alaptörvény E) cikk (2).

sakor tudták a jogalkotók, hogy a köz- és magánszféra szabályozása együttes, mindenre kiterjedő szabályozása nem lehetséges, erre egyetlen megoldás lehetne lehetséges: a két területet két külön irányelvben vagy rendeletben lehetne szabályozni, ami viszont sok éves munkafolyamat lenne, és közel sem biztos, hogy célravezetőbb lenne, mint a jelenlegi szabályozás. A bűnügyi irányelv terén nagyobb függetlenséget kapnak a tagállamok, hogy hogy harmonizálják a jogrendjükbe. Ez nagyban függ az adott tagállam büntetőjogi szabályozásától is, illetve – véleményem szerint –, hogy mennyire szigorítják az alaprendelkezéseket. Amit viszont a legfontosabbnak tartok a tagállami és az uniós szabályozás összekapcsolódása között, hogy a magyar jogalkotásnak az Alaptörvény és a GDPR részéről is biztosítani kell a személyes adatok védelméhez fűződő jogokat. Ezzel az Alaptörvény mellett további biztos ponton nyugszik a személyes adatok védelme.

A GDPR rendelkezéseit megsértő esetek száma folyamatosan nő, minden tagállamból lehet hallani adatvédelmi incidensekről. Számos világcég ellen is indult eljárás, mint pld. a Google vagy a Morgen Stanley ellen. Eljárások szempontjából élen jár ebben Spanyolország, Svédország és Lengyelország is. Az adatvédelmi incidensekről érdemes megemlíteni, hogy a mai fejlett technológiai közegben – egy kevésbé gyakorlott személy számára – nagyon könnyen elkövethetővé váltak, így ennek is köszönhető a megsokszorozódott szám; ha csak a magyar gyakorlatot nézzük: a NAIH 2018-ban 67 hatósági eljárást indított, 2021-ben ennek több, mint nyolcszorosát, 556-ot.[25] Két rövid nemzetközi esetet szeretnék bemutatni, hogy milyen jogsértések fordultak elő egy-egy tagállam esetében.

2019. október 9-én, a hollandiai Almerében, egy kórház parkolójában egy pendrive-ra lett figyelmes egy illető. Felvette, otthon megnyitotta és korábbi kórházi betegek adatait találta meg rajta. Mindezen adatokat a *Flevoziekenhuis* egészségügyi szolgáltató egyik munkatársa hagyta el és ők voltak az adatkezelők is. Az illető visszajuttatta az USB sticket a kórháznak, akik tájékoztatták az érintetteket az incidensről.[26] Összesen 4325, 2014 és 2017 között kezelt beteg adatait tartalmazta a pendrive, a következő információkkal: név, születési hely és idő, betegszám, és rövid orvosi megjegyzések, ezen felül semmilyen más érzékeny adatot nem tartalmazott az adathordozó. Az adatok tárolása hatékonyság-elemzés céljából volt a pendrive-on. A holland adatvédelmi hatóság

[25] A Nemzeti Adatvédelmi és Információszabadság Hatóság 2021. évi beszámolója. NAIH, Budapest, 2022. 20.

[26] Flevoziekenhuis informeert patiënten over datalek. 2020. március 3. shorturl.at/tHUX0

vizsgálatot indított egy külső ügynökség bevonásával, és szigorították a teljes protokollt, továbbiakban nem lehet használni külső adathordozót adatok tárolására. A kórház bocsánatot kért az érintettektől.[27]

A másik eset Lengyelországban történt, 2019 novemberében. A Varsói Élettudományi Egyetem (SGGW) egyik alkalmazottjának ellopták személyes laptopját, amin nemcsak személyes adatok, hanem üzleti célú személyes adatok, közel 100.000 felvételiző személyes adatai is rajta voltak. A lengyel adatvédelmi hatóság, az UODO az incidenst követően egyből eljárást indított, a végső döntés pedig 2020. augusztus 21-én született meg.[28] A hatóság szerint az egyetem több szempontból is megsértette a GDPR egyes rendelkezéseit. Egyrészt az adatok kezelése miatt, hiszen közel öt éven keresztül folyt jogszerűtlenül a felvételi eljárás során a felvételizők adatainak kezelése. A százezres érintettségi szám is csak hozzávetőleges, pontosan nem lehetett megmondani, hogy hány érintett fél adatainak kezelése sérült, mivel az öt év alatt nagyon sok felvételiző megfordulhatott az SGGW-n.[29] Másrészt pedig megsértették az adattakarékosság elvét, mivel 5 éven keresztül tárolták a 3 hónapon át tárolható személyes adatokat. A helyzet súlyosságát mutatja, hogy az UODO először csak figyelmeztetni szokta az oktatási intézményeket, itt viszont egyből közigazgatási bírságot szabott ki. Az egyetem nem rendelkezett megfelelő technikai háttérrel, az egyetem adatvédelmi felelőse pedig nem volt bevonva a felvételi eljárás ellenőrzésébe.[30]

A fejezet végén vessünk egy pillantást a modern kori technológia és az adatvédelem problematikájára. Mára már megkerülhetetlenné vált a modern technológia használata a mindennapokban – a teljesség igénye nélkül – kezdve az internethasználattól egészen az okosotthon rendszerekig. Ezek jelentős részével – akarva, akaratlanul – a GDPR kapcsolatba kerül. Elsődleges kérdésként a mesterséges intelligencia alapú rendszerek használata és szabályozása vet fel komoly kérdéseket a jogalkotó számára, akár csak a jogalanyisága kapcsán és adatvédelme, adatkezelése kapcsán, hogy mennyire tud egy automatizált rendszer azoknak a kritériumoknak megfelelni, amit a GDPR kiköt. Az MI önmagában egy bonyolult és külön dolgozatként is helytálló téma, így erre rész-

---

27 Adatvédelmi incidens egy holland kórházban. 2020. április 24. https://gdpr.news.hu/cikkek/adatvedelmi-incidens-egy-holland-korhazban/

28 Urzedu Ochrony Danych Osobowych (UODO) ZSOŚS.421.25.2019 (Warszawa, dnia 21 sierpnia 2020 r.) [A lengyel adatvédelmi hatóság 2020. augusztus 21-én hozott ítélete a fent hivatkozott ügyszámon.]

29 Az adatok arányosítása végett: ma az egyetem 14 karán 27.000 hallgató folytatja tanulmányait.

30 Vizsgálat a McDonald's-nál és egy bírság. *GDPR apró,* 2020. október 2. https://gdpr.news.hu/cikkek/gdpr-apro-vizsgalat-a-mcdonalds-nal-es-egy-birsag/

letesebben nem térnék ki. Egyre inkább elterjedtté vált az arcfelismerő rendszerek, arcfelismerő kamerák alkalmazhatóságával kérdése, hiszen – véleményem szerint – az adatvédelmi alapelvként meghatározott célhoz kötöttség elve sok esetben sérülhet. A nagy adathalmazok, algoritmusok, felhőszolgáltatások stb. mint önálló rendszerek működése is vizsgálatra szorul adatvédelmi szempontokból. A joggyakorlatban felmerülhet – egyelőre csak utópisztikus – kérdés, hogy mikor lesz az a pont, amikor olyan szakmák gyakorlását veszi át az MI, amelyekhez szükség van a személy emberi voltára, pld. bírókat, ügyvédeket, ügyészeket mikor fogja felváltani a mesterséges intelligencia. A bevezetőben említett magyar pénzintézet esete némi aggályra adhat okot, azonban – meglátásom szerint – amíg a helyén tudjuk kezelni a mesterséges intelligencia működését és személyes közreműködéssel felül tudjuk bírálni egyes döntéseit, addig nem kell tartanunk az MI rendszerek működésétől. Ennél persze jóval árnyaltabb a helyzet, hogy mi az, ami aggodalomra adhat okot a személyes adatok szempontjából a mesterséges intelligencia területén és mi az, ami nem indokolja az MI-ben való kételkedést, de erre itt most nem kívánok kitérni.

3. Hogyan védik a személyes adatainkat itthon? – A NAIH joggyakorlata

2011-ben, az Infotv.[31] hatálybalépésével új autonóm szerv jött létre az információszabadság és az adatvédelem biztosításának és eljárásainak lebonyolítására: a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH).[32] Korábban, 1995-től ezeket a feladatokat az adatvédelmi biztos látta el, viszont ez a pozíció a törvény hatálybalépésével megszűnt. A NAIH elmúlt közel egy évtizede alatt és különösen a GDPR hatályba lépése óta számos újítást hozott és számos ügyet oldott meg az adatvédelem terén, ugyanakkor még maradtak olyan nyitott kérdések, amelyekre csak részleges válasz érkezett vagy – egyelőre – egyáltalán nem sikerült megoldást találni. Meg kell azonban azt is említeni, hogy az adatvédelmi perek az Infotv. hatálybalépése után a polgári bíróságok hatásköréből a közigazgatási bíróságok hatáskörébe helyeződött át.[33]

---

31 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.).

32 A NAIH alapító okirata a Hivatalos Értesítő 2012/1. számában jelent meg.

33 Dudás Gábor: A magyar rendes bíróságok adatvédelmet érintő döntései. In: Szabó Endre Győző (szerk.): *Az Infotörvénytől a GDPR-ig.* Budapest, Ludovika Egyetemi Kiadó, 2021.

A NAIH bevett gyakorlata, hogy számos témában állásfoglalásokat ad ki. Ezekről általánosságban elmondható, hogy egy-egy ügyet vagy kérdést illetően adja ki a Hatóság, különböző csoportosításokban, gondolok itt arra, hogy külön beszélünk jogi szabályozással kapcsolatos állásfoglalásokról, információszabadsággal kapcsolatos és adatvédelmi állásfoglalásokról. A jogi szabályozással kapcsolatos állásfoglalásoknál egy-egy jogszabály módosításakor vagy elfogadásakor kérik a Hatóság állásfoglalását. Az információszabadsággal és adatvédelemmel kapcsolatos állásfoglalások között annyi a különbség, hogy míg az információszabadsággal kapcsolatos állásfoglalásokat egy-egy közösséghez, állami, önkormányzati szervhez intézik, addig az adatvédelmi állásfoglalások egy-egy eset kapcsán általános jelleggel közölnek megállapításokat, főleg és elsősorban adatvédelmi témakörökben. Az állásfoglalások fontosságát egy hétköznapinak mondható tény kapcsán látom fontosnak: hogy az adatkezelők, valamint mindazok, akik bármilyen kapcsolatban állnak az adatvédelemmel, számukra példaként, egyfajta iránymutatásként funkcionáljon egy-egy kérdés kapcsán. Ezek széles spektrumon mozognak a témájukat illetően: a szcientológiától[34] elkezdve a *Google Street View* kérdésén át[35] az éttermi asztalfoglalásig[36] sok témát érintenek. Ebből hozok most néhány tanulságos esetet.

Az első állásfoglalásban a kérelmező egy sokakat érintő és sokak érdeklődését felkeltő kérdéssel fordult a Hatósághoz: a Facebook-kérdéssel, hogy ti. egy, a Facebook-on működő, személyes adatokat kezelő oldal vizsgálata a Hatóság hatáskörébe tartozik-e.[37] Ilyen esetben a Hatóság először megvizsgálja a panaszt, majd az ügy súlyosságától függően meghozza a döntését a bejelentés érdemi vizsgálatáról. Azonban ebben az esetben, bár érint magyar felhasználókat is a Facebook kérdése, mivel a cég magyarországi tevékenységi hellyel nem rendelkezik, így az Infotv. meghatározott szakaszai nem alkalmazhatók a Facebook ellen. Korábban pont egy magyar vonatkozású ügy, a Weltimmo-ügy[38] esetén mondta ki azt 2015-ben az Európai Unió Bírósága, még a GDPR elfogadása előtt, hogy az adatvédelmi felügyeleti hatóság a 95/46/EK irányelvben meghatározott feladatkörei és együttműködése ellenére, de leginkább javára, ki kell ezt a kört bővíteni olyan cégekre is, amelyek ugyan külföldiek, tehát más tagállam területén van a székhelyük, de tevékenységi helyük az adott tagállamon is meg-

34 NAIH/2015/3940/2/V.

35 NAIH-5711-16/2012/B.

36 NAIH/2016/2916/2/V.

37 NAIH/2018/2198/2/V.

38 C-230/14. sz. ügy Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [ECLI:EU:C:2015:639].

található, *ergo* rájuk is vonatkoznak az Infotv. szabályai. Jelen esetben a NAIH, mint érintett felügyeleti hatóság vesz részt az eljárásban, viszont a Facebook ír székhelye folytán az ír adatvédelmi hatóság fogja vizsgálni az ügyet. A Hatóság rendkívül pontos: arra is külön kitér, hogy a Facebook internetes oldalán belül hol tudja a kérelmező jelenteni az oldalt.

A második és a harmadik állásfoglalás a jelenleg is tomboló koronavírus-járvány során felmerült kérdésekkel foglalkozik: a lázméréssel és a digitális tanórákkal. A lázmérés kérdése először április végén merült fel, amikor kérdésként tették fel a NAIH részére, hogy mi az álláspont a kötelező munkahelyi testhőmérséklet-méréssel kapcsolatban.[39] Ekkor a Hatóság úgy vélekedett, hogy az adott helyzetben nem tartja arányosnak a minden munkavállalóra általánosan kiterjedő szűrővizsgálatok előírását, valamint amennyiben egészségügyi kockázat miatt mégis szükség volna erre, akkor is csak szakember bevonásával történhet meg a testhőmérséklet-mérés. Az adattakarékosság elvét itt is tartani kell, tehát nem lehet hosszú időkig tárolni a testhőmérséklet adatokat, egyrészt, mert szenzitív adatnak minősülnek, másrészt, mert nem megfelelő és nem releváns az adatkezelési cél. Mára ez a helyzet változott, ugyanis a Kormány 2020. szeptember 12-én bejelentette, hogy október elsejétől kötelező a lázmérés az iskolákban a diákoknak és tanároknak egyaránt. dr. Péterfalvi Attila, a NAIH elnöke ennek kapcsán azt nyilatkozta egy internetes hírportálnak,[40] hogy itt elsősorban az arányosság elvét figyelembe véve kell eljárni, és mivel a járvány második hulláma – az elsővel szemben – már indokolttá teszi a lázmérést, így az nem ütközik semmilyen jogi normába. Viszont azt továbbra is kihangsúlyozza a Hatóság, hogy a testhőmérséklet adatok szenzitív személyes adatnak minősülnek, így rögzíteni nem lehet őket.

A harmadik állásfoglalás kérdése érdekes problémát vet fel a Hatóság számára. A kérdés arról szól, hogy mennyire felel meg az adatvédelmi előírásoknak a Hatóság szerint az a tény, hogy 14 és 16 éves kor közötti gyerekektől a tanár videófelvételt kér a feladat ellenőrzésének céljából, mindenféle hozzájárulás nélkül.[41] Ennek kapcsán 5+1 főbb pontban szedi össze a kérdésre válaszként formált véleményét. Az első pontban a Hatóság kihangsúlyozza, hogy az ember arca, képmása személyes adatnak,[42] illetve bármely művelet ezeken, adatkeze-

[39] NAIH/2020/3649/.

[40] Szalai Szabolcs: Péterfalvi Attila: Lázat mérni szabad, rögzíteni nem. *Index,* 2020. 09. 28. https://index.hu/belfold/2020/09/28/peterfalvi-attila-naih-lazmeres-iskola-koronavirus/

[41] NAIH/2020/2888/.

[42] Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 4. cikk (1).

lésnek[43] minősül, amennyiben az érintettek felismerhetőek a felvételeken. A 2011. évi Nkt.[44] értelmében azonban nem maga a tanár lesz az adatkezelő, hanem a köznevelési intézmény, így a tanár csak közvetetten válik azzá. A Hatóság kiemeli, hogy itt nem magáncélú adatkezelésről van szó, mivel az adatkezelési cél meghatározása (iskolai nevelés és oktatás) alapján nem fér bele a magáncél körébe. A második pontban a Hatóság felveti annak a kérdését, hogy nem volt-e más módja annak, hogy a cél teljesítését igazolni tudják, pld. a szülő írásbeli igazolásával, vagy online video chat formájában megrendezett óra keretében. A harmadik pont mondja ki lényegében a kérdésre a választ, hogy amennyiben a köznevelésen belüli etikai és egyéb szabályokat betartják a pedagógusok a digitális távoktatás során, akkor kérhetik a diákokat viedófelvétel küldésére. Mindehhez kell egy megfelelő jogalap, amely meghatározza a pontos célt és a jogszerűséget alátámasztó jogalapot; ezekre a GDPR rendelet nyújt biztosítékot. A negyedik pontban a kérdésben felmerült Ptk. hivatkozásra reflektál a Hatóság. Jogos a kérdésfeltevés, hogy a Ptk. 2:48. §-a alapján, hogy viszonyulnak ezek a videófelvételek a képmás- és hangfelvétel jogához, itt viszont, mivel ez közfeladat ellátására szolgál,[45] így nem válik relevánssá ez a kérdés. Az ötödik, utolsó pontban sorra veszik azokat az elveket, amelyeket a rendelet határoz meg és amelyek ebben a kérdésben érdekeltek, így az elszámoltathatóság, az adattakarékosság, a korlátozott tárolhatóság, a bizalmasság és integritás, és az adatbiztonság elvét, egy-egy rövid magyarázattal kiegészítve, hogy ebben az esetben hogyan valósul ez meg. Majd sorra veszi a kötelezettségeket is, miszerint tájékoztatást kell adni az érintetteknek és adatkezelési tájékoztatót kell kidolgoznia. Végezetül szankciókról is szól: meghatározza a Btk. tényállását[46] és a közigazgatási bírságot helyezi még kilátásba. Álláspontom nagyban egyezik a Hatóság által kiadott állásfoglalással, egy kérdés azonban nyitva maradt számomra. Hogyan követhető le, hogy az adatkezelő betartja-e az adattakarékosság elvét? A helyzetet árnyalja az a tény, hogy az adatkezelő a köznevelési intézmény és csak közvetetten a pedagógus, akinek nem ellenőrzik a laptopját az iskolában. De például a tanár hogyan tudja bizonyítani, hogy ő betartotta az elvet? Ráadásul, a mai technikai megoldások esetén sok rendszer már automatikusan tárolja is ezeket az adatokat. Ebben a Hatóság sem tud részletszabályokat adni, mivel sokkal inkább a folyamatos fejlődés „eredménye”

43 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 4. cikk (2).

44 2011. évi CXC. törvény a nemzeti köznevelésről 43. § (1) bekezdés.

45 Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete 6. cikk (1).

46 2012. évi C. tv. 219. § (4) bekezdés.

az, ami itt tetten érhető. Elengedhetetlen azonban azt is hangsúlyozni, hogy a Polgári Törvénykönyv generálklauzulájában feltüntetett alapelveket, a jóhiszeműség és tisztesség, valamint az elvárható magatartás elvét[47] itt is fenn kell tartani abban a tekintetben, hogy az adatkezelő szabályszerűen járt el.

Vannak azonban olyan helyzetek az adatvédelemben, amikor 'a szükség törvényt bont'. Ilyen helyzet adódott a koronavírus megjelenésével és az ebből adódó veszélyhelyzet bevezetésével Magyarországon. Adatvédelem kérdésében itt elsősorban azt kell kiemelni, hogy az információs önrendelkezési jog olyan alapjog, amelynek lényeges tartalma veszélyhelyzetben sem korlátozható, ugyanez igaz a szükségesség – arányosság tesztjére is.[48] Ezzel együtt viszont meg kell jegyezni, hogy az állam életvédelmi kötelezettsége indokolhatja a korlátozást. Sokat vitatott rendelet a 179/2020. (V. 5.) Korm. rendelet,[49] amely korlátozta az érintettek személyes adataikkal összefüggő jogainak gyakorlását, melyet a veszélyhelyzet megszűnésével hatályon kívül helyeztek.[50] Érdekes kérdést vet fel a kontaktkövető appok használata, ugyanis maga a használat önkéntes alapon működik, de ez nem jelenti egyből azt, hogy a személyes adatok kezelése szükségszerű hozzájáruláson alapszik. Így tehát ebben az esetben is feltétlen szükséges a hozzájárulás megadása.[51]

Az állásfoglalások mellett fontos azonban megvizsgálni azt is, hogy melyek azok a tények, amelyek generálják az állásfoglalásokat. Hogy egészen pontos legyek: mire tudja építeni az állásfoglalásokat, mi a konkrét joggyakorlat a NAIH intézményében? A Hatóság a számos állásfoglalás mellett számos jogeset megoldásával is foglalkozik. A fejezet záró szakaszában egy olyan jogesettel szeretnék foglalkozni, amely bemutatja azt, hogy egy alapvetően polgári jogi vonatkozású kérdés hogyan is válik adatvédelmi eljárás tárgyává, illetve rámutat arra is, hogy egy nem teljesen hétköznapi kérdésben hogyan és mi alapján kell a hatóságnak döntenie.

---

47 Ptk. 1:3–4. §§.

48 Klein Tamás – Liber Ádám: Adatvédelem koronavírus idején: az Általános Adatvédelmi Rendelet, különösen az alapelvek érvényesülési peremfeltételei a járványügyi veszélyhelyzetben. In: Miskolczi-Bodnár Péter (szerk.): *Acta Caroliensia Conventorum Scientiarum Iuridico-Politicarum XXXIV. – Oktatók és hallgatók közös tanulmánykötete.* Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2021. 188., 208.

49 179/2020. (V. 4.) Korm. rendelet a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről.

50 Klein–Liber i. m. 190.

51 Klein–Liber i. m. 201.

Az eset 2021 januárjában történt és került a Hatóság látóterébe.[52] Az ügy érintettje (tehát akinek a jogai sérültek) elsősorban egy kiskorú, akinek édesanyja (a Kérelmező), egy harmadik személy (továbbiakban: Kérelmezett) és az óvodavezető beszélgetést folytattak az érintett gyermek viselkedési szokásairól. A Kérelmezett a beszélgetés első 46 percéről felvételt készített, amelyet aztán közzétett egy óvodai szülőkből álló Facebook csoportban, vagyis a nyilvánosság számára közvetlenül hozzáférhetővé tette úgy, hogy az érintettektől hozzájárulást nem kért, továbbá nem tájékoztatta a nyilvánosságra hozatalról a Kérelmezőt. A Kérelmező ezek után kereste meg a Hatóságot. A Kérelmezett előadta, hogy őt nem vezérelte rossz szándék, egyrészt azért vette fel a beszélgetést, mert egy ilyen beszélgetésen szakmai indokok is elhangzanak, amiket nehezen lehet később visszaidézni, másrészt szerette volna ezzel tájékoztatni a többi szülőt, hogy gyermekeik veszélyben vannak és ez ellen senki nem tesz semmit. Elmondása szerint akkor döbbent rá, hogy ezt ilyen formában nem lett volna szabad, amikor az óvodavezető a közzététel napján (5 órával később a közzétételtől) megkereste és kérte a felvétel eltávolítását. A felvett beszélgetés során számos olyan információ elhangzott, ami személyes adatnak, illetve egészségügyi adatnak minősül, így a gyermek neve, lakhelye, betegsége tényére utaló kijelentések, az a tény, hogy magatartásbeli, viselkedésbeli problémákkal küzd, továbbá hogy a közelmúltban három haláleset is érte a családot. Ezután a Hatóság sorra veszi azokat a jogszabályokat, amelyeket az adott ügyben alkalmaztak. A NAIH döntésében két adatkezelést különbözetett meg. Egyrészt adatkezelésnek minősült a felvétel rögzítése, másrészt a felvétel közlése két úton is: a Facebook csoportba, másrészt emailben is elküldte három személy számára. Mindkét eset a GDPR alapján adatkezelésnek minősül. A Hatóság ebben a körben vezette be a „háztartási adatkezelés" fogalmát, ami azt jelenti, hogy mindaddig, míg olyan magánjellegű célokat szolgál az adatkezelés, mint amilyet a Kérelmezett is megjelölt, miszerint szerette volna a beszélgetésen elhangzott szakmai szempontokat otthon is felidézni a felvétel segítségével, mindaddig háztartási adatkezelésnek minősül, azaz nem tartozik az adatkezelés rendeletbeli fogalma alá. Az esetben azonban a Kérelmezett túllépte a háztartási adatkezelés körét, hiszen a felvételeket, amelyen személyes és különlegesen személyes adatok is elhangoztak, nyilvánossá tette többféle úton is, melyről nem tájékoztatta a Képviselőt, mint a gyermek szülőjét. Ezzel megsértette a célhoz kötöttség elvét – melyről már korábban kifejtettem, hogy az egyik legfontosabb adatvédelmi alapelv –, továbbá megsértette az adattaka-

[52] NAIH-1743/2021.

rékosság elvét is. Az adatkezelés jogalapja sem volt tisztázott, ezt a Kérelmezett el is ismerte, hogy már tisztában van azzal, hogy nem volt joga továbbítani a felvételt azoknak a szülőknek, akik kérték. Súlyosítja a helyzetet, hogy különleges személyes adatok is megjelentek az ügyben. A Hatóság arra is kitért határozatában, hogy az adatkezelés tisztességes volta felülkerekedik az adott helyzeten, emiatt nem kerülhet kiszolgáltatott helyzetbe sem a gyermek, sem a családja. Ráadásul mindezt titokban tette és igyekezett az édesanyával kimondatni azt, hogy a gyermeke igenis beteg. Mindezek olyan érzékeny kérdések, amelyeknél elsődlegesen arra kell törekedni, hogy minél kevesebb sérelmet okozzanak a felek egymásnak. Mindennek ellenére a Hatóság nem szabott ki adatvédelmi bírságot, csak figyelmeztetésben részesítette a Kérelmezettet.

Azért is tartottam fontosnak ismertetni ezt az esetet, mert – álláspontom szerint – ezen keresztül tökéletesen látszik az, hogy egy adatvédelmi ügy hatósági megoldása mennyire komplex feladat. Pontról pontra, lépésről lépésre kell szemlélni az egyes történéseket, mérlegelni az érdekeket, értékelni a tényeket és erre egy mindenre kiterjedő választ találni. A téma érzékenysége (kiskorú, betegség) is kellőképpen figyelemfelhívó jellegű is lehet, jelentős szerepet játszik véleményem szerint a kérdés társadalmi elfogadottsága is az ügyben. A NAIH határozatával egyet tudok érteni. Érdekesnek tartom, hogy a NAIH egyáltalán nem hivatkozik a Ptk. nevesített személyiségi jogai közül a személyes adatok védelmének jogára, feltehetőleg azért, mivel ezt kellőképpen hangsúlyozza a GDPR és az Infotv. is. Ebben az esetben nem kifejezetten látszott az, hogy egy ellentmondásos kérdést kellett feloldani a Hatóságnak, azonban számtalan olyan helyzet van – és lesz is – az adatvédelem, az információszabadság és a személyiségi jogok területén belül, amelyek feloldásra szorulnak és amelyekre a joggyakorlat folyamatosan dolgozza ki a megoldásokat. A Kúria egy határozatában[53] tett lépéseket afelé, hogy egységesítse az adatvédelmi perek gyakorlatát, ugyanakkor meg kell jegyezni, hogy a határozatot 2015-ben hozták, még a GDPR előtt, azóta nem ismert a bíróságok gyakorlatából ilyen egységesítő törekvés.[54]

[53] Kúria Kfv. II. 37.886/2015/7.

[54] Dudás i. m. 59.

4. Konklúzió

Yuval Noah Harari izraeli történész egyik művében úgy fogalmazott:

> „A XXI. századi élet legfontosabb ténye az, hogy az emberek hackelhető állatok lettek. Ha elég adatod van és elég a számítási kapacitásod, akkor meghackelheted az embereket és jobban megértheted őket, mint ők értik saját magukat. Megjósolhatod a döntéseiket, manipulálhatod a vágyaikat és bármit eladhatsz nekik, amit csak akarsz, legyen az politikus vagy árucikk. Ez azt jelenti, hogy az adat válik a legfontosabb erőforrássá a világon."

Harari ezzel a gondolatsorával abszolút felhívja a figyelmet az adatvédelem lényegére. Személyiségünk alapegysége az adat, amely minket tanúsít, rólunk szól, mi vagyunk az alanyai. Mivel mára pont ez az adat vált Harari szerint a legfontosabb erőforrássá, így különleges védelemben kell részesítse mind az állam, mind az egyén részéről a személyes adatokat. A GDPR erre – közel tökéletes – jogi környezetet biztosít, és amennyiben egy tagállami védelmi mechanizmus jól tud működni, keretek között lehet tartani az incidensek és az eljárások számát. Láttuk, hogy a leghétköznapibb eset is adatvédelmi szempontból problémás lehet, így fokozott felelősség van az egyénen, egyrészt amiatt, hogy maga ne kövesse el a jogsértést, másrészt amiatt, hogy ő se váljon sértettként alanyává egy ilyen helyzetnek.