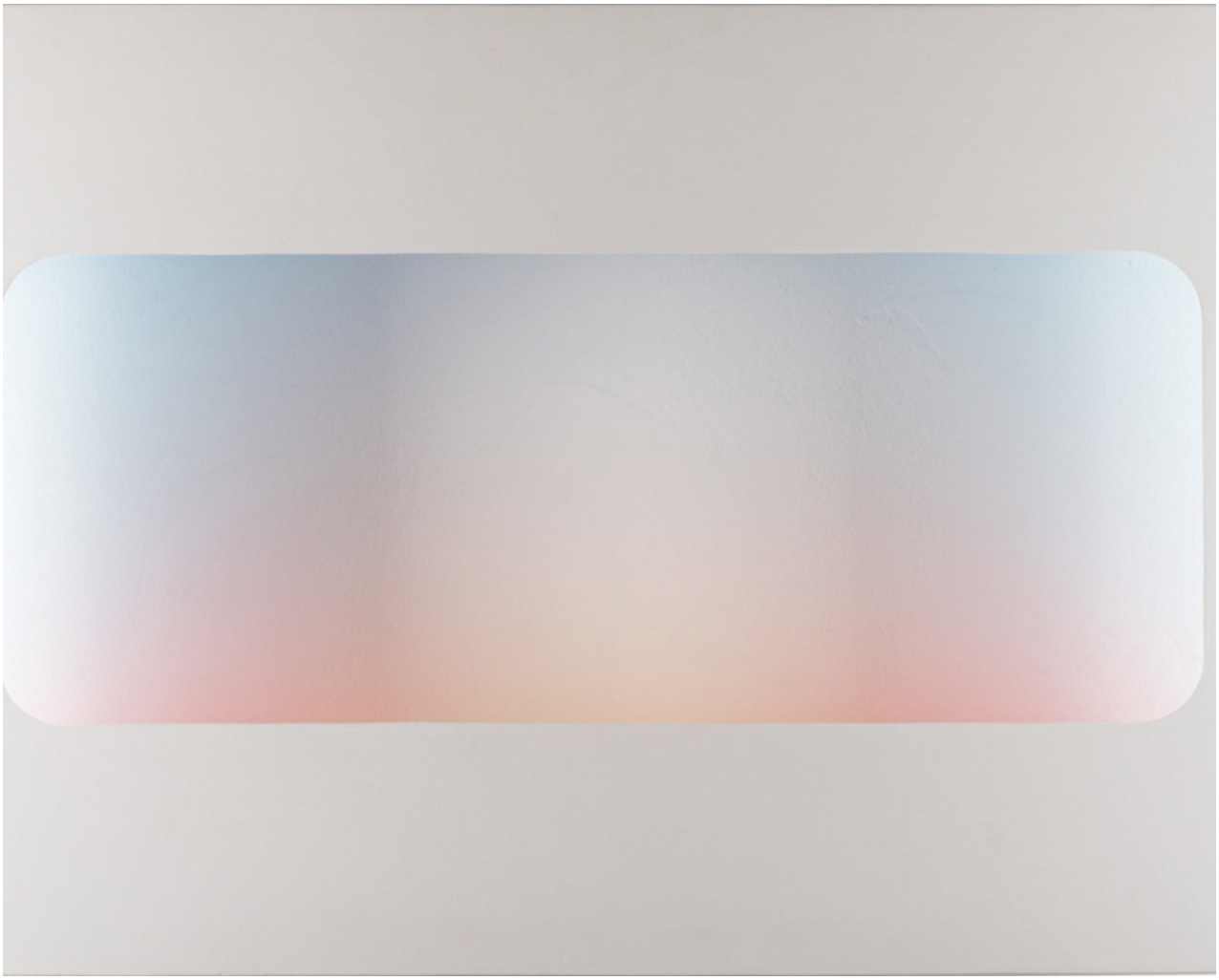
2023. MÁRCIUS

DATAPATRON

www.datapatron.hu

NO. 2.



DATAPATRON MAGAZIN

Adatvédelmi- és adatbiztonsági folyóirat
negyedéves elektronikus kiadvány

IMPRESSZUM

Kiadó:Ivánka-Csontos Andrea e.v.
5000 Szolnok, Dr. Kronberg J. u.9.
Kiadásért és szerkesztésért felelős: Ivánka-Csontos Andrea
Elérhetőség: info@datapatron.hu
ISSN 2939-7553
NO31.||2023.március

DATAPATRON

Előszó

A kibertér olyan világ, amelynek szabályai és szereplői egyelőre nem konkretizálhatóak. Bár léteznek bizonyos elfogadott szabályok, de ezek közel sem elegendőek ahhoz, hogy a felhasználóknak irányt mutassanak. A szakembereken is múlik, hogy világosabbá tegyék a kibertér működését, és segítsék a felhasználókat abban, hogy a legjobb tudásuk szerint használják ki annak lehetőségeit.

Ez a terület folyamatosan fejlődik, és egyre fontosabbá válik az átlagember számára is, hogy megismerje annak újdonságait és használja azokat. Azonban egyelőre nem áll rendelkezésünkre egy egységes szabályrendszer vagy útmutató, amely alapján dönthetnénk, hogy mit tartunk hitelesnek és valódinak.

A jogszabályok, felhasználói kézikönyvek és etikai kódexek csak korlátozottan hasznosak, mivel a kibertér folyamatosan változik és fejlődik. Odafigyeléssel, folyamatos alkalmazkodással és szakmák közötti kommunikációval azonban mindannyian képesek lehetünk a kihívásainak leküzdésére, és az általa nyújtott lehetőségek kiaknázására.

Ivánka-Csontos Andrea

Főszerkesztő

AZ ÁLLAMPOLGÁROK MAGÁNSZFÉRÁJÁRA JELENTŐS VESZÉLYFORRÁST JELENT AZ ELEKTRONIKUS EGÉSZSÉGÜGYI SZOLGÁLTATÁSI TÉR DISZFUNKCIONÁLIS MŰKÖDÉSE

SZERZŐ: DR. ALEXIN ZOLTÁN, SZEGEDI TUDOMÁNYEGYETEM SZOFTVERFEJLESZTÉS TANSZÉK

Az utóbbi néhány évben új használati esetei jelentek meg az EESZT-nek, amelyek az eredeti tervekben nem, vagy csak a távoli jövőben esetleg megvalósuló célként jelentek meg.

Közös jellemzőjük, hogy elvitatják a polgárok önrendelkezési jogait, megkerülik a DÖR (Digitális ÖnRendelkezés) beállításait. Sőt, megjelent az a tendencia is, hogy jogszabállyal fosztják meg a polgárokat az önrendelkezési jogaiktól, a legintimebb adataikat is egyszerűen lemásolják és továbbítják az EESZT-ből privilegizált szereplők számára. Bár a kormányzat korábban ezt határozottan visszautasította, végül mégis egy rendőr egészségügy alakult ki. A betegek ebbe vagy beletörődnek, vagy kétségbe esve próbálkoznak jogorvoslatot nyerni, ami gyakorlatilag lehetetlen, mert az EESZT-ben elkövetett szabálytalan adatkezelések ellen szinte semmilyen jogorvoslati lehetőség nincs, esetleg sérelemdíjért lehet polgári pert indítani.

Az EESZT Információs Portál[1] szigorú fellépést ígér a szabálytalanságok elkövetőivel szemben, ennek azonban nyoma sincs. Egyszerűen tehetetlenek, és nem is látszik semmilyen szándék arra, hogy komolyabb felelősségre vonás legyen. Ma a működtető[2] az incidenseket (a jogellenes hozzáféréseket) bejelenti a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) számára és ezzel a saját részéről elintézettnek tekinti az ügyeket. A NAIH pedig több mint egy év óta nem alakította ki a saját álláspontját arra nézve, hogy az EESZT önrendelkezési beállításainak önkényes feltörésével kapcsolatos panaszok ügyében mit tegyen, egyáltalán tegyen-e valamit? Ennek köszönhetően az orvosi szoftverekben mára megjelent az EESZT-ben szereplő adatok automatikus, és tömeges (a rendelkezésre álló összes adatra kiterjedő) letöltés, sőt az orvosi szoftverbe történő importálás - ezt a NAIH rendben levőnek találta, pedig a nézetem szerint ez a célhoz kötött adatkezelés elvével nem egyeztethető össze,

[1]https://e-egeszsegugy.gov.hu/
[2] Korábban az Országos Kórházi Főigazgatóság volt, de 2023. január 1.-től a belügyminiszter lett a működtető.

sőt a kettős tárolás tiltásának alapelvével sem, viccet csinál az önrendelkezésből, visszaél a páciens bizalmával. Ugyancsak kaphatók olyan háziorvosi, foglalkozás-egészségügyi szakorvosi szoftverek, amelyek az EESZT-ben elérhető vények adatait dolgozzák fel évekre visszamenőleg, és automatikusan ellenőrzik bizonyos gyógyszerek fogyasztását (kiváltását) az orvos számára. Az adatvédelmi hatóság ezt is elfogadhatónak találta. [3]

1. Tisztázatlan jogalap és tisztázatlan felelősségi rendszer

Az EESZT angol nyelvű ismertetőiben a digitális önrendelkezést rendre consent management-nek (hozzájárulás kezelésnek) hivatkozzák, pedig semmi köze sincs a hozzájáruláshoz, ugyanis az adatkezelés előtt nincs tájékoztatás, és nem is feltétele a hozzájárulás az adatkezelésnek. Az informatikai rendszer úgy van kialakítva, hogy a lehető legnagyobb mértékben személytelen legyen, még az orvos se tudjon semmit a rendszer működéséről, főleg ne tudja azt semmiképpen befolyásolni. Ennek ellenére a felelősség az övé, az orvos lett az adatkezelő. A belügyminiszter (korábban OKFŐ) ebben a folyamatban csak működtető (adatfeldolgozó), akit jogszabály rendelt ki erre a feladatra. Azokban az esetekben, amikor az EESZT-ből valamilyen állami szerv számára kell adatot továbbítania, akkor lesz csak a működtető adatkezelő.

A Digitális Önrendelkezésnek valójában kevés köze van a hozzájáruláshoz, a GDPR 21. cikk szerinti tiltakozás jogát valósítja meg, tovább viszi a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló (már régen hatályát vesztett) 1992. évi LXIII. törvény 16/A. § (1) bek. c) pontjának[4] gondolkodásmódját, hogy kötelező adatkezelések esetén is - ha jogszabály megengedi - akkor a polgár tiltakozhat az adatkezelés ellen, hasonlóan ahhoz, ahogyan a polgárok tiltakozhatnak a lakcím nyilvántartóból a lakóhely adatoknak reklámlevelek küldése céljából történő kiadása ellen a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 2. §-a alapján. [5]

Az EESZT esetében a működtető szándékosan nem lett adatkezelő, mert ennek az lenne a következménye, hogy mint adatkezelőnek joga lenne meghatározni az adatkezelés célját, dönthetne a személyes adatok kezeléséről. Azonban jelen esetben egyedül az Országgyűlésnek van erre lehetősége olyan módon, hogy törvényeket módosít, vagy új törvényeket hoz létre. Ezért, ha valakinek jogvitája lenne, nem tud kihez fordulni,

[3] NAIH-5487-12/2022. számú levele.
[4] https://njt.hu/jogszabaly/1992-63-00-00
[5] https://njt.hu/jogszabaly/1992-66-00-00

a szereplők mindegyikét törvény kötelezi az adatkezelésre (az orvost az adatok feltöltésére, a működtetőt az adatmegosztásra és az adatok megőrzésére).

Az EESZT nem tud mit kezdeni az orvosi titoktartással. Az egészségügyi és a hozzájuk tartozó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak.) 8. §-a szerint a kezelőorvos csak annak a másik orvosnak adhat tájékoztatást a beteg állapotáról, aki a beteg gyógykezelésében részt vesz. A szoftver viszont úgy tartja, hogy bárki kezelőorvos, aki ismeri a beteg TAJ azonosítóját. A beteg semmilyen módon nem tudja ezt visszaigazolni, megerősíteni. Külföldi rendszerekben van PIN kód, vagy jelszó, az olasz rendszerben a beteg maga veszi fel a kezelőorvosait a lakossági portálon, ilyen módon a lekérdezések felett ellenőrzést gyakorol. Ez azért nem valósítható meg Magyarországon mert számtalan hatóság kapott lehetőséget adatkérésre, sőt közvetlen elérésre (titokban, tájékoztatás nélkül), ami nem lenne lehetséges, ha kellene ehhez a beteg jóváhagyása. A fentiek ellenére az illetéktelen megtekintések ügyében a törvény a páciensekre hárítja a teljes felelősséget, amiért nem állítottak be korlátozást a hozzáférésekre.

Az Eüak. 35/I. § (2) bekezdése szerint „Ellenkező bizonyításig vélelmezni kell az EESZT felhasználó jóhiszeműségét, ha az önrendelkezési nyilvántartásba bejegyzett nyilatkozat alapján jár el.”. A lakosság több mint 99%-a semmilyen korlátozást nem állított be, az alapbeállítást használja, amely lényegében minden adathoz hozzáférést enged bármely EESZT felhasználó számára.

Kezdetben, 2016. január 1-től az EESZT-ben tárolt adatokat csak három célból lehetett kezelni (Eüak. 4. § (1) bek. a), b), c) pontok):

a) az egészség megőrzésének, javításának, fenntartásának előmozdítása;

b) a betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is; és

c) az érintett egészségi állapotának nyomon követése.

Az egészségügyi dokumentumtár adatait ezen kívül még fel lehetett használni a 4. § (1) bek. d) népegészségügyi, közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele céljából. Itt a mikrobiológiai leletről van szó, amely ha bejelentendő fertőzést mutat, akkor ez a lelet egyúttal a járványügyi bejelentést is szolgálja. Ez az adatkezelési cél egy hatósági intézkedés, itt már eleve nincs is lehetőség élni az önrendelkezés lehetőségével.

2020-ban jogszabály módosítással[6] az összes magánszolgáltatót, köztük a foglalkozás-egészségügyi szakorvosi rendelőket is csatlakozásra, majd 2020. június 1-től kezdve pedig az ellátások jelentésére kötelezték. Az adatok lekérdezésére azonban ekkor még nem volt meg a jogi felhatalmazás (Eüak. 4. § (2) bek. o) pont).

2021. január 1-től az EESZT-ben tárolt adatok kezelésének lehetséges céljai kibővültek még egy ponttal, az Eüak. 4. § (2) bek. f) pontjával: „a társadalombiztosítási, illetve szociális ellátások megállapítása, amennyiben az az egészségi állapot alapján történik, valamint a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló törvény szerinti rendvédelmi egészségkárosodási ellátás megállapítása, továbbá a Nemzeti Adó- és Vámhivatal személyi állományának jogállásáról szóló törvény szerinti egészségkárosodási ellátás megállapítása”. Egyúttal az Országos Rehabilitációs és Szakértői Intézet (ORSZI) megkapta a jogot az EESZT-hez történő hozzáféréshez.. A jogalkotó ismét nem határozta meg az adatkezelés jogalapját, pedig itt a hozzáférés komoly emberi jogi kérdéseket vet fel. Azt azért lehet tudni, hogy a rehabilitációs eljárás során a hatóság az EESZT-től függetlenül is megszerzi a sérült polgár bárhol elérhető összes egészségügyi adatát születésétől fogva, ezért az emberi méltóságot jelentősen megterheli az eljárás, a magánszféra itt eleve nem létezik. Rendkívül nagy lelki terhet jelent a páciensnek, ha erre kényszerül. A hatósági eljárás feltétele, hogy az adateléréshez a beteg (sokszor teljesen kiszolgáltatott, elesett, megrokkant személy) hozzájáruljon.

2021. június 29-étől [7]az Országgyűlés visszamenőleges módon lehetővé tette az EESZT-ben tárolt adatok kezelést huszonhét különböző, az Eüak 4. § (1) és (2) bekezdésben felsorolt összes célból. Az új célok esetében a jogalkotó ismét nem határozta meg (egyiknél sem) az adatkezelés jogalapját. A NAIH ellenezte a módosítást, a parttalan adatelérés lehetővé tételét, teljesen hiába.[8] Mivel ezek az adatkezelések a GDPR előtti időkben is kényszerintézkedések voltak, ezért a szakma úgy tartja, hogy a GDPR után is a GDPR 6. cikk (1) bek. c) pont alapján történik a hozzáférés, ami komoly ellentétben állhat a DÖR beállításaival. Egyértelművé vált, hogy az EESZT működtetőjének van technikai lehetősége megkerülni a DÖR beállításait, sőt akár a naplófájlba történő bejegyzést is, ha betegadatokra van szüksége.

Ez egyértelműen látszik a Covid-19 igazolvány, a zöld útlevél adatkezelésénél, vagy a NEAK-nál létrehozott (Covid-19) pandémia értékelő regiszter feltöltésénél (Eüak. 35/Q. §), vagy az Operatív Törzs

[6] Az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról 39/2016. (XII. 21.) EMMI rendelet 2. § (1a) bekezdése, 22. § (5a) bekezdése.
[7] https://njt.hu/jogszabaly/1997-47-00-00.43
[8] https://www.naih.hu/files/NAIH-3290-2-2020-200409.pdf

számára adott közvetlen EESZT hozzáférés szabályozásában. Az utóbbi kettőről a beteg nem is szerezhet tudomást, mert ezek az adattovábbítások nem szerepelnek a naplófájlban.

A szerző úgy tapasztalja, hogy az EESZT-be az összes egészségre vonatkozó személyes adat feltöltése, és a halál után 10 évig történő megőrzése kötelező adatkezelés (GDPR 6. cikk (1) bek. c) pont. A kezelőorvos lekérdezését közérdekű adatkezelésnek tartják (GDPR 6. cikk (1) bek. e) pontja), ami ellen lehet tiltakozni, azonban ezt a kezelőorvos felülbírálhatja. A tiltakozást csak előzetesen, egy Kormányablaknál vagy a lakossági portálon lehet megtenni, az orvosnál már nem, mert a szoftver erre nem ad lehetőséget. A beteg itt már nem nyilváníthatja ki a szándékát. Az állami szervek felé történő adattovábbítás az EESZT-ből minden esetben kötelező adatkezelés (GDPR 6. cikk (1) bek. c) pont).

2. A lakosság nagy többsége számára lényegében elérhetetlen önrendelkezés

Az EESZT Információs Portál[9] felhívja a polgárok figyelmét arra, hogy van joguk és lehetőségük korlátozásokat beállítani azonban a weboldal működését, az egyes korlátozások hatásait, működését már nem magyarázza el. Ezért sok ember nem tudja érdemben használni ezt a szolgáltatást.

A kezelőorvos által használt szoftver, ha a beteg ezt külön nem tiltja meg értesíti az orvost arról, hogy korlátozások vannak érvényben. Ez sokszor félelmet kelt a páciensekben. Főleg az idősek félnek attól, hogy nézeteltérés alakuljon ki a háziorvosukkal, mert már nem tehetik meg, hogy egy 20 km-re rendelő másik háziorvoshoz átjelentkezzenek. A hivatalos EESZT promóciók is azt a nézetet képviselik, hogy mindenki az alapbeállítást használja, mert az már megvédi az adataikat.

Az alapbeállítás kizárólag orvosi érdekeket vesz figyelembe: Magyarország összes orvosa kapott hozzáférést lényegében az összes feltöltött adathoz. Ez szöges ellentétben áll a GDPR 25. cikkével, a privacy-by-default elvével. Jól kihasználja azt, hogy a lakosság jelentős többségét nem érdeklik adatvédelmi kérdések, csendes beletörődéssel tudomásul vesznek szinte bármit. Ennél megengedőbb az alapbeállítás már nem igen lehetne, hiszen bármely EESZT felhasználó számára elérhetővé teszi a nőgyógyászati, urológiai, genetikai, lombikkezelési, a nemi identitással kapcsolatos eltérések, fejlődési rendellenességek stb. adatokat, teljesen lemezteleníti a pácienseket. A páciensek arról sem tudnak, hogy az EESZT egy másik alrendszere, az eProfil önrendelkezési beállításait külön kell megtenniük.

[9] https://e-egeszsegugy.gov.hu/

A eProfil esetében ugyancsak nem érvényesül a privacy-by-default elve, mert kezdetben a „minden felhasználó minden adatot láthat, és új adatot vehet fel” beállítás az aktív vö. a GDPR 25. cikk (2) bekezdés utolsó mondatával: „Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.”.

Az önrendelkezési beállításokat közelebbről megvizsgálva azt állapíthatjuk meg, hogy ha a Magyarországon praktizáló összes orvos hozzáférése helyett egy ennél szűkebb halmaznak adnánk csak hozzáférést pl. csak egy rendelőintézet orvosainak, akkor azt kizárólag az összetett rendelkezéssel szabályozott állapotban tehetjük meg. Tizenhárom előre megadott orvosi szakterület (pl. urológia, nőgyógyászat, fejlődési rendellenesség, onkológia stb.) adatainak elérését egyenként megtilthatjuk az egyszerű rendelkezéssel szabályozott állapotban, de az ezeken kívül még fennmaradó adatok eléréséről itt nem rendelkezhet az állampolgár. Az EESZT jelenleg nem tekinti szenzitív adatnak például a genetikai, neurológiai és endokrinológiai adatokat.

Az összetett rendelkezéssel szabályozott állapot nem az egyszerű polgároknak készült. Azt várja el, hogy elsőrendű logikai nyelveket, a predikátum-kalkulust ismerő felhasználók üljenek a gép előtt. Hozzáférési szabályokat kell alkotniuk, amelyek mindegyike egy-egy logikai formula. Egy részletesebb beállítás pedig akár 50-100 szabályt is tartalmazhat. Ilyet egy jól képzett informatikus tud létrehozni. A rendszer nem ad lehetőséget a szabályrendszer tesztelésére, kipróbálására, a szabályokat nem lehet menteni. A szabályokkal való munkát nehézzé teszi, hogy megengedő és tiltó szabályok is lehetnek, amelyek akár konfliktusba is kerülhetnek egymással. Amennyiben megengedő és tiltó szabály is vonatkozik egy EESZT felhasználóra, akkor a rendszer a megengedőt veszi figyelembe - ez is azt bizonyítja, hogy itt nem a hozzájárulás jogalapot alkalmazzák (mert annak egyértelműnek kell lennie), hanem ez valamiféle tiltakozás.[10]

Az EESZT működtetője 2021. október 12-én lekapcsolta az eProfil önrendelkezési beállításait, a korábbi állampolgári beállításokat pedig visszaállíthatatlanul törölte. A szerző a NAIH-hoz fordult és ezért 2022. január 14-én végül visszakapcsolták, de nem tudták a korábbi beállításokat helyreállítani, azok elvesztek. A NAIH végül hatósági eljárást indított a súlyos incidens körülményeinek kivizsgálására - máig nincs eredmény, holott felmerült a Btk. 267. § szerinti,

[10]A szerző készített EESZT oktató videókat: https://www.tisztessegesadatkezeles.org/eeszt-tajekoztatok/

nemzeti adatvagyon elleni bűncselekmény gyanúja. Megdöbbentő, hogy mennyire félvállra veszik az állampolgárok legbizalmasabb adatainak sorsát!

3. Az egészségügyi szervek és az orvosok korlátozhatatlan jogot formálnak a személyes egészségügyi adatokhoz történő hozzáférésre

Ahogy az elektronikus számítógépek megjelentek a kórházakban azzal együtt egyből meg is szűnt a betegek titoktartáshoz való joga. Az adatvédelem nagy tragédiája, hogy a 90-es évektől kezdve ebben semmilyen előrelépés nem történt. Ugyanis hiába lehetne az informatikai rendszerben korlátozásokat tenni bizonyos adatok elérhetőségére (pl. pszichiátriai, urológiai, nőgyógyászati stb.) ezzel nem éltek, a hozzáférések korlátozására semmilyen protokoll, megegyezéses megoldás nem született. Ma minden nagyobb intézmény, rendelőintézet, kórház lényegében korlátlan adatelérést biztosít a felhasználóknak harminc évre visszamenőleg. Nem csak orvosoknak, hanem orvosírnoknak, ápolóknak is. Az egészségügyi adatok kezeléséről szóló törvény (Eüak.) is ezt a szemléletet erősíti, ugyanis állami adatbázisok tucatjait hozta létre kötelező adatkezelésként, az érintett személyek jogait semmibe véve. Ez ma is így van, nem is változott meg. Ma egyébként a kórházi orvosok a helyi informatikai rendszert sokkal szívesebben használják, mert egyrészt sokkal több régebbi adathoz férnek hozzá, másrészt a betegek esetleges korlátozásaival nem kell vesződniük. Ugyanis ezek nem léteznek.

Az ebből a körből kimaradt háziorvosok, foglalkozás-egészségügyi szakorvosok azonban nagy várakozással tekintenek az EESZT-re, amely rálátást ad nekik a betegeik egészségügyi múltjára. Ráadásul nem kell a betegekkel veszekedni, hogy hozzák el a leleteiket, akár akaratuk ellenére is hozzáférhetnek az adatokhoz. Egyes foglalkozás-egészségügyi orvosok az interneten nyíltan buzdítják egymást a DÖR feltörésére, mondván, hogy ehhez nekik joguk van.[11] A szerző szerint egyáltalán nincs, ugyanis az Eüak. 13. § b) pontja azt mondja ki, hogy a foglalkozás-egészségügyi orvos az alkalmasság megállapításához szükséges adat átadására felhívja a munkavállalót, aki ezt köteles átadni. Ez többnyire egy lelet. De messze nincs arról szó, hogy az orvos szabadon szörfözhetne az EESZT-ben kényszerintézkedéssel összegyűjtött, évekre visszamenő bizalmas adatokon.

A fenti gondolkodásmód abban is tetten érhető, hogy a tiltakozás joga egyre inkább relativizálódik, azaz újabb és újabb indokok merülnek fel arra, hogy ne vegyék figyelembe.

[11] https://munkaegeszsegugy.hu/breakglass/

A szoftver úgy készült, hogy az orvost semmilyen módon nem akadályozza az adatelérésben, egy checkbox-ra kattintva korlátlan elérést kap a legintimebb adatokhoz is, amelyeknek semmi köze sincs az életmentéshez.[12] Olyan adatokhoz is, amelyek értelmezéséhez nincs meg a szükséges kompetenciája pl. genetikai adat, pszichiátriai adat, a nemi identitás zavarával összefüggő adat vagy egy lombikkezeléssel összefüggő adat stb. A szerző Facebook csoportjában[13] sorra jelennek meg hozzászólások, amelyek arról tudósítanak, hogy orvos, vagy a foglalkozás-egészségügyi orvos fegyverként használja az EESZT-t a betegekkel szemben, akik zömmel tehetetlenek. A legdurvább eset az volt, amikor a pszichiáter zsarolta a betegét azzal, hogy ha nem tűri el a DÖR feltörését, akkor nem vállalja a kezelését. De több személyiség torzulást, hatalmaskodást és visszaélést panaszoltak be a csoporttagok.

Az ember azt gondolná, hogy az EESZT-ben tárolt adatokra nem veti rá magát az állam azonnal, de aki ezt gondolja, téved. Dr. Kásler Miklós javaslatára a kormány az egészségügyi szolgáltatások Egészségbiztosítási Alapból történő finanszírozásának részletes szabályairól szóló 43/1999. (III. 3.) kormányrendelet módosításával[14] 2020 áprilisában elrendelte, hogy az EESZT-ből, a magán és állami fekvőbeteg-ellátó intézmények által jelentett adatokból továbbítsák a NEAK-hoz minden hónap elején az intézmény nevét, az ellátó osztály azonosítóját, nevét és szakmakódját, az ellátott beteg TAJ-számát, annak hiányában egyéb személyazonosítóját, törzsszámát, érvényes biztosítás országát vagy a beteg állampolgárságát, a felvétel és a távozás időpontját és az ellátó orvos kódját. A kibocsátás utáni napon azonnal hatályba lépő rendelet célja az volt, hogy megbüntesse azokat a renitens fekvőbeteg intézményeket, amelyek nem jelentik le az ellátásokat (műtéteket) az EESZT-be. A NEAK nem fizette ki a számukra a térítési díjat. Nem világos, hogy a magán ellátóktól származó személyes adatokkal mit tesz a NEAK, mire használja azokat. A rendelet annyira sietve készült, hogy az adatkezelés időtartamáról sem rendelkezett.

A Covid-19 járvány 2020-ban érte el Magyarországot, és ez adott okot arra, hogy legelőször az innovációért és a technológiáért felelős miniszter kapjon lehetőséget az EESZT-ből bármilyen adat megismerésére (46/2020. (III. 16.)), azután a belügyminiszter és az emberi erőforrások minisztere (83/2020. (IV. 3)), és végül az Operatív törzs (93/2020. (IV. 6.)). Később az iskolák kaptak jogot arra, hogy lekérdezzék a tanulóik és a dolgozók Covid-19 fertőzöttségi adatait, aztán megjelent a védettségi igazolvány és a zöld útlevél.

[12] Az Egyesült Királyságban és Németországban is vannak külön életmentő adatok, és csak ezek érhetők el életveszély esetén, nem az összes létező adat.
[13] https://www.facebook.com/groups/NagyTiltakozas
[14] 5/C. §

Végül a Pandémia értékelő regiszter, amelyek mind az állam korlátlan hatalmát kívánják demonstrálni. Ezekben az esetekben a DÖR semmit sem ér, az adatokat egyszerűen kényszerintézkedésként veszi el az állam az EESZT-ből.

4. Az adatokon végzett kutatás is kényszerintézkedés

Az adatokon végzett kutatás jogalapjának tekintetében az állapítható meg, hogy az 1992. évi LXIII. törvénynek azzal, hogy csak két adatkezelési jogalapot ismert: a hozzájárulást és a kötelező adatkezelést, sikerült egy az alapvető jogokat jelentősen sértő zsákutcába manővereznie a jogalkotást. Ez harminc éve tartja magát, az egészségügynek roppant kényelmes. Arról van szó, hogy el kellett dönteni, hogy az orvostudományi kutatás hozzájárulás alapú legyen-e vagy kötelező. A kettő közül egyértelműen az utóbbi vált jogi normává. A szerző által benyújtott 129/B/2008. számú alkotmánybírósági indítvány[15] elbukott, az alkotmánybíróság is megerősítette, hogy ez így jól van - a személyes egészségügyi adatok kutatási célú felhasználásába ne szóljon bele a páciens.
Mivel ez egy kötelező adatkezelés, ezért felvilágosítás sem szükséges.

Az, hogy ez szöges ellentétben áll a nemzetközi kutatásetikai szabályokkal (Helsinki Nyilatkozat, az ET Oviedói Egyezménye), nem zavarta a jogalkotót. Ha korábban lettek volna más jogalapok, akkor esetleg megfontolhatták volna, hogy másikat válasszanak, de így a kötelező adatkezelés maradt. A GDPR óta semmi sem változott meg. Az ETT ugyan adott ki állásfoglalást az Oviedói Egyezménnyel kapcsolatos kötelezettségről 2019-ben[16] (17 évvel a hatályba lépése után a szerző indítványára), de nyilván ezt a jogalkotó nem vette figyelembe. Az összes magyar központi egészségügyi adatállomány (regiszter) a GDPR 6. cikk (1) bek. c) pontja alapján működik, végtelen adatmegőrzési idővel. Az érintetti jogok gyakorlatilag nem léteznek velük kapcsolatban, az adatok felhasználása semmilyen ellenőrzés alatt nem áll. Érinthetetlenek. Ez nem jelenti azt, hogy minden orvostudományi kutatás adatkezelésének a jogalapja a GDPR 6.cikk (1) bek. c) pontja. Nemzetközi együttműködésben megvalósuló vagy nemzetközi standardoknak megfelelő kutatások esetén a külföldi partnerek elvárják a hozzájárulást a páciensektől (és vannak egyéb jogaik is), azonban ez csak néhány százaléka az összes kutatásnak.
Az Eüak. 21. § (1) bekezdése szerint „Tudományos kutatás során a tárolt adatokról nem készíthető személyazonosító adatokat is tartalmazó másolat.”

[15] http://public.mkab.hu/dev/dontesek.nsf/0/B7EFDA98413617F6C1257ADA00526224?OpenDocument
[16] https://ett.aeek.hu/wp-content/uploads/2019/12/eu_es_gen_adatok_kutfel_201912.pdf

A személyazonosító adatok a név, a születési név, az anyja neve, születési hely és idő, TAJ, lakcím. Ezek nem szerepelhetnek a tudományos kutatáshoz esetlegesen lemásolt adatokban. A szöveg 1997 óta nem változott, pedig azóta már ismert tény, hogy a személyes azonosíthatóság ezek hiányában is fennállhat. A 90-es években bevezetésre került a kvázi-azonosító fogalma.[17] Születtek eredmények arra nézve, hogy a születési dátum és a lakóhely irányítószáma és a nem (férfi, nő) adatok mennyire egyértelműen azonosítják a polgárokat. Azonban ezeket az érveket lesöpörte a Kúria 2019-ben[18], amikor kimondta, hogy az ún. Tételes Egészségügyi Adattárházban tárolt adatok nem személyes adatok, ezért az érintettnek nincs joga pl. a hozzáféréshez, vagy a tiltakozáshoz. Annak ellenére, hogy az adatok között szerepel a születési dátum, lakóhely irányítószáma, nem, ellátás dátuma, kezelőorvos kódja, intézet kódja, betegség kódja, ellátás kódja, felírt gyógyszer stb. Egyszerűen nem értette meg egyik bíróság sem, hogy ha nincs az adatok között a név, akkor az hogyan lehet mégis személyes adat. Szakmai körökben volt ezzel kapcsolatban néhány levélváltás.[19]

A szerző által indított pernek volt egyetlen pozitív hozadéka: az Eüak. 35/L. § (5) bekezdése, amely a betegregiszterek esetében lehetővé tette az érintettek hozzáférését az tárolt adatokhoz.

A Szegedi Ítélőtábla egy végzése miatt került be ez a törvénybe, de nem terjed ki a Tételes Egészségügyi Adattárra. A per negatív hozadéka az lett, hogy drámai módon megnőtt az olyan regiszterek száma, amely úgy tartják, anonim adatokat kezelnek, hiszen nem szerepel bennük a név, anyja neve, lakcím adat. Kapcsolati kóddal tartják nyilván az állampolgárokat, semmilyen figyelmet nem fordítanak arra, hogy vajon más kvázi-azonosítók vannak-e az állományban.

Az EESZT működtetője konferenciákon kérdésre azt a választ szokta adni[20], hogy egyelőre az EESZT adatok nem használhatók fel orvostudományi kutatásra, mert az Eüak. 21. §-a intézményekről beszél, az EESZT pedig nem egészségügyi intézmény, így nem vonatkoztatható rá ez a szakasz. Erről azonban az ETT TUKEB nem tud, és több olyan kutatásetikai jóváhagyást adott ki az elmúlt években, amely szerint a kutatók az EESZT-ből is vesznek át adatokat.

Az ETT TUKEB 2022-ben rendben levőnek tartotta, ezért engedély adott arra, hogy egy kutatás során a teljes arckoponyáról készült milliméteres felbontóképességű 3 dimenziós CT képeket továbbítsanak magáncéghez, mondván az anonim (mivel nem szerepel mellette a név vagy a TAJ). Természetesen az érintettek tájékoztatása és beleegyezése nélkül. A magyar gyógyszertárak vényadatait egy nemzetközi cégháló felvásárolja

[17] https://dataprivacylab.org/projects/identifiability/paper1.pdf
[18] https://ukp.birosag.hu/portal-frontend/stream/birosagKod/0001/hatarozatAzonosito/Pfv.20954_2018_6/
[19] https://www.linkedin.com/pulse/k%25C3%25BAria-%25C3%25ADt%25C3%25A9lete-az-%25C3%25A1eek-adatkezel%25C3%25A9s%25C3%25A9r%25C5%2591l-alexin-zoltan/
[20] Legutóbb a Digital Health Summit 2022, Budapest rendezvényen: https://dhs.ap.hu/

és értékesíti. Az adatok álnevesítettek. A NAIH-nak sikerült elérnie, hogy a születési dátum, a lakóhely irányítószáma nincs az adatok között, azonban a cég ennek ellenére a teljes magyar lakosság egyénekre szóló vénytörténetével rendelkezik, benne a kiváltott gyógyszerekkel, dátumokkal, gyógyszertár-, betegség- és orvoskódokkal. Erre azt mondják, hogy anonim, amivel a szerző egyáltalán nem ért egyet. Véleménye szerint ezek a historikus adatok egyértelműen személyesek.

Összefoglalás

Az EESZT-ben felhalmozott adatok mennyisége folyamatosan növekszik, és a jogalkotás egyre újabb célokat talál az adatok számára, amelyet visszamenőleges kényszerintézkedéssel valósít meg. Az EESZT adatait máris elérhetővé tették a nemzeti adatvagyonról szóló 2021. évi XCI. törvénnyel ipari szereplők számára. Rendkívül aggályos, hogy a Nemzeti Adatvagyon Ügynökség és a vele kapcsolatba kerülő adatkezelők semmit sem tudnak az azonosíthatóságról, a kvázi-azonosítókról és így fogják az érintettek tájékoztatása és adatvédelmi ellenőrzés lehetősége nélkül kiadni az adatokat. Ma az EESZT létezése napi egzisztenciális kockázat, ugyanis felelősségre vonás nélkül történhet meg az illetéktelen hozzáférés, vagy az önrendelkezési beállítások feltörése.

Az EESZT-ből kiszivárgott információ miatt az állampolgár elveszítheti a munkáját, társadalmi megbecsülését, a magánszférájának utolsó kicsiny maradékát. Az állam pedig bárkiről, bármilyen szenzitív információt megszerezhet, rendőrségi bizonyítékraktárnak, titkosszolgálati adattárháznak használja az adatokat. Az állampolgároknak csak a távolmaradás lehet az egyetlen esélye, a magánorvos, a vény nélkül kapható gyógyszer, a magánorvossal felíratott TAJ nélküli vény vagy a külföldi gyógykezelés. Az egészségügyben az információs önrendelkezés nem létezik, sosem volt. Az állam korlátlan hozzáférése kirobbanthatatlanul belekövesedett már a jogrendszerbe, alkotmánybírósági határozatok legalizálják, ezért a helyzet teljesen reménytelen.

A DPO SZEREPE AZ ADATVÉDELMI ÖNELLENŐRZÉSBEN, AZ ÖNELLENŐRZÉS SZEREPE AZ ADATVÉDELMI MEGFELELÉSBEN

SZERZŐ: DR. CSEKŐ KATALIN - ADATVÉDELMI TISZTVISELŐ: AUCHAN MAGYARORSZÁG KFT, MH AUCHAN BENZINKUTAK KFT., FŐTITKÁR: MAGYAR ADATVÉDELMI TUDATOSSÁGÉRT TÁRSASÁG EGYESÜLETE

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) 39. cikk (1) bekezdésének b) pontja[1] az adatvédelmi tisztviselő feladatai közé sorolja az ellenőrzésekben való részvételt. Mégis azt olvashatjuk a Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolóiban, hogy a DPO-k fele nem vesz részt ellenőrzési/audittervek kidolgozásában, vagy ellenőrzések/auditok elvégzésében.[2]

Az ellenőrzésre időt szánni az alapelveknek megfelelő működés egyik kulcseszköze lehet, így adatvédelmi tisztviselőként,ha eddig nem vettünk részt belső ellenőrzésben a klasszikus értelemben vett adatvédelmi auditban, érdemes ezen változtatnunk és minden lehetséges ellenőrzési szintben megtalálni a szerepünket.

Az adatkezelőnél végezhető ellenőrzések három szinten valósíthatóak meg:

1. az adatvédelmi önellenőrzés, melyet az adatkezelő terület végez
2. adatvédelmi ellenőrzés, melyet nem az adatkezelő terület, hanem vagy az adatvédelmi terület, vagy egy szakmai szempontú ellenőrzést végző más szervezeti egység végez; az ellenőrzésen túl magában foglalja az egyes szintű önellenőrzés vizsgálatát, ami az önellenőrzés megtörténtének rendszerességéről, minőségéről és megfelelőségéről ad információt
3. adatvédelmi audit az adatkezelőnél vagy adatfeldolgozóinál az adatkezelő audit részlege vagy külső auditor által, ahol adott esetben a DPO mint szakértő támogatja az auditorok munkáját.

Jelen cikkben nem a klasszikus, az ellenőrzés 3. szintjét jelentő adatvédelmi audittal, hanem az 1-2. típusú belső ellenőrzési folyamatokkal foglalkozunk.

[1] Az adatvédelmi tisztviselő ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

[2] A NAIH 2021-es és 2020-as beszámolói alapján 2020-ban a DPOK-k 42,8%-a, 2021-ben 47,2%-a készített belső ellenőrzési (audit) tervet; 2020-ban 40,5%, 2021-ben 44,8% folytatott dokumentált módon belső ellenőrzést (auditot)

Biztosan sokan ismerik az ikonikus mondást: „Nem lehet minden pofon mellé egy forgalmi rendőrt állítani”.[3] Ez az adatkezelő szervezetének működtetésére is igaz, pláne a nagyszámú adatkezelést végző szervezeti egységgel rendelkező adatkezelőknél. A DPO bármennyire is szeretné, fizikailag lehetetlen, hogy folyamatosan mindenhol személyesen vizsgálja az adatvédelmi megfelelést, így szüksége lesz olyan kulcsemberekre, akik ezt rendszeresen megteszik, majd megosztják vele az ellenőrzések eredményét, ő pedig levonhatja belőle a következtetéseket.

Ha az adatvédelmi tisztviselő megtalálta a kulcsembereit, nem dőlhet hátra azt követően hogy az adatkezelő illetékes területével karöltve végigviszi az önellenőrzési feladat és felelősség szervezési intézkedésbe (szabályzat, munkaköri leírás) foglalását. Mivel az önellenőrzést végző területek a folyamatokat még az oktatások ellenére is elsősorban szakmai és nem adatvédelmi szemmel nézik, a DPO segítségére és szakértelmére van szükség önellenőrző listák kialakításához, melynek köszönhetően már a terület kezében lesz az önellenőrzés elvégzésének kulcsa. Gyakorlati tapasztalatom, hogy nem elég leírni, hogy mit ellenőrizzenek, de szükséges a jó megoldás ismérveit is felsorolni: pl. ha ellenőrizni kell, hogy az adatkezelési tájékoztató aktuális-e, akkor rendszeresíteni kell egy olyan felületet, ahol az összes aktuális anyag megtalálható, de még ennél is jobb megjelölni a tájékoztató legújabb részét, melynek alapján néhány másodperc alatt kiderül az ellenőrzést végző számára, hogy az általa látott anyag aktuális-e.

Az adatvédelmi tisztviselő az önellenőrzésekből kapott visszajelzések alapján fogja látni, hogy a követelmények, amelyeket támasztott a munkatársak felé, számukra érthetőek és valóban illeszkednek-e a munkafolyamatokhoz. Ha a hiányosságok folyamatosan fennállnak vagy ismétlődnek, annak csak az egyik lehetséges oka a munkatársak hanyagsága. Több olyan ok is lehet, ami a DPO-n is múlik: tudatosítás, megfelelő feladatmeghatározás hiánya, illetve az adatvédelmi követelmények folyamatidegensége. Az önellenőrzések kiértékelésekor tehát nem az az egyetlen következmény, hogy a mulasztók felelősségre vonását kezdeményezze a vezetőknél az adatvédelmi tisztviselő, hanem célszerű párbeszédet indítania a szakmai és az adatkezelési követelmények jobb összhangja érdekében.

A belső fejlődésből leginkább az olyan területeken lehet látványosan profitálni, ahol az adatkezelés a kirakatban, az érintettek szeme előtt zajlik, és ekképpen különösen alkalmas arra, hogy az érintett akár az adatkezelőhöz benyújtott panaszt,érintetti kérelmet kihagyva,

[3] Rejtő Jenő: Piszkos Fred, a kapitány

a hatósághoz forduljon. A személyesen, helyben nyújtott, adatkezeléssel járó szolgáltatások, vevőszolgálatok üzemeltetése pl. tipikusan ilyen eset. Hétköznapi hibák vezethetnek hatósági ügyekhez: hiába készül el a világ legtökéletesebb adatkezelési tájékoztatója, ha annak nem a legfrissebb, az adatkezelést ténylegesen leíró változata kerül az érintett elé. Ha nem ellenőrizzük rendszeresen, hogy incidensmegelőző intézkedéseink működnek-e sokkal nagyobb eséllyel bekövetkezik a baj: pl. a kereskedelemről szóló 2005. évi CLXIV. törvény 5.§ (4a) bekezdése alapján a vásárlók könyvéből haladéktalanul ki kell tépni a bejegyzést tartalmazó lapokat[4]. Napi szintű önellenőrzés nélkül az adatvédelmi incidensnek hatalmas az esélye, ha ezt a rendelkezést nem tartják be. Ugyanígy hiába készültek remek fotók a honlapra, ha azoknak az adatvédelmi hátterét nem rendezték.

A DPO által végzett ellenőrzés

A szakmai irányító területek ellenőrzése, holott már egy magasabb szintű ellenőrzés, a DPO szempontjából és a módszereket illetően megegyezik az önellenőrzésekkel, így jelen pontban kizárólag a DPO ellenőrzéseit tekintjük át.

Az adatvédelem és művelői még mindig gyakran részesülnek abban a negatív megítélésben, hogy elefántcsonttoronyból szónokolnak. A DPO által végzett ellenőrzés az egyik legjobb módja annak, hogy erre rácáfoljon. Ez természetesen csak akkor valósul meg, ha túl tud lépni az adatbekéréssel végzett ellenőrzéseken és visszatérő jelleggel helyszíni ellenőrzésre, helyszínbejárásra is sort kerít. Sok telephely esetén persze nem fog mindenhova eljutni egy év alatt, de ezekből a látogatásokból is számos következtetés levonható.

A módszer (beszélgetés, iratbetekintés, helyszínbejárás, próbavásárlás) ezekben az esetekben teljes mértékben rajta múlik. Ami biztos, hogy érdemes az ilyen látogatások során nyitott szemmel járni, mert ez a legjobb alkalom arra, hogy láthassa, valóban minden folyamatba be lett-e vonva, vagy szembejön vele olyasmi, amiről nem tudott, így adatvédelmi szempontból kockázatot jelent az érintettekre és az adatkezelőre is. Az önellenőrzéshez képest itt mindenképpen plusz tényező a szakmai szem. Számos, látszólag bárki számára észlelhető hibát lehet így észrevenni, pl. azonnal kiszűrhető, ha az adatkezelési tájékoztatót úgy készítik el helyben, hogy az az átlagember számára nem látható helyen van vagy olvashatatlan.

[4] Más vásárlók által a vásárlók könyvébe bejegyzett személyes adatok megismerése lehetőségének kizárása céljából a vásárlók könyvéből a kereskedő a bejegyzést követően haladéktalanul eltávolítja a (4) bekezdés szerint panaszt vagy javaslatot tartalmazó oldalt, azt elzártan - a folyamatos sorszámozás rendjének megfelelően - megőrzi és a hatóság felszólítására rendelkezésre bocsátja

Lehet, hogy akad, aki úgy gondolja, hogy ezek elengedhető szempontok, de ha felidézzük pl. a Vodafone bírságot[5], ahol az ügy azért indult, mert „a bejelentő továbbá arról számolt be, hogy a „számhúzó rendszer" második „választós képernyőjén" lehet látni a többihez képest kevésbé feltűnő betűkkel és helyen elhelyezve egy tájékoztatást", máris látható, hogy szükség van a szakértői szemre a „terepen".

A helyszínen a hibákon túl felfigyelhetünk a megváltozott körülményekre, amelyre reagálni kell, pl. megszűnt adatkezelési célokhoz tartozó dokumentáció eltávolítása, helyiség funkciójának megváltozása - kamerás adatkezelések kapcsán.

Ezen az ellenőrzési szinten a DPO-nak feladata az is, hogy az általa végzett ellenőrzés eredményét összevesse az önellenőrzések eredményével, így könnyen kiszűrhető, ha a területi kulcsember nem adott meg valós adatot, nem vagy nem megfelelően végezte az ellenőrzést vagy egy hiba, hiányosság visszatérő jellegű az adott területen vagy ugyanaz a hiba több telephelyen, szervezeti egységnél is fennáll.

Ezeknek az ellenőrzéseknek ugyanúgy megvan az a haszna, mint az önellenőrzésnek: csökkenti az adatkezelőnél jelentkező kockázatokat, a bírságnak való kitettséget, de ezen túl is hatalmas profitot jelent a DPO számára: folyamatosan tanulhat újat az adatkezelő szervezetéről, naprakész lehet, kétoldalú kommunikációt alakíthat ki az adatkezelő területekkel, reagálhat a problémáikra, ezzel együtt emészthetőbbé teheti számukra az adatvédelmi elvárásokat, megalapozhatja a területek bizalmát, ezzel pedig azt, hogy ha éppen nincs a helyszínen, akkor is bevonják a folyamatok kialakításába.

Ezek az ellenőrzések tehát olyan eszközök, amelyek támogatják az adatkezelő adatvédelmi megfelelését, egyben pedig jobb szakemberré tesznek minket. Éljünk velük!

[5] NAIH/2020/2758/4. számú határozattal kiszabott 60 millió Ft-os bírság

SIP BEMUTATKOZÁS

A Nemzetközi Gyermekmentő Szolgálat 1998 óta rendez médiakonferenciákat, melyek témája a gyerekek és fiatalok médiafogyasztási szokásai és ennek hatása az ő és a családjaik életére.

A Szolgálat 2009 óta az európai uniós Safer Internet Program (SIP) konzorciumvezetője, a programban tudatosságnövelő központként és forródrótként (hotline) is működik. Célja és feladata a gyerekek, szülők, pedagógusok és szociális munkások, döntéshozók oktatása és a program népszerűsítése. Szeretnénk elérni, hogy az országban minél több internethasználó böngészhessen biztonságosabb körülmények között, illetve, hogy probléma esetén az érintettek tudják, kihez fordulhatnak, kitől kaphatnak segítséget. Fontos, hogy a felhasználók tisztában legyenek az internet biztonságos használatának szabályaival, a világháló előnyeivel, lehetőségeivel és veszélyeivel egyaránt.

Netezz biztonságosan! előadásaink ingyenesen megrendelhetők a lenti linken [1].

Ezeket elsősorban diákok, szülők, pedagógusok és szociális munkások számára ajánljuk.

2022-ben 95 magyarországi településen, összesen 358 oktatást tartottak trénereink. Büszkén elmondhatjuk, hogy ezzel csaknem 25.000 főnek nyújtottunk szakmai segítséget a biztonságosabb online jelenléthez, amiből több mint 22.000 gyerek volt.

Az oktatáson kívül konferenciákon, rendezvényeken és kampányokkal is felhívjuk a figyelmet a világháló előnyeire és hátrányaira. Minden év februárjában, a nemzetközi Safer Internet Day eseményeihez kapcsolódva, „Együtt egy jobb internetért” mottóval, Biztonságos Internet Napot rendezünk itthon. Az eseményhez kapcsolódva a témába vágó kreatív pályázatokat is hirdetünk általános és középiskolás diákok számára. A rendezvényen az ország legjobb szakembereitől hallhatnak előadásokat a rokon szakmák képviselői, szülők és pedagógusok. Ezzel párhuzamosan a pályázaton győztes gyerekek és fiatalok interaktív, az internet okos használatához köthető feladatokat oldanak meg.

[1] https://www.saferinternet.hu/legyel-az-internet-asza/oldalsav/oktatasok-megrendelese

Minden ősszel pedig médiakonferenciát tartunk „A média és az internet hatása a gyermekekre és fiatalokra“ címmel, a Magyar Tudományos Akadémián.
Hotline-unkon keresztül a felhasználók bejelenthetik az interneten fellelt káros és illegális tartalmakat, akár névtelenül is, a www.biztonsagosinternet.hu honlapon. A forródrót elsődleges célja, hogy az internetről a lehető legrövidebb idő alatt eltűnjenek azok a káros és jogsértő tartalmak, amelyek veszélyesek lehetnek a gyerekekre, fiatalokra. Ezért az operatív működés - a hatályos jogszabályok alapján - szoros együttműködést kíván a magyar hatóságokkal és az internetszolgáltatókkal, illetve, külföldi illetékesség esetén, a nemzetközi INHOPE szövetség tagjaival.

SHARENTING, AVAGY HOGYAN NE LEGYÜNK TÚLPOSZTOLÓ SZÜLŐK, NAGYSZÜLŐK

SZERZŐ: DR. BARACSI KATALIN LL. M CSALÁDJOGI SZAKJOGÁSZ, LL. M INFOKOMMUNIKÁCIÓS SZAKJOGÁSZ INTERNETJOGÁSZ, KÖZÖSSÉGI MÉDIA TRÉNER

A közösségi média a kezdetektől fogva táptalaja az emberek szereplési vágyának. A 15 másodperces hírnév ma már nem álom többé, hanem mindenki számára elérhető a közösségi média különböző alkalmazásai segítségével.

Sokan életcélként tekintenek a minél több lájkot, követőt hozó digitális hírnévre. De nem mindegy, hogy saját magunkat vagy gyermekünket, unokánkat helyezzük a digitális színpad reflektorfényébe.

Nemcsak a gyerekek, fiatalok számára fontos a tudatos és biztonságos internethasználathoz kapcsolódó ismeretek megszerzése, fejlesztése. A szülő, nagyszülő éppúgy kockázati forrás, amikor a közösségi oldalakat a gyermekeikről, unokáikról készült felvételekkel árasztják el. Ezt a jelenséget hívjuk sharentingnek. A share (megosztani) és a parenting (szülői szerep) angol szavakból ered, azaz, amikor az előbbi két szereplő állandóan képeket, videókat, vicces (vagy szerinte vicces), kihívásokat teljesítő (pl. rángassuk ki az ágyból a még alvó gyermeket és vegyük rá egy közös táncra, ami azonnal megy a TikTokra) felvételeket posztol gyermekéről, unokájáról. A nyilvánosság számára elérhetővé tett anyagok azonban bárki számára hozzáférhetőek és felhasználhatóak, néhány évvel később cyberbullying (internetes bántalmazás) alapja is lehet egy-egy meggondolatlan megosztás. Melyik szülő, nagyszülő szeretne ilyen fájdalmat okozni?

Az ultrahangfelvételektől, az első bilire ültetésig, fürdetős képeken, kisgyerekkori énekes-táncos videókon át a teljes gyerekkor dokumentálható az interneten. Miért kell külön felhívni erre a figyelmet? Mert egy nyilvánosan megosztott felvétel rövid idő alatt a sötét weben landolhat vagy olyan oldalakon, ahol a gyerekek felvételeit szexuális célokra használják fel. Az osztálytársak, barátok megtalálják ezeket és már el is indul a bántás, sértés, megalázás, zaklatás. Ezeket a helyzeteket összefoglaló néven kidshamingnek, azaz a gyerekek szülő általi megalázásának nevezzük. Amikor ez történik az a gyermekjogok súlyos megsértését és akár a kiskorú veszélyeztetése bűncselekmény megvalósulását is jelentheti. Joggal merülhet fel a kérdés, hogy akkor egyáltalán ne osszunk meg semmilyen

tartalmat a gyerekről? Nem a teljes tiltás híve vagyok, hanem a felelős megosztásnak.

Mielőtt kiteszünk, egy tartalmat gondoljuk végig a következőket:

Kérdés: A valóságban kinek mutatnám meg a gyermekemet?
Válasz: Biztosan nem az egész világnak, így ne nyilvános posztban szerepeljenek a róla készült képek, videók.

Kérdés: Örülnék annak, ha rólam a fent leírt felvételek bármelyike napvilágot látna, és mindenki rajtam röhögne és beszólogatna nekem?
Válasz: Biztosan nem, akkor miért teszem ezt a saját gyerekemmel, unokámmal?

Beszéljük meg a gyerekkel a fénykép, videókészítés mikéntjét (miért csináljuk azt, hová tesszük fel és azt ki fogja látni) és csak az engedélyével (mondjon egyértelműen igent) használjuk fel a felvételeket. Ha még nem tud véleményt mondani életkorából adódóan egy-egy ilyen helyzetről, akkor felnőtt fejjel gondoljuk végig azt, hogy az minden szempontból ártatlan vagy épp ellenkezőleg megalázó, nevetség tárgyává tevő, kiszolgáltatott helyzetet bemutató, megalázó felvétele. A gyerek nem lehet a meg nem valósult álmaink beteljesítője, a lájkvadászat eszköze.

A közösségi oldalon tekintsük át az adatvédelmi beállításokat! Gyerekposztok esetében vegyük le a hozzászólás, megosztás lehetőségét. Hozzunk létre zárt csoportokat, ahol tényleg csak azok láthatják a gyerek mindennapjait, akikkel ezt tényleg szeretnék megosztani.

A közelmúltban a gyerekek is hangot adtak annak, hogy milyen magatartást várnak el tőlünk, ha internetes posztolásról van szó.
Figyeljük, óvjuk, segítsük, támogassuk, tanítsuk gyermekeinket az internet biztonságos, értékes és pozitív használatára és közben ne feledkezzünk meg saját tudásunk naprakészen tartásáról sem!

6 ÜZENET A GYERMEKEKTŐL

Kerüld el a **sharenting** generálta konfliktusokat!

KÉRDEZD MEG, HOGY LEFOTÓZHATSZ-E!

Attól, hogy gyerek vagyok, még jogom van eldönteni, hogy szeretnék-e egy képen szerepelni.

FIGYELJ ODA A VÁLASZOMRA!

Ha megkértelek, hogy ne fotózz le, kérlek, ne hagyj figyelmen kívül! Ezzel megbántasz és azt sugallod, hogy a véleményem, kérésem jelentéktelen.

MUTASD MEG A RÓLAM KÉSZÜLT KÉPET, HOGY TETSZIK-E NEKEM!

Ha nem, készíthetünk újat, de ha meg sem mutatod, esélyt sem adsz nekem a döntésre.

MINDIG KÉRJ TŐLEM ENGEDÉLYT, HA OSZTANI KÍVÁNSZ RÓLAM VALAMIT!

Jogom van eldönteni, kivel, mit szeretnék megosztani. Kérlek, tartsd ezt tiszteletben!

TARTSD TISZTELETBEN A MAGÁNÉLETEMET!

A barátaim, a szerelmem, ha öltözöm, ha utazom, stb mind az intimszférám részei.

BELEEGYEZÉSEM NÉLKÜL ÉLETEM SEMMILYEN RÉSZLETÉT NE TEDD KÖZZÉ!

A bizonyítványom, a sikereim, a bukásaim, a kapcsolataim rám tartoznak és nem a nyilvánosságra.

Források: diva-portal.org/smash/get/diva2:1445724/FULLTEXT01.pdf, ELTE Alfa Generáció Labor

SZABÁLYOZÁSI KEZDEMÉNYEZÉSEK A RANSOMWARE KIBERTÁMADÁSOK KEZELÉSÉRE

SZERZŐ: DR. DOMOKOS MÁRTON SZENIOR TANÁCSADÓ|REGIONÁLIS ADATVÉDELMI CSOPORT KOORDINÁTORA, KERESKEDELMI JOG, TMT, ADATVÉDELEM

2023-ban az egyik legtöbbet emlegetett kiberbiztonsági kockázat a „ransomware", vagyis a zsarolóprogramok segítségével elkövetett kibertámadás, amikor a bűnözők titkosítják a megtámadott szervezet által kezelt adatokat, és a titkosítást csak egy meghatározott pénzösszeg (váltságdíj) megfizetése ellenében oldják fel, illetve a váltságdíj elmaradása esetén nyilvánosságra hozzák, vagy továbbértékesítik az adatokat.

A legújabb jelenség a „Ransomware-as-a-Service" megjelenése - a rosszindulatú felhasználók akár előre kifejlesztett „zsarolóprogram-csomagot" is vásárolhatnak az interneten.

A ransomware által felvetett specifikus problémák mind a jogalkotók, mind a kiberbiztosítási piac szereplőinek a figyelmét felkeltették. Ebben a cikkben megvizsgáljuk a legfontosabb szabályozási kezdeményezéseket és a joggyakorlat fejleményeit.

Magas szintű szabályozási kezdeményezések az Amerikai Egyesült Államokban

Az Amerikai Egyesült Államok (USA) kormányzatának frissen kidolgozott Nemzeti Kiberbiztonsági Stratégiája (National Cybersecurity Strategy)[1] átfogó szövetségi és nemzetközi megközelítést javasol a zsarolóvírusok növekvő problémájának kezelésére - várhatóan 2023 folyamán dől el, ez milyen formában valósul meg, és milyen tanulságokkal szolgál más országok számára.

AAz USA kormányzatának másik figyelemreméltó kezdeményezése a nemzetközi zsarolóvírus-ellenes kezdeményezés (International Counter Ransomware Initiative - CRI)[2], melynek célja, hogy az EU, valamint 36 másik ország konkrét együttműködési intézkedéseket dolgozzanak ki a ransomware támadások elterjedése ellen. A CRI öt munkacsoporttal dolgozik: reziliencia (Litvánia és India vezetésével), zavarok elhárítása (Ausztrália vezetésével), jogszabálysértő finanszírozás elleni küzdelem

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/

(Egyesült Királyság és Szingapúr vezetésével), közszféra-magánszektor partnerség (Spanyolország vezetésével) és diplomácia (Németország vezetésével). A CRI keretében kidolgozásra kerülne egy „nyomozói eszköztár" - tanulságok és stratégiák kidolgozása a ransomware támadásokra való reagáláshoz, trendfigyelés, valamint erőforrások biztosítása kapacitásépítéshez. További figyelemreméltó eleme a tervezetnek, hogy közös lépéseket irányoz elő annak megakadályozására, hogy a támadók a kriptovaluta ökoszisztémáját használhassák a kapcsolódó fizetések lebonyolítására. Ide tartozik a bitcoin pénztárcákkal kapcsolatos információk megosztása, valamint pénzmosás elleni/terrorizmus finanszírozása elleni nemzetközi (AML/CFT) szabványok és ügyfélazonosítási (KYC) szabványok kidolgozása és végrehajtása a kriptovaluták használatával kapcsolatban.

Franciaország - kötelezettségek a biztosítási szerződésekkel kapcsolatban

A ransomware által jelentett fenyegetést a kiberbiztosítások feltételei is folyamatosan tükrözik, adott esetben a biztosítási díjak növelésével, valamint a biztosítási események körének finomításával. Úgy tűnik, hogy az ilyen jellegű biztosításokkal kapcsolatban specifikus jogszabályok is meghatározzák majd, milyen kötelezettségei vannak a biztosítóval szerződő feleknek kibertámadások esetén.

A francia biztosítási törvény új, 2023. április 24-én hatályba lépő L12-10-1 cikke új kötelezettségeket vezet be a kibertámadások által érintett felek számára. Azok a szervezetek, akiknek az automatizált nyilvántartási rendszerét kibertámadás érte, csak akkor igényelhetik a biztosításuk alapján járó - a „jogsértésből eredő veszteségek és károk" fedezetére szolgáló - összeg megtérítését, ha a tudomásszerzését követő 72 órán belül jelezték a támadást az illetékes hatóság számára. Az értesítési kötelezettség fő célja egyrészről, hogy felgyorsítsa a nyomozást, megkönnyítse az elkövetők azonosítását, és elkerülje az anyagi veszteséget, másrészről pedig az, hogy az illetékes hatóságok által gyűjtött adatok lehetővé tegyék a kibertámadások jobb megértését. A kötelezettség bármely típusú biztosításra vonatkozik, nem csak a kiberbiztosításokra, és kiegészíti az egyéb, a GDPR és a NIS 2 Irányelv alapján fennálló incidens-bejelentési előírásokat.

A francia jogszabály módosítás alapján bekövetkező változások tanulságosak lehetnek más országok jogalkotói, valamint a biztosítási szektor szereplői számára, a törvényszöveg azonban számos gyakorlati kérdést nyitva hagy.

Az „illetékes hatóság” fogalmát a jogszabály például nem határozza meg részletesen, de a bejelentést feltehetőleg a rendőrség számára kell megtenni. A jogszabályból nem derül ki az sem, hogy milyen formában kell a bejelentést teljesíteni, és hogy a megtámadott szervezeten belül melyik döntéshozó szint tudomásszerzésétől számítandó a 72 órás időablak. Bizonytalan az is, hogy a rendelkezés kifejezetten megtiltja-e a biztosítóknak az alapulfekvő összeg kifizetését, vagy ezt esetről-esetre mérlegelhetik.

A biztosításokkal kapcsolatos bírósági gyakorlat az Amerikai Egyesült Államokban

Érdekes tanulságul szolgál az Emoi Services LLC kontra Owners Insurance Company ügy[3], amelyben az Ohio-i Legfelsőbb Bíróság megállapította, hogy a szoftver olyan immateriális tárgy, amelyet nem érhet közvetlen kár vagy veszteség, ha a felperes nem volt képes hozzáférni vagy használni a szoftvert egy zsarolóvírus-támadás során.

Az Emoi Services számítógépes szoftvercég orvosi alkalmazásokkal kapcsolatos online szolgáltatásokat nyújt egészségügyi szolgáltatóknak. 2019 szeptemberében ransomware támadás indult a társaság ellen,titkosítva annak szoftvereit, és használhatatlanná téve online szolgáltatásait.

Az Emoi körülbelül 35.000 USD váltságdíjat fizetett a visszafejtési kulcsokért cserébe. A visszafejtési folyamatot követően az Emoi rendszereinek és fájljainak többsége visszaállt normál működési állapotába.

A kibertámadás idején az Emoi az Auto-Owners Insurance Group nevű biztosítónál tartott fenn biztosítást. A biztosító szerint a kötvény „elektronikus berendezésekre” vonatkozó rendelkezései nem fedezik a károkat, vagyis az Emoi nem jogosult az általa birtokolt, bérelt vagy ellenőrzött „médiában” bekövetkezett közvetlen kár vagy veszteség megtérítésére, valamint az elvesztett adatok azonosításához és helyreállításához szükséges költségek megtérítésére. Az Ohio-i Legfelsőbb Bíróság egyetértett ezzel az érveléssel - véleménye szerint „a szoftver olyan immateriális tárgy, amely nem szenvedhet közvetlen fizikai veszteséget vagy közvetlen fizikai kárt”.

Figyelemmel az ítélet megállapítására, fontos minden esetben részletesen megvizsgálni a biztosítási feltételeket, hogy megfelelően kiterjednek-e egy ransomware támadás által okozott károkra.

Jogszabályi tiltás a váltságdíj kifizetésére

Az Amerikai Egyesült Államokban a Pénzügyminisztérium Pénzügyi Bűnüldözési Hálózata

[3] https://law.justia.com/cases/ohio/supreme-court-of-ohio/2022/2021-1529.html

(Department of the Treasury's Financial Crimes Enforcement Network - FinCEN) és a Külföldi Vagyonellenőrzési Hivatal (Office of Foreign Assets Control - OFAC) 2020. október 1-jén iránymutatás bocsátottak ki a ransomware támadásokkal kapcsolatos váltságdíjak kifizetésével teljesítésével kapcsolatos lehetséges jogi kockázatokról. Az OFAC szerint az egyik fő kockázat, hogy a kifizetés valamely szankciós listán szereplő személy vagy szervezet javára történik, ezzel pedig a kifizetést teljesítő fél megszegi a szankciót előíró jogszabályt.

Egyes esetekben a váltságdíj kifizetése a „terrorizmus finanszírozása" bűncselekményét is megvalósíthatja. Az Egyesült Királyságban a Nemzeti Kiberbiztonsági Központ (National Cyber Security Centre - NCSC) és az adatvédelmi hatóság (Information Commissioner's Office - ICO) ezért közös nyilatkozatukban[4] rögzítették, hogy nem támogatják a ransomware támadások során a váltságdíj kifizetését. Az Egyesült Királyság gyakorlata szerint ugyanis nem szükséges, hogy az elkövető ténylegesen tudatában legyen annak, hogy a váltságdíj kifizetésével terrorcselekmény elkövetését támogatja - elegendő, ha az elkövető által objektíven ismert információk alapján észszerűen gyanítható, hogy a váltságdíjat terrorcselekmény támogatására használják.

Az USA-ban eddig Észak-Karolina tiltotta meg jogszabályban az állami szerveknek és a helyi önkormányzatoknak, hogy ransomware támadást követően váltságdíjat fizessenek. A jogszabály azt is megtiltja az érintett szerveknek, hogy kommunikáljanak a támadóval, a ransomware támadást pedig jelenteni kell az illetékes hatóságnak (North Carolina Department of Information Technology). A jogszabály elfogadásának indoka az állami szerveket ért ransomware támadások megnövekedett száma: 2022. április 8-án a North Carolina A&T Egyetemet például zsarolóvírus-támadás érte, amely megszakította az iskola vezeték nélküli kapcsolatait, és számos online oktatási eszközt leállított. Észak-Karolina példáját követve a pennsylvaniai szenátus a közelmúltban jóváhagyott egy törvényjavaslatot[5], amely tiltja közpénzek felhasználását váltságdíj kifizetésére, kivéve, ha a kormányzó engedélyezi. New York állam jogszabálytervezete általánosságban tiltaná a váltságdíj kifizetését mind az állami, mind a magánszektorban.[6]

A szervezeteknek érdemes tehát felülvizsgálniuk a hatályos kockázatkezelési és incidenskezelési eljárásaikat, hogy tartalmaznak-e rendelkezéseket a ransomware támadók ellenőrzésére, különös tekintettel a pénzmosás-ellenes és a szankciós szabályoknak való megfelelés, valamint a bűnüldöző szervek és más kormányzati szervek bevonása szempontjából.

[4] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/07/ico-and-ncsc-stand-together-against-ransomware-payments-being-made/
[5] https://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2021&sessInd=0&billBody=S&billTyp=B&billNbr=0726&pn=1326
[6] https://www.nysenate.gov/legislation/bills/2021/s6806

SZABÁLYOZÓI CÉLKERESZTBEN A SÖTÉT MEGOLDÁSOK

SZERZŐ: DR. HORVÁTH ANNA ZSÓFIA LL.M (GÖTTINGEN), A CMS BUDAPEST KERESKEDELMI JOGI CSOPORTJÁNAK ÉS TMT CSOPORTJÁNAK ÜGYVÉDJELÖLTJE, ÉS A GEORG AUGUST UNIVERSITÄT GÖTTINGEN PHD HALLGATÓJA, KORÁBBAN AZ EURÓPAI ADATVÉDELMI BIZTOS HIVATALA TECHNOLÓGIAI ÉS ADATVÉDELMI OSZTÁLYÁNAK MUNKATÁRSA.

"A Google egyik csapata nem tudott dönteni két kék szín között, ezért 41 árnyalatot teszteltek az egyes kék színek közül, hogy kiderüljön, melyik teljesít jobban. Nemrégiben vitát folytattam arról, hogy a szegélynek 3, 4 vagy 5 pixel szélesnek kell-e lennie, és megkértek, hogy bizonyítsam be az érveimet "[1].

A megállapítás Douglas Bowmantól, a Google korábbi vizuális megjelenésért felelős tervezőjétől származik, és hűen tükrözi a tudatos tervezés szerepét az online platformok kialakításában. Jelen cikk célja annak bemutatása, hogy mi áll e tervszerűen kialakított design alkalmazása mögött, mekkora jelentősége van ennek a felhasználói döntések meghozatalában, és milyen eszközök állnak a jogalkotó rendelkezésére ennek szabályozására.

1. A sötét megoldások megjelenése

Az emberi gondolkodás folyamatainak megismerésével foglalkozó kognitív pszichológia képviselői viszonylag korán felismerték, hogy a hétköznapi döntéshozatal során az emberek ahelyett, hogy a döntéseik következményeit és azok valószínűségét részletesen mérlegelnék, jellemzően bizonyos beépített „döntéskönnyítő" mechanizmusokat alkalmaznak [2, 3]. Ezek a mechanizmusok kognitív torzításhoz, egyfajta nem tudatos logikai hibához vezetnek, amely lényege, hogy az egyén adott helyzet tényleges értékelése helyett bizonyos gondolkodási sémák alapján jut el egy döntésre [2]. Az egyik leggyakoribb kognitív torzítás a lehorgonyzási torzítás, mely szerint a döntés meghozatal során általában a témában kapott első információ a legmeghatározóbb, a később kapott információ kisebb súllyal esik latba [3], de ilyen például az ún. egyetlen szempontú döntéshozatal, amely szerint az egyén keres egy szempontot, amely alapján a két választási lehetőség megkülönböztethető, és e szempont alapján dönt (például: a zölddel jelölt opció jó, a piros rossz).

Számos kutatás született annak alátámasztására, hogy a megfelelő megjelenés, és a választási lehetőségek prezentálásának körülményei mérhető hatással vannak a felhasználók választásaira, ez pedig ajtót nyitott olyan, kezdetben offline, majd az internet elterjedésével megjelenő online stratégiáknak, amelyek kifejezetten az egyén döntésének fenti módokon történő befolyásolásán alapulnak, például marketing területen reklámokban, vagy pénzügyi befektetésekkel kapcsolatban [3]. Az Európai Bizottság 2022-ben nyilvánosságra hozott riportja több, 3-4 tagállamot lefedő reprezentatív kutatással támasztotta alá, hogy a digitális környezetben alkalmazott sötét megoldások alkalmasak a felhasználók döntéseinek befolyásolására [4].

2. A sötét megoldások fogalom megalkotása és elhatárolási kérdések

A felhasználókat, fogyasztókat érintő fenti gyakorlatot összefoglaló "dark pattern", később „deceptive pattern”, azaz sötét megoldások kifejezést Harry Brignull UX designer használta először 2010-ben, aki a sötét megoldásokat olyan internetes oldalakon és applikációkban alkalmazott trükkökként írta le, amelyek arra késztetik a felhasználót, hogy akkor is egy bizonyos választás, pl. egy termék megvásárlása, vagy szolgáltatásra való feliratkozás mellett döntsön, ha ez egyébként nem állt kifejezett szándékában.

Ugyan máig ez tekinthető a legelterjedtebb meghatározásnak, ezt követően mind a szakirodalomban [3, 5, 6], mind a jogalkotók részéről több absztrakt definíció született. Az Európai Unióban 2022. október 19-én elfogadott, a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló 2022/2065 rendelet (Digital Services Act, "DSA") 67. preambulumbekezdése szerint a sötét megoldások "olyan gyakorlatok, amelyek akár szándékosan, akár ténylegesen jelentősen torzítják vagy korlátozzák a szolgáltatás igénybe vevőinek azon képességét, hogy önálló és megalapozott döntéseket hozzanak". A méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról szóló adatmegosztási jogszabály („Data Act”) jelenleg jogalkotási fázisban lévő tervezetének meghatározása szerint a sötét megoldások „olyan webszerkesztési technikák, amelyek a fogyasztókat megtévesztő módon számukra hátrányos következményekkel járó, nem kívánt döntések felé terelik”. Az Európai Adatvédelmi Testület ("EDPB") a sötét megoldásokat adatvédelmi szempontból, és kizárólag a közösségi médiaplatformokon megvalósított "megtévesztő tervezési mintákként" definiálja,amelyek olyan, felhasználói felületeket és felhasználói utakat jelentenek,

amelyek „akaratlan és potenciálisan káros döntések meghozatalára sarkallják a felhasználókat, gyakran olyan döntésre, amely a felhasználók érdekeivel ellentétes, ellenben a közösségi médiaplatformok érdekeit szolgálja a felhasználók személyes adatainak kezelésével kapcsolatban” [7].

A fenti meghatározások két közös eleme, hogy a sötét mintázatok (i) a felhasználó számára tudatosan nem érzékelhető befolyásoló tényezők, és (ii) a felhasználókra nézve valamilyen negatív hatást váltanak ki. Attól függően, hogy ez a két jellemző hogyan valósul meg, a sötét megoldások lehetnek az elérhető információt és információáramlást befolyásoló, vagy a felhasználó döntési folyamatát befolyásoló sötétmegoldások. Előbbire tipikus példa a megtévesztő megjelenés vagy tartalom, ahol a dizájn szándékosan egy dologra irányítja a figyelmet, pl. harsányabb színekkel, az elfogadás, vásárlás gomb nagyobb, zöld, továbblépés vagy elutasítás nehezen kivehető, kisebb gomb. Cookie-hozzájárulásnál személyre szabható cookie beállítások megerősítésekor az ’összes elfogadása’ zöld színnel, a ’beállítások elfogadása’ szürke színnel szerepel. Ilyen továbbá a „kosárba csempészés”, ahol a vásárlási folyamat során a webhely egy további terméket ad hozzá (pl. pluszbiztosítás jegyfoglaláskor úgy kerül a kosárba, hogy a „Választ utasbiztosítást?” kérdésre a „nem” helyett a "biztosítás" az alapbeállítás), és a „zsákutca” megoldás, ahol a felhasználó számára feltétlenül szükséges információ nem áll rendelkezésre, pl. hozzáférési jog gyakorlása lehetőségre kattintás a felhasználó profiljához irányít. A felhasználó döntési folyamatát befolyásoló sötét megoldás például az szimmetrikus hozzáférés a felhasználó részéről, például nincs lehetőség valamely, pl. analitikai cookie elutasítására, a korlátozás, amikor bizonyos opciókat teljesen kizárnak a felhasználói felületről: pl. az ÁSZF-re lehet kattintani, de az adatvédelmi tájékoztatóra külön nem, a „pókháló”, amikor a felhasználó könnyen kerül egy helyzetbe, amiből később nehezen jut ki, például prémium feliratkozás, ingyenes néhány hónapos használat, ahol a leiratkozás, illetve az ingyenes próbaidőszak után a lemondás nagyon bonyolult, és a „sürgetés”, amikor a vásárló időnyomás alá kerül, például számláló jelzi az akció végét, vagy a még elérhető termékek számát [8]. A sötét megoldásoknak számos további kategorizálása ismert, például aszerint, hogy általános, bármilyen megjelenésbe ültethető, stratégiaként működő sötét megoldásról van-e szó (például kikényszerített felhasználói cselekedet, valaminek kényszerű elfogadása),vagy olyan, tartalomszenzitív sötét megoldásról,

amely csak bizonyos esetekben alkalmazható (például a rejtett árazás) [9].

3. Szabályozási háttér az Európai Unióban

A sötét megoldások szabályozásának központi eleme, hogy azok alkalmazása egyszerre több szabályozási rendszer által támasztott jogi követelményt is érint [8]. Ilyen, párhuzamosan alkalmazható szabályrendszer a fogyasztóvédelmi jog és az adatvédelmi jog, valamint általában a digitális platformok szabályozását megcélzó e-kereskedelmi szabályok.

3.1 Adatvédelmi szabályozás

A sötét mintázatok személyes adatok kezelésére kifejtett hatása jellemzően abból ered, hogy az érintettek számára rendelkezésre álló választási lehetőség, és a személyes adatok megosztásának tényleges szándéka eltérő [3]. Ezzel is magyarázható a "privacy paradox" jelenség, mely szerint ellentmondások vannak a megadott adatvédelmi preferenciák és a tényleges közzétételi magatartás között, azaz a felhasználók azt állítják, fontos számukra a magánélet védelme, közben egyidejűleg jelentős mennyiségű személyes adatot adnak meg magukról [10].

Adatvédelmi szempontból a 2016/679(EU) általános adatvédelmi rendelet ("GDPR") 5. cikk (1) bekezdésében meghatározott alapelvek az irányadók, amelyeket a GDPR további rendelkezései konkretizálnak. A GDPR 12. cikkében foglalt tájékoztatási kötelezettség megfelelő teljesítését, a GDPR 6. cikk (1) bekezdés a) pontjában meghatározott hozzájárulás jogalap esetén a GDPR 4. cikk 11. pontjában és 7. cikkében foglalt feltételek teljesülését. Kiemelendő e tekintetben a hozzájárulás tájékoztatott és önkéntes, azaz befolyástól mentes volta [7]. Kiemelten csorbítja az önkéntesség feltételének érvényesülését a sürgetés, amely az érintettet korlátozó nyomás alá helyezi [11]. Önmagában, a platformok kialakítását tekintve átfogó jelentőségű a GDPR 25. cikkében foglalt beépített adatvédelem elve, mert erre tekintettel alakítandók ki az érintett és az adatkezelő közötti erőviszonyok, a fogyasztó elvárásai és interakciói [7]. A beépített adatvédelem elve közvetlenül szembeállítható a sötét megoldások alkalmazásával, tekintettel arra, hogy előző célja az érintetti jogok hatékony érvényesülését biztosító adatkezelési rendszer kialakítása, ideértve pl. az adatminimalizáció és a transzparencia követelményeinek érvényesülését, míg utóbbi jellemzően a személyes adatok túlzott mértékű és átláthatatlan kezelésének eszköze. Ez alapján alapjaiban véve jogellenesnek tekinthetők a "design" részeként beépülő sötét megoldások, amennyiben azok lehetőséget nyújtanak az adatkezelőknek arra, hogy megkerüljék a beépített és alapértelmezett

adatvédelem elvét, és a fogyasztókat ösztönözzék az adatvédelemhez való jogaik figyelmen kívül hagyására, és a szükségesnél több személyes adat megadására [8, 12].

Megjegyzendő, hogy az EDPB kifejezetten szűk mozgásteret biztosít a közösségi média üzemeltetőinek azáltal, hogy a tájékoztatott hozzájárulás megadását bármilyen szempontból megnehezítő gyakorlatot megtévesztő mintaként jogellenesnek értékel, pl. túl sok kattintás szükséges az adatkezelési tájékoztató megismeréséhez, vagy ha egy adatkezelő adatkezelési tájékoztatója és elérhető adatfeldolgozási szerződései egymásra mutató linkeket tartalmaznak [7].

3.2. Fogyasztóvédelem

A fogyasztóvédelem célja a sötét megoldások vonatkozásában az elérhető információ különbségéből eredő fogyasztó és vállalkozás közötti eltérő erőviszonyok szabályozása, legyen az akár az elérhető információk aszimmetriája, akár a fogyasztó döntési folyamatának befolyásolása [8].Az észszerűen elvárható módon tájékozott átlagfogyasztó meg nem engedett befolyásolása kérdését az Európai Unió Bírósága több ízben közvetve a sötét megoldások értékelésére is alkalmas ügyben tárgyalta. A C-562/15 ügy szerint a kereskedelmi reklámra vonatkozóan általánosságban figyelembe kell venni a szubjektív érzékelést, hogy „a szokásosan tájékozott, észszerűen figyelmes és körültekintő, átlagos fogyasztó hogyan észleli a szóban forgó reklám tárgyát képező termékeket vagy szolgáltatásokat”. A C-54/17 ítélet pedig konkrétan a rejtett többletköltségeket és előzetes hozzájárulás nélkül nyújtott szolgáltatásokat tárgyalva jogellenesnek minősíti, ha egy távközlési szolgáltató úgy forgalmaz SIM-kártyát, hogy arra előre telepítettek és aktiváltak az internetes böngészéshez vagy az üzenetrögzítőhez hasonló bizonyos szolgáltatásokat, anélkül, hogy előzetesen megfelelően tájékoztatták volna a fogyasztót ezen előzetes telepítésről és aktiválásról, illetve e szolgáltatások költségeiről [8].

Az adatvezérelt termékekkel és szolgáltatásokkal kapcsolatban a Data Act fogyasztóvédelmi oldalról is közelítve mondja ki a 34. preambulumbekezdésében, hogy a digitális interfészeik tervezői nem hagyatkozhatnak sötét megoldásokra.

3.3. Platformszabályozás

A közvetítő szolgáltatásokat nyújtó szolgáltatókra vonatkozó DSA 25. cikke kifejezett kötelezettséget teremt online interfészek tervezésével és kialakításával kapcsolatban. A DSA szerint "online platformot üzemeltető szolgáltatók nem tervezhetik meg, alakíthatják ki vagy üzemeltethetik online interfészeiket oly módon,

amely megtéveszti vagy manipulálja a szolgáltatásaikat igénybe vevőket vagy más módon lényegesen torzítja vagy gyengíti a szolgáltatásaikat igénybe vevők szabad és tájékozott döntéshozatalra való képességét". Ez a rendelkezés tekinthető a GDPR 25. cikkében foglalt beépített adatvédelem elve kiterjesztő alkalmazásának, ugyanis a DSA 67. preambulumbekezdése kimondja, hogy a sötét mintázatok tilalmára vonatkozó rendelkezés alkalmazandó a GDPR hatálya alá nem tartozó gyakorlatokra. Ki kell emelni ugyanakkor, hogy a DSA 25. cikke nem minden közvetítő szolgáltatót érint, csak az online platformokat. A DSA 25. cikk (2) bekezdése emellett meghatározza a tiltott interfész-kialakítások kategóriáit is, melyek i) egyes választási lehetőségek kiemelése a szolgáltatás igénybe vevőjének döntésre való felkérésekor, ii) a szolgáltatás igénybe vevőjének ismételt felkérése valamely választásra olyan kérdésben, amellyel kapcsolatban már döntést hozott, különösen a felhasználói élményt zavaró felugró ablak alkalmazásával, és iii) a szolgáltatás megszüntetésére irányuló eljárásnak az előfizetési eljárásnál nehezebbé tétele. Bár ez a három minta széles körben elterjedt, ez a lista közel sem tekinthető kimerítőnek. . Az, hogy a DSA kifejezetten erre a három mintára összpontosít, azt sugallja, hogy a sötét megoldások tilalmának kezdeti fókusza a manipulatív gyakorlatok viszonylag szűk körére összpontosít majd [13].

A digitális jogalkotási csomag másik pillére, a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról szóló 2022/1925(EU) rendelet (Digital Market Act, "DMA") a kapuőrök, azaz a DMA 2. cikk 1 pontjában és 3. cikkében meghatározott alapvető platformszolgáltatásokat nyújtó vállalkozásokra tekintettel elvi éllel állapítja meg a 70. preambulumbekezdésben, hogy tilos a felhasználói felületet, vagy annak egy részét, funkcióit vagy működési módjait úgy kialakítani, hogy az a felhasználói autonómiát, döntéshozatalt vagy választást aláássa, vagy csorbítsa. Ezáltal a DMA általános kötelezettséget teremt a sötét megoldások elkerülésére, vagy beszüntetésére. A DMA 63. preambulumbekezdése nevesítve tartalmazza a fenti "pókháló" módszer tilalmát, azaz, "a kapuőrök számára nem szabad megengedni, hogy szükségtelenül megnehezítsék vagy bonyolulttá tegyék az üzleti felhasználók és a végfelhasználók számára, hogy leiratkozzanak egy alapvető platformszolgáltatásról. A fiók megszüntetése vagy a leiratkozás nem lehet bonyolultabb, mint a fiók létrehozása vagy az ugyanazon szolgáltatásra való előfizetés". Míg a DMA szabályrendszere a nagy

platformokra kötelező erővel hat, a DMA egyik korlátja, hogy a fenti szabály hatálya a kisebb méretű platformokra nem terjed ki [13].

4. A magyar szabályozás

Uniós tagállamként a fent ismertetett jogszabályok Magyarországon is alkalmazandók. A magyar jogban a fentiek mellett a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. törvény (Fttv.) veendő figyelembe, amely 3. § (1) bekezdése általános elvként mondja ki a tisztességtelen kereskedelmi gyakorlat tilalmát.

Hatósági oldalon is léteznek kifejezetten a sötét megoldások tárgyában született döntések, függetlenül attól, hogy ezekben a sötét megoldás kifejezés nem szerepel. A Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH-3195-11/2022 sz. határozatában a weboldalon elhelyezett cookiekkal kapcsolatos adatkezelést a GDPR 5. cikk (1) bekezdésébe ütközőnek találta, mert a cookiek elhelyezéséhez való hozzájárulás megadására szolgáló felugró ablakban az „OK, tovább” és egy „Adatkezelési tájékoztató” gomb szerepelt. Ez a megoldás a fent leírt az szimmetrikus hozzáférés esete, hiszen a felhasználó egyetlen tényleges lehetősége a hozzájárulás megadása. Többek között sötét megoldásnak is értékelhető kereskedelmi gyakorlat miatt marasztalta el a GVH 2,5 milliárd forintra a Booking.com vállalatot 2018-ban. A GVH álláspontja szerint agresszív és ezért tiltott kereskedelmi gyakorlat az oldalon a szálláshelyek melletti ajánlatoknál megjelenő sürgető, fogyasztót nyomás alá helyező üzenetek és felvillanó jelzések, pl. „ezen az áron már csak egy elérhető szoba maradt”.

5. Zárógondolatok

A gondosan kialakított megjelenés, és a megfelelő kontextusban bemutatott választási lehetőség alkalmas a felhasználók döntési autonómiájának befolyásolására. A sötét megoldások alkalmazására emiatt jelentős motiváció áll fenn a piaci szereplők oldaláról. A jogalkotó és a szabályozó hatóságok oldalán megjelenő tapasztalatok és tendenciák szerint ugyanakkor növekvő szabályozói hajlandóság áll fenn a fogyasztói autonómia erősítése, a felhasználók védelme, nem utolsó sorban a személyes adatok védelme érdekében. Megfigyelhető az adatvédelem, a fogyasztóvédelem és a platformszabályozás konvergálása, egyfajta „digitális jog”, mint olyan önálló jogterület kialakulása, amely az említett jogterületek által szabályozott, online térben is megjelenő magatartásokat fedi le, ideértve a sötét megoldásokat. A sötét megoldások alkalmazása ezért, bár rövidtávon kecsegtetőnek tűnhet, hosszú távon komoly kitettséget is okozhat az

azt alkalmazók számára, többek között azért is, mert könnyen észrevehetők. A sötét megoldások elhagyása az online platformok részéről sok esetben a működésük és megjelenésük teljes átértékelését teszi szükségessé. Kiemelt szerepet kap ennek során az „etikus design”, ahol a felhasználói felület kialakítása túlmutat a vizuális, tervezői elgondolásokon, és egyúttal a jogszabályi megfelelést szolgálja, amely végeredményben a fogyasztói bizalmat erősítve egyre inkább egyfajta márkaépítő hatással is bír.

Források

[1] Bowman, D. (2009). Goodbye, Google 1. rész. elérhető: https://stopdesign.com/archive/2009/03/20/goodbye-google.html, utolsó hozzáférés ideje: 2023. március 23.

[2] Tversky, A. és Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science, 185. évfolyam, 4157. szám, 1124-1131. oldal.

[3] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the ‘privacy paradox’. elérhető: doi, https://doi.org/10.1016/j.copsyc.2019.08.025, utolsó hozzáférés ideje: 2023. március 23.

[4] Európai Bizottság (2022). Viselkedési tanulmány a digitális környezetben alkalmazott tisztességtelen kereskedelmi gyakorlatokról: sötét megoldások és manipulatív mintázatok. elérhető: https://data.europa.eu/doi/10.2838/859030, utolsó hozzáférés ideje: 2023. március23

[5] Narayanan, A. és mtsai (2020). Dark Patterns - Past, Present, and Future - The evolution of tricky user interfaces. ACM Queue, 18. évfolyam, 2. szám.

[6] Bösch, Ch. és mtsai. (2016). Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proceedings on Privacy Enhancing Technologies, 4. szám, 237-254. oldal.

[7] Európai Adatvédelmi Testület (EDPB), (2023). Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, elérhető: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf, utolsó hozzáférés ideje: 2023. március 23.

[8] Domokos, M. és Horváth, A. (2021). Dark patterns - napvilágra kerülő sötét megoldások. elérhető: https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/, utolsó hozzáférés: 2023. március 23.

[9] Gray, C.M. és mtsai (2023). Towards a Preliminary Ontology of Dark Patterns Knowledge. elérhető: doi, https://doi.org/10.1145/3544549.3585676, utolsó hozzáférés: 2023. március 23.

[10] Norberg, P. és mtsai (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, elérhető: doi, https://doi.org/10.1111/j.1745-6606.2006.00070.x, utolsó hozzáférés ideje: 2023. március 23.

[11] Information Commissioner's Office (2019). Consultation: Age Appropriate Design code. elérhető: https://ico.org.uk/media/about-the-ico/consultations/aadc/2616602/act-the-app-association.pdf, utolsó hozzáférés: 2023. március 23.

[12] Európai Adatvédelmi Biztos Hivatala (EDPS), (2019). Legal Design Roundtable, elérhető: https://edps.europa.eu/sites/default/files/publication/19-04-27_dark_patterns_en.pdf, utolsó hozzáférés: 2023. március 23.

[13] King, J, és MacKinnon, E. (2022). Do the DSA and DMA Have What It Takes to Take on Dark Patterns? elérhető: https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/, utolsó hozzáférés: 2023. március 23.

MESTERSÉGES INTELLIGENCIA ÉS AZ ADATVÉDELEM

SZERZŐ: DR. DÓSA IMRE, JOGÁSZ, JOGI INFORMATIKUS,
2004. ÓTA FOGLALKOZIK INTENZÍVEN ADATVÉDELEMMEL

Kifogyhatatlanul népszerű téma napjainkban a mesterséges intelligenciával kapcsolatos gondolatok, vélemények, félelmek közlése. Akit a vita téma tudományos szintű adatvédelmi vetülete érdekel, azok számára az Európai Adatvédelmi Testületnek a mesterséges intelligencia rendelet tervezetével kapcsolatos véleményét tudom ajánlani.

Első közelítésben engem is elért a magyar értelmiség sok évtizedes betegsége: nem magával a jelenséggel, hanem az arról formált véleményekkel találkoztam. Elkezdett hát érdekelni, hiszen régi emlékeket idézett fel. Ezért megkérdeztem ChatGPT-t, mit tud rólam. Azt válaszolta, adatvédelmi okokból nem felelhet ilyen kérdésre. Tehát ez az út járhatatlannak bizonyult, de a válasz biztató.

Ha valaki kedveli a tudományos eredményekre adott spontán társadalmi reakciók történelmi leírásait, akkor sok párhuzamot tud felállítani néhány, napjainkban megszokott technikai találmány fogadtatása és a mai mesterséges intelligencia vélemények között.

Pápai átirat például a az emberi társadalom pusztulását vetítette előre egy tömegpusztító fegyver, a számszeríj feltalálása után, mert úgy tűnt, hogy a fa lombjai között elrejtőzöl és ilyen fegyverrel felszerelt harcos korlátlan számú embert tud megölni. Hasonlóan vészjósló jó volt a múlt század 20-as éveiben megjelent írás, amelyben a telefon elháríthatatlan káros hatására hívták fel a figyelmet: elegendő egy betörőnek odatelefonálni a lakásba, mert ha nem veszi fel senki, akkor szabadon dolgozhat.

Ezekkel a veszélyekkel a társadalom megtanult együtt élni. Azt remélem, hasonlóan tudjuk majd a mesterséges intelligencia előnyös oldalát kihasználni. Ez nem jelenti azt, hogy ennek a technológiának nincsenek veszélyben, de az ember úgy működik, hogy vagy elhárítja vagy felvállalja a kockázatokat. Pontosan úgy, ahogyan az a történelmi példák esetében is történt.

Számomra a mesterséges intelligencia kihívásai közül az emberi racionalitás és az irracionalitás gépi kezelése tűnik a leginkább izgalmasnak.

Racionalitásra optimalizált gépek mit kezdenek majd az emberi viselkedés irracionalitásával? Talán ezt nevezik a hozzáértők a mesterséges intelligencia humanizálásának. Ez vajon kecsegtető vagy ijesztő?

A digitális adattárolás robbanás szerű fejlődésével nem csak akkor növeljük adat-testünket, amikor TikTok videót teszünk közzé, hanem akkor is ha romantikusan andalogva sétálunk egy térfigyelő kamera látószögében. Ezért a technikai lehetőség már most rendelkezésre áll ahhoz, hogy minden eddiginél pontosabb személyiségi, viselkedési profil készüljön mindenkiről. Mit kezd, mid kezdhet ezzel az információs hatalommal a mesterséges intelligencia? Nem tudom.

Számomra meglehetősen egyértelmű, hogy az adatvédelem nem adhat egységes választ a mesterséges intelligencia által felismert kihívásokra. Az orvosi diagnosztikában nem szeretnék visszatérni a „ha fáj akkor pálinka, ha vérzik akkor ragtapasz” népi bölcsességéhez. Azt sem szeretnénk, ha az említett sétálós példában a telefonunk suttogná fülünkbe: „Most csókold meg, mert most ezt várja.”

Mindezek miatt azt remélem, hogy nálam sokkal képzettebb emberek tudják majd megmondani, mely területen mely szabályozás lesz hatékony.

Sem a realitást mellőző kategorikus, szigorú szabályozás (mint amilyen a felvétel készítéshez történő engedélykérés kivételt alig ismerő szabály), sem a gyeplőt a jogalkalmazás lovai k közé Dobó általános fogalmak (mint a „megfelelő”, „Hatékony”) lesznek megfelelőek. Ezért izgalommal várom, mit hoz a jövő.

Lehet, hogy saját szabályozásáról is a mesterséges intelligenciát kellene megkérdezni? Meglepne, ha ez korábban nem merült volna fel. Mindenesetre érdekelne a válasz.

INTERJÚ KELETI ARTHURRAL

A FŐSZERKESZTŐ KÉRDEZ CÍMŰ ROVAT

Keleti Arthur
Kiberbiztonsági szakértő, kibertitok jövőkutató, író, az Informatikai Biztonság Napja (ITBN) és az Önkéntes Kibervédelmi Összefogás (KIBEV) alapítója

ICSA: Milyen kihívásokkal szembesülnek a kibervédelmi szakemberek a metaverzumban?

KA: A válaszhoz messziről indítanék, mert ennél a kérdéskörnél azt szükséges meghatározni, mi is pontosan az a metaverzum. Ez jelenleg egy definíciós probléma, mivel a technológusok hamarabb nevezik el és kezdik hypolni, mint mondjuk a tényleges meghatározások megszületnének rá. De ha úgy tekintünk a metaverzumra, mint a következő internetre, vagy a kibertérnek a következő lépcsőfokára, egy sokkal interaktívabb, emberközpontúbb, az emberrel jobban interakcióba lépő környezet kapunk. Ebbe beleérthetjük a web3-at, ami túlmutat a hagyományos weboldalakon. Mondhatni közelebb áll egy szimulációhoz, mint a két dimenziós dimenziós internet (amit leginkább nagyon olyan technológia korlátok alakítottak ki mint az- jó példa erre az email prokoll-ami, őszintén szólva, egy rémálom). Szóval először is a definíciók, környezetek, normák meghatározása a feladat, majd azt követheti a kihívások felmérése.

ICSA: Az emberközpontúbb, közvetlenebb felület már maga lehet egy nagyobb veszélyforrás?

KA: Ezt kétféle képpen lehet nézni: a mostani webes felületek sem alkalmazkodnak teljesen az emberi normákhoz. Ezekre nincsenek kialakítva 100%-ban emberi normák. Tehát az újdonság amennyi veszélyt behoz, annyi előnye is lehet, sőt akár biztonságosabban lesz használható lesz.

ICSA: Valódi védelmi funkciókat tudnak beépíteni ezekbe a rendszerekbe?

KA: Technológiailag igen- bármibe lehet bármit. De itt is távolabbról közelítenék a válaszhoz. Mivel se normarendszer, se szabály nincs az új technológiákhoz, így azt sem tudjuk hogy ezeket ki vagy mi határozza meg vagy micsoda. Ezért biztos, hogy sokkal nagyobb veszélyek várnak ránk, mivel nem tudunk mihez és nem tudunk mivel igazodni. Sem a jog, sem a társadalomtudományok egyéb területei nem tudják ezeket a helyzeteket kezelni, nincsenek rá írott vagy íratlan szabályok és tapasztalások.

Nem raktuk ki azt a környezetet, amelyben ezeket az esetleges normákat/szabályokat a technológusoknak alkalmazni kellene. Valószínűleg majd a tech cégek ezeket saját maguknak kialakítják- mindenki a sajátját. Etikai normákat ugyan elkezdtek már kitalálni (mit illik, nem illik), de ezek nem reálisan betartrathatóak és betartattathatóak, és ami a legfontosabb- nem szankcionálhatóak. Már az internet normarendszerét leírni szándékozó Netikett is tulajdonképpen elbukott. A jogi terület most is nehezen és lassan dolgozik- az előzővel internetes megoldásokkal is küzd, nem hogy felzárkózzon az újhoz.

Ez a fajta világ behoz olyan új viselkedési elemeket, amikkel eddig nem találkoztunk.

Ezzel kapcsolatosan van egy friss élményem, egy VR környezetben tartott három dimenziós oktatásról. Eltekintve olyan apróságoktól, mint egy falnak masírozó alak az előadás alatt, az előadótól nem messze ült egy kutya. Senki sem tudta, hogy az mi - egy résztvevő, egy kiegészítő elem a térnek, vagy egy robot. Majd az előadás közben odaállt az előadó mellé és bámulta őt. Kínosan egy érdeklődő kérdést tettek fel neki, de válasz nem érkezett, így az eredeti dilemmára - mi ez - nem érkezett válasz. Ez egy teljesen hétköznapi helyzet lesz a VR világban. Ott az a legkisebb probléma, hogy kutya-e vagy ember. A teljesen hétköznapi normarendszerek és protokollok nem alakultak ki, így biztonsági réteg kialakítása szinte lehetetlen - azt akkor tudjuk, ha van alap normatíva -ami itt nincs.

A technológiai fejlődés lehetővé teszi, hogy valódi védelmi funkciókat építsünk be az új rendszerekbe, de ennek létrehozása garantáltan nem egyszerű folyamat. Jelenleg nincs egyértelmű normarendszer vagy szabályrendszer, amely alapján az új technológiákat értelmeznénk és kezelnénk. Ennek következtében az új technológiák veszélyeket rejtenek magukban, mivel nem tudjuk, mire kellene igazodnunk és hogyan kellene kezelni az esetleges problémákat.

A védelmi folyamatokat a tech cégek fogják kitalálni a saját felületeik védelme érdekében. Még bizonyos protokollok is kialakulnak, mint például egy avatár valakinek a sajátja-e, vagy ha ellopják és visszaélnek vele, mi a teendő. Ezekre bizonyosan lesz minden szervezetnek egy saját megoldása.

ICSA: Az AI lehet a védelem kialakításában a szakemberek segítségére?

KA: Az AI kétségtelenül segítséget nyújthat a védelem kialakításában, de azt is figyelembe kell venni, hogy az AI is csak olyan jó, mint amennyi adat áll rendelkezésére. Ha nem áll rendelkezésre elegendő adat az adott rendszerhez, akkor az AI nem fog tudni hatékony védelmi funkciókat kialakítani.

Emellett az AI rendszerek is hibázhatnak, és félreértelmezhetik a felhasználók tevékenységét, ami további biztonsági problémákat okozhat.

ICSA: Ha a tech cégek vállalják fel magukra ezeknek a védelmi rendszereknek és protokolloknak a kialakítását, akkor annak mennyi lehet a realitása, hogy ezt a felhasználók védelmében teszik és nem további adatgyűjtés céljából? Hisz most is ez az alapkoncepció.

KA: A kérdés jogos. Ezekben a kezdeményezésekben kell, hogy legyenek felhasználó védelmi törekvések, ahogyan az Apple most ezt az irányt erősíti. De tény, hogy nagy volumenben ennek a kivitelezése több hibalehetőséggel is jár. De a biztonság igenis eladási pont lett mára, és a hitelesség egyre nagyobb érték.
A Meta fizetős részénél is hamarosan látható lesz, hogy hány embernek ér többet a megbízhatóság és hitelesség, és hogy fizetnek-e érte valóban a felhasználók.
Az értéke biztos, hogy van a hitelességnek, ahogyan a biztonságnak is. A cégek figyelembe fogják venni ezt bizonyos szintig, de kétségtelen, hogy mindig az üzleti érdek fogja vezérelni őket. Éppen ezért fontos, hogy független felügyelettel és szabályozással rendelkező szervezetek figyeljék a cégek tevékenységét és biztosítsák a felhasználók védelmét.

ICSA: A fiatalok jobban ki lesznek téve a veszélyeknek?

KA: Nem gondolom. Van egy elmélet, hogy a gamerek lesznek a fő felhasználók (ebben az esetben nyilván a fiatalok jobban veszélyeztetve lesznek), de van olyan verzió is, hogy a cégek lesznek a fő fogyasztók és ők hozzák meg az igazi áttörést például a a VR szemüvegek világába. Az igazi VR akkor fog megérkezni, amikor top 500 cég elkezdi kiosztani a VR szemüvegeket a dolgozóinak a meetingekre.

ICSA:A fiatalokra visszatérve. Tiltás vagy a tanítás lehet a jó eszköz felkészülni a kibertér újdonságaira?

KA:Amikor a fiatalokról beszélünk, meg kell találnunk azokat az eszközöket, amelyek segítségével felkészülhetnek a kibertér újdonságaira . Én sohasem voltam tiltás párti, a tanítás lehet a jó eszköz. Magam is 9 éves korom óta ülök gép előtt, és nagyon szeretem a technológiát. Ha ez nem lett volna, akkor én ma nem lennék sem kiberbiztonsággal sem kutatásokkal foglalkozó szakember, az biztos. Az sem lehetetlen, hogy egy másik típusú gyerekre, majd felnőttre lesz szükség a kibertérben, amihez meg pont ez a fajta fejlődés és tanulás kell. Nyilván értelmesen és okosan…de szerintem tanítani kell, és nekünk felnőtteknek is tanulni kell, mert gyorsabban és kreatívabban használják a fiatalok a

technológiát és ez arra kényszeríti az idősebb generációt hogy alkalmazkodjon jobban, s ne a szociális hálóba kelljen bíznia, hogy ha nem tudja felvenni a versenyt. Az aktív élethez nekünk is alkalmazkodnia kell a digitális világhoz. Már az nem lesz működő képes, hogy „á én ezt már nem értem, majd foglalkozik vele a következő generáció". Igenis a változás már itt van, és ha nem akarunk akár 40-50 évesen kiesni a körforgásból, akkor alkalmazkodnunk kell a digitális világhoz, és meg kell tanulnunk az új technológiákat

Az a helyzet, hogy most mindenkire rá van bízva hogy ki hogyan áll ehhez a fejlődéshez. Mesterséges intelligencia, robotok, meddig tart az ember. Sem egyházak, sem senki nem foglalt még állást igazán a témában, így mindenki a saját értékrendszere szerint dönti el, mit tart jónak, elfogadhatónak, alkalmazhatónak- és honnantól nem elfogadható egy gép segítsége. Mert online meeting jöhet, beültetett chip nem… bőrömnél van-e a határ, vagy kinek hol van a határ…Mert azért az agyunkban már logikailag már benne van a technológia egy ideje- csak fizikailag nem.

ICSA: Mindez morális szempontból problémás lehet. Ha ennyire ellenőrzés alá vonhatóak vagyunk - hiszen ezekhez a folyamatokhoz rengeteg adatot kell megadni -, akkor az adatvédelemmel és az egyéni szabadsággal kapcsolatos kérdések merülnek fel.

KA: Nehéz téma. Megint messziről közelítenék. Ahhoz is óriási bizalom kell, hogy neked más biológiai lények segítsenek. Támaszkodsz dolgokra, emberekre. Az definíció kérdése (ha kivesszük a bigtechet és „kémkedésüket"- mert így is bonyolult a képlet), hogy van egy technológia és az miben segít téged és valamilyen szinten beleszól az életedbe- akkor az nem is biztos hogy morális kérdés kellene hogy legyen. Azonban fontos, hogy tisztázzuk a technológia és az ember közötti viszonyt, és hogy milyen szinten engedjük meg a technológiának, hogy beleszóljon az életünkbe. A párommal való online kommunikáció és a digitális szívecskék küldése például szintén technológiai közvetítéssel történik, de a morális kérdéseket ezzel kapcsolatban általában nem vetjük fel.

Ami a tech cégek motivációját illeti, nehéz megmondani, hogy ténylegesen a felhasználók védelmében kívánják-e kialakítani ezeket a rendszereket, vagy csak az adatgyűjtés céljából teszik. Mindenesetre fontos lenne, hogy a jogszabályok és a szabályozások elegendő ellenőrzést és felügyeletet biztosítanak ahhoz, hogy az adatgyűjtés

ne sértse az egyének személyes jogait.
Összességében azt lehet mondani, hogy az új technológiák fejlődése nagy kihívásokat jelent a biztonság és a védelem területén. A szabályozóknak és a tech cégeknek egyaránt nagy felelősséggel kell eljárniuk annak érdekében, hogy az új technológiák biztonságosan és hatékonyan használhatóak legyenek, és ne veszélyeztessék az egyének jogait és biztonságát.

ICSA: Nem lehet h az ember csak a kontroll hiányát félti?

KA: Biztos vagyok benne, hogy így van. Az elutasítás helyett azonban érdemes lenne közelebb kerülnünk a gépekhez és a technológiához, hogy igazán megértsük őket és ellenőrzésünk alá vonjuk őket. Úgy gondolom, hogy a technológia elutasítása azonos a fejlődésünk megállításával. Van egy mondás, miszerint tartsd az ellenségeidet közel magadhoz. Ha valamiben nem bízunk, akkor jobban meg kell ismernünk, mert lehet, hogy nem is ellenségünk.
Szerintem ugyanez igaz a technológiára is.
Ha a Chat GPT rosszul válaszol valamit egy IT-snak, akkor már sejti mi romlott el benne s nem szétverni akarja, hanem máshogy megközelíteni. Szerintem ez lehet a megoldás. Teljesen mindegy amúgy, hogy hiszünk-e benne, mehetünk biológiai irányba is, amerre amúgy eddig is mehettünk volna erre. De mi nem telepátiával kommunikálunk- mert úgy nem tudunk, hanem online beszélünk, mert erre van megoldásunk.
Szóval nem a technológiai vállalatok vették el tőlünk az embertől való kommunikációs képességet, mint például a telepátiát, mert ez a képesség sosem volt a miénk. Az online kommunikáció lehetősége azonban fejlődött és vált elérhetővé, így ezt használjuk."

ICSA: Ezek szerint fel kellene a szakembereknek is venni a kesztyűt és megoldási javaslatokat tenni, nem elutasítani és figyelni?

KA: Azt javaslom, hogy a szakemberek ne utasítsák el és ne féljenek megoldási javaslatokat tenni, hanem vegyék fel a kesztyűt és üljenek le kommunikációs szakemberekkel, jogászokkal és társadalomkutatókkal. Sajnos a mai világban a legtöbb ember nem tud kilépni a saját környezetéből, és ez a legnagyobb pofára esés az adatvédelem oldalán is. Az embereknek meg kell érteniük a felhasználói környezetet, ami jelenleg absztrakt és nehezen érthető még a szakértők számára is. A VR lehetőséget nyújthat arra, hogy a felhasználók számára érthetőbbé tegyük az adatvédelmi kérdéseket. Ha az emberek érzékelik az adatszivárgás szagát, akkor ösztönösen reagálnak és cselekednek, ezért fontos, hogy az adatvédelmi koncepciókat olyan módon tervezzük meg, hogy az emberek képesek

legyenek megérteni és reagálni rájuk. A nagy cégek profit és innováció iránti elkötelezettsége hajtja őket arra, hogy foglalkozzanak az adatvédelemmel, és az összeszedett fejlesztési folyamatok és termékek mögött nincsenek előre eltervezett összeesküvés-koncepciók. Ezért fontos, hogy mindenki tegye meg a saját kezdő lökését, és a szakemberek segítsék az embereket megérteni az adatvédelmi kérdéseket.

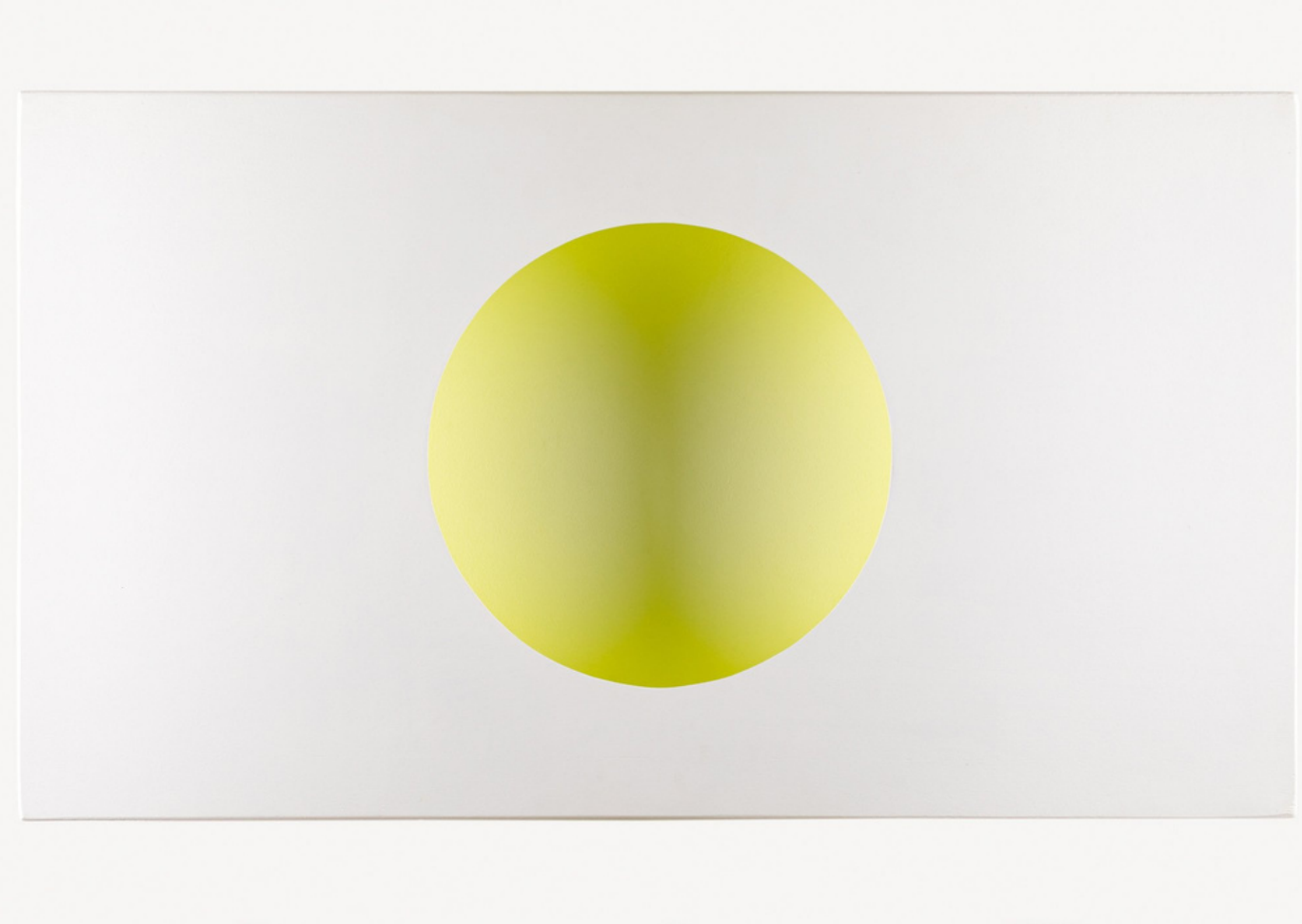
Csak a nagy cégek lépnek ez ügyben- de őket profit és innováció iránti valamiféle elköteleződés hajtja. A multicégek sem olyan összeszedetten és megkomponálva fejlesztik ki ezeket a folyamatokat és termékeket, mint mi feltételezzük- nincsenek előre eltervezett összeesküvés koncepciók. Nem megvalósítható. Egy filmkészítésnél is ahhoz, hogy jelenet úgy álljon össze, mennyi előkészület kell, és mennyi felvétel. Hogy részükről kifejezetten a szolgáltatások a biztonság és magánszféra ellen irányuljanak, az nonszensz, de nem jelenti azt hogy nem használják ki ha adódik egy lehetőség, csak az egész koncepció nem így indul sosem…

Az a kiber világ amit felépítettünk a felhasználók köré az absztrakt, az emberek nem tudják elképzelni, még néha szakértői szemmel sem. Fontos felelősség lenne számukra jobban értelmezhetővé tenni, és ez nem bizonyos biztonsági sorok kántálása.

A felhasználói környezetet tenném megérthetőbbé, s talán a VR erre egy lehetőség lesz. Például, ha adatszivárgás történik egy cégnél, akkor érezhetően büdös lesz a levegő. Ebben az esetben reagálnak (ösztönösen), mert ha büdös van akkor teszünk ellene. Az ember arra tud reagálni, van rá evolúciós képessége. Egy átlagfelhasználót ha szétoktatsz,hogy mit kell csinálni adatszivárgásnál, akkor sem biztos hogy csinálod, míg ha érzed a büdöset, akkor teszel ellene valamit.

ICSA: Többször példálóztál vele, ha online beszélsz a kollégáiddal, akkor megtréfálod őket, hogy vajon valóban veled beszélnek-e. Én honnan tudhatom, hogy ez a beszélgetés igazi volt? Veled történt?

KA: Kérdezd meg ismerőseimet, merre járhattam, és mondtam-e nekik valamit az interjúval kapcsolatban. A hitelesség és az eredet kérdése egyre fontosabbá válik. Nem azt bizonyítjuk, mi a hamisítvány, hanem mi az eredeti. Itt nyilatkoztam, és ezek az emberek tudnak róla, van bizonyítékom. Ez a jövőben egyre fontosabbá és egyre inkább hangsúlyos lesz, és erre már egyre fejlettebb technológiai eszközök állnak rendelkezésre. Ez lesz a jövő.



A kiadvány aktív támogatója a kortárs művészetnek!

No.2. magazin képeinek alkotója: Mátrai Erik

Képek forrása: http://erikmatrai.com

Címlap:Ablak||fa, akril||60x80x12||2015

Belső borító:Naplemente||fa, akril, polisztirol||58 x 87 cm||2014

15.o.: Glória kúp||Installáció,karton,tükrök,lámpák||40x40x40||2010

22.o.: Szpot kapu||fényinstalláció||szpot lámpák, füst||2011

40.o.: Turul||installáció||változó méret||2012

Hátsó borító: Sárga kör||fa, akril, polisztirol||50,2 x 85,7||2014