Nincs új a nap alatt, avagy figyelemmel az eddigi Európai Uniós hatósági gyakorlatra is, választ ad a GDPR a mesterséges intelligencia használata kapcsán felvetődő adatvédelmi kérdésekre?

Tartalomjegyzék

1. Bevezetés, a vizsgálni kívánt kérdés ismertetése

A technológia rendkívüli mértékben felgyorsult fejlődésének ténye aligha megkérdőjelezhető, a mesterséges intelligencia (MI), annak különféle típusainak terjedése megállíthatatlan, a mesterséges intelligencián alapuló szoftverek számos területen egyre inkább a mindennapi életünk részét képezik.

Az MI használata számos esetben személyes adatok kezelésével jár együtt, amelyre tekintettel nem megkerülhető az adatvédelmi kérdések vizsgálata akkor, amikor mesterséges intelligencia használatán alapuló szoftverek tervezésére, megírására és használatára kerül sor.

Jelen szakdolgozat célja annak vizsgálata, hogy milyen hangsúlyos adatvédelmi kérdések vetődnek fel a személyes adatok kezelésével járó mesterséges intelligencia rendszerek megtervezésével, illetőleg használatával kapcsolatban az Európai Unió általános adatvédelmi rendelete (GDPR) szemszögéből, kirajzolódik-e a mesterséges intelligencia kapcsán eddig ismert hatósági gyakorlat alapján, hogy a GDPR megfelelő mértékű szabályozást tartalmaz, amelyre tekintettel adatvédelmi szempontból nincs szükség új szabályok meghozatalára, csupán a meglévő szabályok megfelelő alkalmazására szükséges figyelmet fordítani, avagy van-e, lehet-e jogalkotási teendő ezen a téren.

Figyelembe véve, hogy a mesterséges intelligenciának jelenleg nincs jogszabályban meghatározott definíciója, jelen írás szükségképpen az Európai Bizottságnak a mesterséges intelligencia rendelet megalkotására tett javaslata[1] (Javaslat), illetőleg a Javaslatra az Európai Tanács, majd az Európai Parlament által az MI fogalmára tett javaslata szerinti fogalmából indul ki. A Javaslat szerint a „*„mesterségesintelligencia-rendszer (MI-rendszer)”: olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek;*”[2]. Az Európai Tanács által javasolt fogalom szerint az MI rendszer *„olyan rendszer, amelyet úgy terveztek, hogy autonóm módon működjön, és amely gépi és/vagy ember által szolgáltatott adatok és bemenetek alapján, gépi tanulás és/vagy logika- és tudásalapú*

[1] Javaslat az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról (Brüsszel, 2021.4.21. COM(2021) 206 final 2021/0106 (COD)).

[2] A Javaslat szerinti rendelet 3. cikkének 1. pontja.

megközelítések segítségével következtet arra, hogy adott célokat hogyan lehet elérni, és amely a rendszer által generált kimeneteket, például tartalmat (generatív MI-rendszerek), előrejelzéseket, ajánlásokat vagy döntéseket generál, amelyek befolyásolják azt a környezetet, amellyel az MI-rendszer kölcsönhatásba lép"[3]. Az Európai Parlament által javasolt fogalommeghatározás szerint az MI rendszer *"olyan gépi alapú rendszer, amelyet úgy terveztek, hogy változó szintű autonómiával működjön, és amely meghatározott vagy előre meg nem határozott célok érdekében képes olyan kimenetek, például előrejelzések, ajánlások vagy döntések generálására, amelyek befolyásolják a fizikai vagy virtuális környezetet;"*[4]. A Javaslat szerinti rendelet I. mellékletében felsorolt három technika és megközelítés[5], illetve a fentiek szerint javasolt MI fogalmak elemzésére jelen szakdolgozat nem tesz kísérletet, ehelyett a mesterséges intelligencia javaslatok szerinti rendkívül széles fogalmát veszi irányadónak, amely szerint lényegében minden olyan szoftver mesterséges intelligenciának minősül, amely a beletáplált adatok alapján (akár gépi tanulás segítségével, akár anélkül) valamilyen műveletet végez el, amelynek van egy „kimeneti eredménye", azaz a program a megadott adatok, információk alapján valamilyen következtetés levonására, adott esetben döntés meghozatalára képes, amelyet megismerhetővé tesz az MI használója számára. Érdemes megjegyezni, hogy a Parlament tárgyalási pozícióját tartalmazó módosítási javaslat adatvédelmi szempontból meglátásom szerint nem hoz olyan újdonságot, ami ne következne a GDPR-ból[6].

---

[3] Lásd a Tanács 2022. november 25-én kelt „általános megközelítését". Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach* (https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf) (2023. 08. 27.), 71.o.

[4] Lásd az Európai Parlament tárgyalási pozíciójáról 2023. június 14-én elfogadott dokumentumot, amely a Javaslat szerinti MI rendelet szövegének módosítására tartalmaz többszáz javaslatot. European Parliament, *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))(1)* (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html) (2023. 08. 27.).

[5] Ezek a következők: (i) gépi tanulási megközelítések, (ii) logikai és tudásalapú megközelítések, valamint (iii) a statisztikai megközelítések, Bayes-féle becslés, keresési és optimalizálási módszerek.

[6] A Parlament javaslata hat alapelvet sorol fel, amelyek valamennyi MI rendszer esetében alkalmazandók: (i) az MI-rendszer emberi felügyelete, (ii) műszaki ellenállóképesség és biztonság, (iii) a magánélet tisztelete és adatkezelés megfelelősége, (iv) átláthatóság, (v) sokszínűség, diszkrimináció-mentesség és tisztességesség, (vi) társadalmi és környezeti jólét, továbbá attól függően, hogy milyen típusú MI-ről van szó, írna elő bizonyos

Az írás a GDPR egyes rendelkezéseiből kiindulva, azok eddigi adatvédelmi hatósági gyakorlatát ismertetve közelíti meg a feltett kérdést, azaz, hogy a mesterséges intelligencia használata milyen odafigyelést igényel adatvédelmi szempontból, milyen lényeges kérdések merülnek fel egy ilyen típusú modern technológia alkalmazásával kapcsolatban, figyelemmel többek között a GDPR 25. cikkében szereplő beépített és alapértelmezett adatvédelem elvére és az abból következő kötelezettségekre, valamint az érintetti jogok közül különösen a GDPR 22. cikkére, az abban szereplő „tilalomra”[7], az automatizált döntéshozatallal kapcsolatos követelményekre.

2. A beépített és alapértelmezett adatvédelem elve

Amennyiben személyes adatok kezelésére kerül sor, történjen az akár mesterséges intelligencia használatával, akár anélkül, szükséges a GDPR rendelkezéseinek való megfelelés, így az abban foglaltak szükségképpen irányadóak MI használata esetén is.

2.1 A GDPR 25. cikke

A GDPR 25. cikke (1) bekezdésében szereplő beépített, valamint a 25. cikke (2) bekezdésében szereplő alapértelmezett adatvédelem elve minden adatkezelő számára kötelezettséget ír elő, függetlenül attól, hogy milyen tevékenységet végző adatkezelőről és milyen összetettségű adatkezelésről van szó.

A beépített adatvédelem elve értelmében az adatkezelő köteles már az adatkezelés módjának meghatározásakor, majd pedig az adatkezelés során is megfelelő technikai és szervezési intézkedéseket kialakítani, illetve alkalmazni, amelyek révén megvalósítható az adatkezelésre vonatkozó elveknek és a GDPR előírásainak való megfelelés, valamint az érintettek jogainak hatékony, garanciákkal biztosított védelme. Az adatkezelő mindezt a tudomány és a technológia állása, a megvalósítás költségei, valamint az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a tervezett adatkezelés természetes személyek jogait és

kötelezettségeket (például bizonyos, magas kockázatúnak tekintett MI rendszerek esetében ún. alapjogi hatásvizsgálat végzését, hatósággal való konzultációt, illetve generatív MI rendszerek esetében például a rendszer tanításához használt, a szerzői jog által védett adatok felhasználására vonatkozó nyilvános tájékoztatást).

[7] A GDPR 22. cikkének (1) bekezdésében meghatározott rendelkezés lényegében annak tilalmát tartalmazza, hogy főszabály szerint nem terjedhet ki az érintettre az olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

szabadságait érintő, változó valószínűségű és súlyosságú kockázat figyelembevételével köteles megtenni.

Az alapértelmezett adatvédelem elve alapján minden adatkezelő köteles olyan módon meghatározni és meghozni a megfelelő technikai és szervezési intézkedéseket, hogy kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adatkezelő által meghatározott konkrét adatkezelési cél szempontjából szükségesek. Ez a szükségesség kiterjed többek között a gyűjtött személyes adatok számára és az adatok megőrzésének időtartamára.

Ha egy mondatban kellene meghatározni a 25. cikk lényegét, akkor azt lehetne mondani, hogy az adatkezelő már az adatkezelés megkezdése előtt, azaz az adatkezelés megtervezésekor köteles átgondolni, hogy milyen módon felel meg a tervezett adatkezelés a GDPR-ban foglalt alapelveknek és egyéb, pl. adatbiztonságra vonatkozó előírásainak és a megfelelést folyamatosan, az adatkezelés teljes tartama alatt is hatékony módon fenn kell tartania (adott esetben az adatkezelés egyes jellemzőinek módosítása, kiigazítása révén). Az Európai Adatvédelmi Testület megfogalmazásában: „*Az adatkezelő az adatkezelés előtt és az adatkezelés során folyamatosan megvalósítja a beépített és alapértelmezett adatvédelmet azáltal, hogy rendszeresen felülvizsgálja a választott intézkedések és garanciák hatékonyságát.*”[8]

Azzal, hogy a 25. cikk kifejezetten utal az adatvédelmi alapelvekre, a GDPR 5. cikkében szereplő alapelveket hívja fel, amelyek közül mesterséges intelligencia segítségével történő adatkezelés esetén nem túlzás azt mondani, hogy kiemelt szerep jut a tisztességes eljárás, az átláthatóság, a célhoz kötöttség, az adattakarékosság, valamint a pontosság elvének. (Természetesen a többi alapelvnek is meg kell feleljen az adatkezelés, így a jogszerűség, korlátozott tárolhatóság, integritás és bizalmas jelleg, valamint az elszámoltathatóság elvének.) A GDPR nem tartalmaz előírást arra vonatkozóan, hogy az adatkezelőnek konkrétan milyen intézkedéseket kell tennie, így az adatkezelőknek maguknak kell megfelelő időben megtervezniük és kialakítaniuk a végezni kívánt adatkezelésre vonatkozó azon intézkedéseket, amelyek révén folyamatosan biztosítani tudják a jogszabályi követelményeknek való megfelelést.

[8] Az Európai Adatvédelmi Testület 4/2019. számú iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat (Elfogadás időpontja: 2020. október 20.), 4. o.

A megfelelés megítélésekor kulcsszerepe van a „folyamatos hatékonyságnak”. A 25. cikkben megfogalmazott kötelezettség – egyezően számos más, a GDPR-ban lefektetett kötelezettséggel – nem egy statikus kötelezettség, hanem egy dinamikus, folyamatosan fennálló kívánalom, amelynek való megfelelés érdekében a GDPR eligazítást nyújt abban a tekintetben, hogy az adatkezelőnek milyen szempontokat kell figyelembe vennie[9].

A megfelelő technikai és szervezési intézkedések tekintetében pedig a 25. cikk lényegében felhívja a 24. és a 32. cikket. Előbbi az adatkezelőkre fogalmaz meg kötelezettséget, lényegében a beépített adatvédelem elvét fogalmazza meg némileg másképpen, utóbbi cikk pedig az adatkezelőre és az adatfeldolgozóra egyaránt tartalmaz kötelezettséget az adatok megfelelő biztonságának kialakítása tekintetében.

A kockázatarányos megközelítés hangsúlyos, tekintettel arra, hogy az adott kockázat és annak fennállása vagy fenn nem állása nem egy statikus állapotot jelent, ennek megfelelően a megteendő intézkedések sem lehetnek egyszer és mindenkorra megtettek, hiszen azok éppen a változó kockázatok kezelésére hivatottak. Az adatkezelőnek (és a 32. cikk alapján az adatfeldolgozónak is) ezen kockázatokat, azok valószínűségét és súlyosságát előzetesen fel kell mérnie és ezen elemzés alapján kell megtennie a megfelelő, az adatvédelmi jogszabályoknak való megfelelést biztosító intézkedéseket. Jóllehet az adatvédelmi hatásvizsgálat jelen írásnak külön nem tárgya, érdemes megjegyezni, hogy mesterséges intelligencia használata révén történő adatkezelés esetében különös figyelmet kell fordítani arra, hogy szükséges-e az adatkezelés megkezdését megelőzően adatvédelmi hatásvizsgálatot végezni, amely kérdésre számos esetben igenlő válasz adható a mesterséges intelligencia jelentette technológiai újdonság okán[10], illetve, még ha adott esetben nem is szükséges hatásvizsgálatot végezni, célszerű dokumentálni, hogy mi alapján jutott erre a következtetésre az adatkezelő, illetve érdemes lehet algoritmus tesztelést végezni „próba adatok” betáplálásával, majd figyelni, hogy azok módosítása milyen hatást vált ki az algoritmus működésében.

[9] A tudomány és a technológia állása, a megvalósítás költségei, valamint az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a tervezett adatkezelés természetes személyek jogait és szabadságait érintő, változó valószínűségű és súlyosságú kockázat.

[10] Az adatkezelés sajátosságaitól függően a hatásvizsgálat elvégzésének szükségességére a 25. cikkből is következtethetünk. Jelen írásnak úgyszintén nem tárgya, azonban érdemes röviden megemlíteni azt is, hogy elképzelhető, hogy egy ún. alapjogi hatásvizsgálat is szükséges lesz majd bizonyos, mesterséges intelligencia használatával megvalósuló adatkezelés megkezdését megelőzően a majdan elfogadásra kerülő Mesterséges Intelligencia Rendelet alapján.

A tervezett adatkezelés jelentette kockázatok előzetes megfelelő azonosítása elengedhetetlen, hiszen enélkül nem lesz képes megtenni az adatkezelő (illetve az adatfeldolgozó) a kockázatokhoz igazítandó megfelelő intézkedéseket, amely szükségképpen meg nem felelést fog jelenteni.

A GDPR 25. cikkének való megfelelés olyan szempontból is kiemelt, hogy a GDPR értelmében a bírság kiszabásával kapcsolatos döntés meghozatalakor figyelembe kell venni az adatkezelő, illetve adatfeldolgozó felelősségének mértékét, az általuk a 25. és 32. cikk alapján foganatosított technikai és szervezési intézkedéseket[11].

2.2 A mesterséges intelligencia a 25. cikk szemszögéből

A fent írtak egyfelől ugyanúgy alkalmazandók mesterséges intelligencia használatával megvalósuló adatkezelés esetén, másrészt azok különös súllyal esnek latba akkor, amikor egy szervezet mesterséges intelligencia szoftvert tervez, majd tesztel és használ, tekintettel arra, hogy az MI technológia különösen alkalmas arra, hogy a meglévő kockázatokat súlyosbítsa, új kockázatokat idézzen elő, illetve a meglévő kockázatokat nehezebben kezelhetővé tegye[12].

Az Európai Adatvédelmi Testület iránymutatásában hangsúlyozza, hogy „*[a] beépített és alapértelmezett adatvédelem korai figyelembevétele kulcsfontosságú az elvek érvényesítéséhez és az érintettek jogainak védelméhez. Költség-haszon szempontból továbbá az adatkezelők érdeke is, hogy a beépített és alapértelmezett adatvédelmet minél hamarabb figyelembe vegyék, mivel a már elkészített terveken és a már megtervezett adatkezelési műveleteken a későbbiekben nehéz és költséges lehet változtatásokat eszközölni.*”[13]

Egy mesterséges intelligencián alapuló szoftver alkalmazásának több fő fázisa van, amelyek közül az első a tervezés, amelyet a fejlesztés, a teszthasználat követ, amely után az éles használat, a valós életbeli alkalmazás fázisa következik (amelybe beleértendő a rendszer működésének folyamatos ellenőrzése, felügyelete), végül a szoftver használatának abbahagyásával zárul.

[11] GDPR 83. cikk (2) bekezdés d) pont.

[12] Information Commissioner’s Office, *Guidance of AI and data protection* (https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection-2-0.pdf (2023. 08. 03.), 8. o.).

[13] Az Európai Adatvédelmi Testület 4/2019. számú iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat (Elfogadás időpontja: 2020. október 20.), 36. pont, 11. o.

3. Az egyes GDPR előírások és a mesterséges intelligencia

A GDPR nem tartalmazza a mesterséges intelligencia kifejezést, azonban szabályai minden tevékenységre vonatkoznak, amely során személyes adatok kezelését végzik.

Jóllehet MI-alapú technológia GDPR-ral való összehangolásakor jellemző nehézség az átláthatóság[14], a célhoz kötöttség, az adatminimalizálás és a pontosság elvének való megfelelés, a megfelelő tájékoztatás, valamint az érintetti jogok biztosítása, azt azonban minden bizonnyal túlzás lenne kijelenteni, hogy a GDPR lehetetlenné tenné az MI alkalmazását, inkább úgy lehetne fogalmazni, hogy időigényesebb és költségesebb egy MI modellt úgy működtetni, hogy az megfeleljen a követelményeknek[15].

Gyakran hangzik el, hogy a GDPR előírásai sokszor nem konkrétan megfoghatók, nem adnak kellő útmutatást az adatkezelést tervezők, végzők számára. A GDPR valóban tartalmaz „semleges" rendelkezéseket (pl. „megfelelő technikai és szervezési intézkedések" megtételét írja elő), amelyek alkalmazása megköveteli az egymással versengő érdekek mérlegelését és az MI esetében a kérdéseket a technológia újdonsága, összetettsége és az egyénre gyakorolt hatásainak mértéke még inkább hangsúlyossá teszi[16]. Ugyanakkor nem elvárás a kockázatokkal szembeni „zéró tolerancia", hiszen abban az esetben nem lehetne adatot kezelni, a hangsúly a megfelelő egyensúly kialakításán van[17]. Az alábbiakban azokat a főbb érintkezési („ütközési") pontokat említem meg az alapelvek, jogalapok és érintetti jogok viszonylatában, amelyek különös hangsúllyal vetődnek fel MI-alapú adatkezelés esetén.

[14] Alan Turing már az 1950-es években úgy fogalmazott, hogy egy tanulni képes gép olyan módon fogja elérni a céljait, amit alkotói és tanítói nem látnak előre, bizonyos esetben anélkül, hogy ismernék a gép belső működésének részleteit. Ez az ún. „black-box" jelenség bizonyos MI modellek sajátja.

[15] Álláspontom szerint helyes a Mesterséges Intelligencia Rendelet javaslatában található azon megközelítés (amelyet az Európai Tanács és az Európai Parlament is oszt), hogy egyes MI-alapú adatkezelések eleve tiltottak legyenek, azok rendkívül invazív voltára tekintettel, míg más MI-alapú adatkezelések magas kockázatú adatkezelésekként speciális további feltételeknek feleljenek meg, ezen adatkezelések azonban nem képezik jelen írás tárgyát.

[16] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530 – June 2020, Executive summary, III. o.

[17] Information Commissioner's Office, op. cit., 13. o.

3.1 Az alapelvek és az MI

3.1.1 Átláthatóság és tisztességes eljárás

Ezen elvek jelentik egyfelől azt, hogy tömör és érthető tájékoztatást kell nyújtani az érintettek részére[18], másrészt azt, hogy ha például profilalkotást végeznek, akkor az adatkezelő a profilalkotáshoz olyan technikai és szervezési intézkedéseket (beleértve matematikai és statisztikai eljárásokat) alkalmazzon, amelyek révén biztosított az adatok pontatlanságát okozó tényezők kijavítása és a hibák minimálisra csökkentése. Úgyszintén, az adatkezelő köteles figyelembe venni az érintett jogaira kockázatot jelentő tényezőket és gondoskodni arról, hogy ne legyen diszkriminatív az adatkezelés[19]. Mindez különös éllel vetődik fel automatizált döntéshozatal esetén.

Ezen alapelvek jegyében tekintettel kell lenni arra is, hogy fennáll-e az „újraazonosítás" lehetősége, az, hogy a technológia fejlődése vagy akár az adatkezelés körülményei okán (pl. gépi tanulás) utólag egy adott személy azonosíthatóvá válik annak ellenére, hogy eredetileg alkalmaztak pl. álnevesítést.

Az átláthatóság biztosítása komoly kihívást jelenthet különösen gépi tanulás esetében[20], ha adott esetben a szoftver írója sem tudja (még a legjobb szándék mellett sem), hogy a gép pontosan miért az adott következtetésre jut. Ilyen esetben kérdéses az adott technológia alkalmazhatósága, hiszen, ha maga a készítő sem tudja, hogy hogyan működik a modell, akkor más, így az érintett sem fogja tudni, sem érteni.

Ha közvetlenül az érintettektől gyűjtik az adatokat, akkor a tájékoztatást az adatok gyűjtésekor, a modell tanítása előtt, illetve a modell alkalmazása előtt meg kell adni az érintettek részére, míg, ha az adatokat nem az érintettől gyűjtik, akkor észszerű időn, de legkésőbb egy hónapon belül kell megadni az információt, vagy korábban, ha és amikor felveszik a kapcsolatot az érintettel, vagy amikor az adatokat másnak átadják.

Kérdés lehet a GDPR 14. cikk (5) bekezdés b) pontja alkalmazhatósága, amely szerint nem szükséges megadni a tájékoztatást abban az esetben, ha „*a szóban forgó információk*

[18] GDPR (58) Preambulumbekezdés.

[19] GDPR (71) Preambulumbekezdés.

[20] Az Egyesült Királyság adatvédelmi biztosi hivatala, az Information Commissioner's Office is hangsúlyozza, hogy adott esetben jelentős kihívást jelent érthető magyarázatot adni az MI működéséről. Lásd Information Commissioner's Office, op. cit., 7. o.

rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen… tudományos… kutatási… vagy statisztikai célból, a 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében….” A GDPR azonban ilyen esetben is megköveteli, hogy az adatkezelő megfelelő intézkedéseket hozzon az érintett jogainak védelme érdekében.

3.1.2 Célhoz kötöttség

Az MI modellek egyik jellemzője, hogy lehetővé teszik az eredeti célból gyűjtött adatok másik célra történő felhasználását. Például, a vélemény kifejezésére szolgáló "Like" gomb használata alapján pszichológiai jellemzőkre, politikai véleményre, fogyasztói szokásokra vonatkozó következtetések vonhatók le.

A GDPR előírja, hogy az eredeti célokkal össze nem egyeztethető módon nem kezelhetők az adatok, hozzátéve, hogy nem minősül az eredeti céllal össze nem egyeztethetőnek a például tudományos kutatási vagy statisztikai célból történő további adatkezelés (amennyiben az megfelel a 89. cikk (1) bekezdésének)[21]. A jogszabály orientál továbbá a tekintetben, hogy amikor nem az érintett hozzájárulásán vagy uniós vagy tagállami jogon alapul az adatkezelés, akkor milyen szempontok segíthetnek annak eldöntésében, hogy az új cél összeegyeztethető-e az eredeti céllal[22]. Kérdés, hogy MI használat során mit lehet az eredeti céllal összeegyeztethetőnek tekinteni.

Például abban az esetben, ha egy MI modellt arra képeznek ki, hogy a betáplált egészségügyi adatok alapján bizonyos egészségügyi kockázatokat előre jelezzen a résztvevő érintettek felé, akkor aligha valószínű, hogy az érintett ne kifogásolhatná azt joggal, ha az adatbázist majd arra is használnák, hogy a betáplált egészségügyi adatok alapján az érintetteknek azon adatokból levont következtetések alapján adjanak biztosítási díjra ajánlatot. Előbbi használat egyértelműen lehet pozitív az érintettre, hiszen lehetséges, hogy időben felfedeznek egy betegségre való hajlamot, utóbbi azonban lehet rendkívül hátrányos és diszkriminatív az érintettre nézve.

Az eredeti céltól eltérő adatkezelés kérdése gyakran előjön például nagy adathalmazok tekintetében, ahol adott esetben újabb és újabb összefüggések tárhatók fel adatelemzés révén. Kérdés, hogy hol húzódik a határ az eredeti céllal összeegyeztethető és össze nem egyeztethető

[21] GDPR 5. cikk (1) bekezdés b) pont.

[22] GDPR 6. cikk (4) bekezdés.

adatkezelések között. Ez természetesen az adott konkrét eset elemzését igényli, azonban a GDPR kimondja, hogy az adatkezelés eredeti céljával összeegyeztethető adatkezelés esetében „*nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését*”[23].

Abban az esetben, ha például az eredeti céltól eltérően statisztikai célokra használják egy modell algoritmusának tanítására használt és egyébként álnevesített vagy titkosított adatokat, akkor az összeegyeztethető lehet az eredeti céllal. Amennyiben azonban ugyanezen adatokat egy személy profilozására használnák fel, az már túlmehet az összeegyeztethetőség határán[24].

3.1.3 Adattakarékosság

Nyilvánvalónak tűnő ellentét feszül az adattakarékosság elve és különösen a big data mesterséges intelligenciával történő feldolgozása között, hiszen utóbbi alapvetően éppen abban „érdekelt”, hogy minél több adathoz jusson hozzá annak érdekében, hogy azokból következtetéseket, mintázatokat tudjon leírni (és adott esetben azokból tanulni).

Ehelyütt fontos megemlíteni, hogy a „minél több adat” semmiképpen sem vehető szó szerint, hiszen abban az MI modell sem érdekelt, hogy minél több, a modell célja szempontjából irreleváns (és/vagy pontatlan) adatot is begyűjtsön, hiszen az a modell megbízhatóságát, így használhatóságát ásná alá. Alapvető, hogy az adatok az adott cél szempontjából relevánsak és reprezentatívak legyenek, ellenkező esetben bizonyos, hogy a modell működése nem lesz megfelelő és komoly torzításokkal, diszkriminatív működéssel kell számolni.

3.1.4 Pontosság

Az MI-alapú algoritmusok csakis annyira tudnak jók lenni, amennyire a tanításukhoz használt adatok azok, így a jó minőségű adatok alapvetően fontosak a minőségi algoritmusokhoz[25]. Fontos, hogy már az MI modell tanításakor biztosított legyen az, hogy a betáplált adatok

[23] GDPR (50) Preambulumbekezdés.

[24] Külön kérdésként vetődik fel a különleges adatok kezelése, főleg, ha nem különleges adatokból von le olyan következtetést az MI, ami már különleges adatnak minősül, így például a vásárlási szokásokból, „lájkolt” tartalmak elemzéséből következtet az algoritmus pszichológiai/egészségügyi jellemzőkre, szexuális orientációra, politikai véleményre, amelyek alapján a tudtán kívül megpróbálhatják befolyásolni az illetőt (például bizonyos termékeket próbálnak meg értékesíteni részére) vagy hátrányos megkülönböztetés érheti az adott személyt.

[25] A *„garbage-in, garbage-out”* elve. European Union Agency for Fundamental Rights, *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, 2019 (https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (2023. 07. 31.), 1. o.).

pontosak legyenek, ami különösen igaz akkor, ha az adatokat arra használják, hogy az érintettre nézve következtetéseket vonjanak le vagy rá nézve döntéseket hozzanak. A pontatlan adatok önmagukban sérelmet okozhatnak az érintettnek, ha például olyan módon kezelik, amely nem felel meg a jellemzőinek. Ezzel együtt biztosítandó a kimeneti adatok pontossága olyan módon, hogy az pontos bemeneti adatokon alapuljon és a modell megfelelően végezze a számításokat egy „jól súlyozott" algoritmus alapján. Megjegyzendő azonban, hogy a pontosság elvének való megfelelés nem jelenti egyben azt is, hogy a modellnek statisztikai értelemben 100%-os pontosságúnak kell lennie[26]. Egyes modelleket bizonyos valószínűségek (pl. betegségre való hajlam, fizetéssel való késedelembe esés) előrejelzésére használnak, így eleve nem arról van szó, hogy a gép kimeneti adata (az előrejelzés) bizonyosan pontos (a tájékoztatóban ezt a tényt is jelezni kell).

Ha egy MI rendszert arra használnak, hogy következtetéseket vonjanak le egyénekről, akkor biztosítani kell, hogy a rendszer a célhoz mérten statisztikai szempontból kellően pontos. Ez nem jelenti azt, hogy minden következtetésnek helytállónak kell lennie, de tekintetbe kell venni annak lehetőségét, hogy a következtetések tévesek, és azt, hogy ez milyen hatással lehet a következtetés alapján meghozott döntésre. Ennek hiánya azt jelentheti, hogy sérül a tisztességes eljárás, illetve a pontosság és az adattakarékosság elve (utóbbi azért, mert téves személyes adat a cél szempontjából nem lehet megfelelő és releváns).

Lényeges a téves értékelések (téves pozitív, téves negatív) kezelése. Például egy önéletrajzok előszűrésére használt program esetében abban az esetben, ha a rendszer olyan személyeket javasol meghívni interjúra, aki nem felel meg a keresett munkavállaló jellemzőinek, akkor felesleges energia és idő megy veszendőbe, míg, ha a rendszer olyat nem javasol meghívni interjúra, aki ideális jelölt lenne, akkor a munkáltató és az érintett is elveszíthet egy lehetőséget.[27]

3.1.5 Korlátozott tárolhatóság

Az alapelvvel kapcsolatban érdemes megjegyezni, hogy a személyes adatok szükségesnél hosszabb ideig történő tárolása abban az esetben megengedett, ha a személyes adatok kezelésére például tudományos kutatási vagy statisztikai célból kerül sor (a 89. cikk (1)

[26] Information Commissioner's Office, op. cit., 39 o.

[27] Information Commissioner's Office, op. cit., 41. o.

bekezdésének megfelelően és feltéve, hogy az érintettek jogai érdekében megteszik a megfelelő biztonsági intézkedéseket).

3.2 A jogalapok és az MI

A jogalap pontos meghatározása érdekében fontos az adatkezelési cél megjelölése. Egy gépi tanulásos modell esetében meg kell különböztetni a fejlesztési-tervezési-tanítási fázist a modell alkalmazásának fázisától[28]. Önmagában a modell tanítása nem feltétlen jár közvetlen következménnyel az érintettre nézve, közvetlen következményekkel inkább a modell érintettre való alkalmazásakor kell számolni.

A jogalapok közül MI használata esetében leginkább az érintett hozzájárulása, illetve az adatkezelő jogos érdeke jöhet szóba[29]. Előbbi nehézségét adja, hogy nem könnyű teljesíteni annak összes feltételét, továbbá sok érintett esetében nehézkes annak beszerzése, ráadásul az érintett bármikor feltétel nélkül visszavonhatja a hozzájárulást, amely eshetőséget az adatkezelőnek célszerű előre számba vennie.

A jogos érdek tekintetében is el kell határolni azt, amikor egy algoritmus tanítására gyűjtenek adatot attól, amikor egy algoritmust már élesben használnak és az adat egy „bemeneti jel", amit a modell az algoritmus (illetve a tanultak alapján) feldolgoz és ad rá egy választ. Előbbi esetben kézenfekvőbbnek tűnik a jogos érdek alkalmazhatósága, feltéve többek között, hogy van egy legitim adatkezelési cél és megteszik a szükséges biztonsági intézkedéseket (pl. álnevesítés, titkosítás). Utóbbi esetben komolyabb vizsgálat tárgya az, hogy használható-e az adatkezelő jogos érdeke vagy esetleg az érintett hozzájárulása lehet inkább a jogalap vagy adott esetben az sem.

Bár a jogos érdek az adatkezelés legrugalmasabb jogalapja, nem mindig a legmegfelelőbb. Abban az esetben például, ha a személyes adatoknak olyan a felhasználási módja, amelyre az

[28] Például egy arcfelismerő szoftvert fejlesztenek, amit később különféle célokra lehet használni (például hitelesítés, barátok bejelölése a neten).

[29] A GDPR 6. cikk (1) bekezdés b) pontja a modell érintettre alkalmazása esetén lehet inkább jogalap (a modell tanítása esetén kevésbé), azonban akkor is csak abban az esetben, ha az adott szolgáltatás nem nyújtható kisebb beavatkozással járó adatkezelés mellett és az adatkezelés objektíve szükséges például az érintettel kötött szerződés teljesítéséhez. A GDPR 6. cikk (1) bekezdés c), d) és e) pontjai szerinti jogalapok használata önmagában nem kizárt, ám jellemzően kevéssé valószínű. A d) pont szerinti jogalapok pedig egy MI modell tanítása esetére lényegében kizárhatók, egyidejűleg az MI modell érintettre alkalmazása tekintetében esetleg valamilyen orvosi célú használat esetében lehetne átgondolni a d) pont használhatóságát.

érintett nem számít vagy az szükségtelen sérelmet okozhat az érintettnek, akkor nem ez lehet a megfelelő jogalap. A jogos érdek használata egyben azt is jelenti, hogy az adatkezelő egyfajta plusz felelősséget vállal az érintettek jogainak védelméért és köteles igazolni az adatkezelés szükségességét és arányosságát[30].

3.3 Az érintetti jogok és az MI

A GDPR az 1. cikkében deklarálja, hogy „*a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi*".

A GDPR fókuszában az érintett, az ő védelme áll, minden egyes rendelkezés ezt a védelmi célt szolgálja, így az érintett jogai szoros összefüggésben vannak többek között az alapelvekkel, beleértve a 25. cikkben foglaltak előírásokat is.

Alább röviden felvetem az MI és egyes érintetti jogok kapcsán felmerülő kérdést, a hangsúlyt azonban a 22. cikk szerinti „jogra" helyezem, amelyről a 4.1 és 4.2 pontokban ismertetett jogeset is szól.

3.3.1 Hozzáférési jog

A hozzáférési jog kapcsán felvetődik többek között az a kérdés, hogy mások jogai mennyiben képezhetik gátját ezen jog gyakorlásának, így például az MI modell fejlesztőjének szerzői jogára hivatkozással meg lehet-e tagadni a tájékoztatás megadását. A GDPR szerint a hozzáférési jog *„nem érintheti hátrányosan mások jogait és szabadságait, beleértve az üzleti titkokat vagy a szellemi tulajdont, és különösen a szoftverek védelmét biztosító szerzői jogokat*", ugyanakkor az is egyértelmű, hogy ezen az alapon nem lehet minden információt megtagadni az érintettől[31].

3.3.2 Helyesbítéshez való jog

Ezen jog teljesítése egy MI modell tanításához használt adat tekintetében érdemben jellemzően nem érinti a modell működését, ugyanakkor kérdés, hogy technikailag megvalósítható-e. A modell érintettre nézve történő alkalmazása során keletkező személyes adatok tekintetében

[30] Ennek igazolására szolgál az érdekmérlegelési teszt, illetve adott esetben az adatvédelmi hatásvizsgálat. Amennyiben az MI fejlesztési-tanítási fázisában el is készül egy ilyen dokumentum, azt felül kell vizsgálni ahogyan és amikor az adatkezelési célok konkrétabbak lesznek, kiegészülnek, illetve ilyen esetben más jogalap lehet szükséges.

[31] GDPR (63) Preambulumbekezdés.

kevésbé vetődhet fel, hogy technikailag nem valósítható meg, hozzátéve, hogy mind a tanítási folyamat, mind az MI alkalmazása során biztosítandó a helyesbítéshez való jog.

3.3.3 Törléshez való jog

A törlési jog tekintetében érdekes kérdés, hogy ha egy MI modellből törölni kell a tanításra használt begyűjtött adatot, akkor csak ezen adat törlendő, vagy az is, amelyet a tanításra használt adatból következtetett ki az algoritmus. Kérdés az is, hogy ha csak a begyűjtött adat törlendő, akkor milyen hatással lehet/lesz a törlés a modell működésére.

Adott esetben vizsgálandó lehet a 17. cikk (3) bekezdés b) pontjában foglalt feltételek fennállása, amely szerint nem szükséges törölni az adatot, ha például tudományos kutatási vagy statisztikai célból került sor az adatkezelésre (a 89. cikk (1) bekezdésével összhangban), amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelést. Tekintettel arra, hogy egy-egy adat törlése önmagában egy nagyobb adatbázis működésére minden bizonnyal nincs különösebb kihatással, ezen rendelkezés eredményes hivatkozhatósága minden bizonnyal kérdéses.

3.3.4 Adathordozhatósághoz való jog

Az adathordozhatósághoz való jog az érintettől begyűjtött (az MI tanítására használt) adatokra terjed ki, ha az adatkezelés az érintett hozzájárulásán vagy a 6. cikk (1) bekezdés b) pontján alapul (az adatkezelés MI esetében értelemszerűen gépi módon történik), a kapott adatokból kikövetkeztetett kimeneti adatokra nem.

3.3.5 Tiltakozáshoz való jog

A tiltakozási jog kapcsán érdemes megemlíteni, hogy az megilleti az érintettet többek között a jogos érdeken alapuló és közvetlen üzletszerzési célú adatkezelés esetén, illetve, ha az adatkezelésre például magáncélú tudományos kutatási vagy statisztikai célból kerül sor. Az adatkezelőnek gondoskodnia kell ezen jog biztosításáról is, amely jogos érdeken alapuló, illetve direkt marketinghez kapcsolódó profilalkotás esetén is fennáll.

3.4 Az automatizált döntéshozatal és az MI

Az MI tekintetében kiemelt figyelmet kap a GDPR 22. cikke, hiszen egyes MI modelleket kizárólag automatizált döntéshozatalra használnak. Azontúl, hogy az ilyen adatkezelés

főszabály szerint tilos[32], ilyen automatizált döntéshozatal esetében az adatkezelő tájékoztatást kell adjon az alkalmazott logikáról[33], az adatkezelés jelentőségéről és az érintettre várható következményeiről[34]. Úgyszintén, amennyiben az automatizált döntéshozatal az érintett kifejezett hozzájárulásán alapul vagy az adatkezelő és az érintett közötti szerződés megkötése vagy teljesítése érdekében szükséges, az adatkezelő köteles megfelelő biztonsági intézkedéseket tenni az érintetti jogok védelme végett, és biztosítani legalább azt, hogy az érintett emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be[35]. Megjegyzendő, hogy a (71) Preambulumbekezdés a megfelelő garanciák között még további két tényezőt is említ, nevezetesen, az érintett külön tájékoztatását és azt, hogy magyarázatot kapjon az ilyen értékelés alapján hozott döntésről. A külön tájékoztatás előírása nem feltétlen érthető, tekintettel arra, hogy az 13. és 14. cikkek azt eleve tartalmazzák, azonban kérdés, hogy a magyarázat nyújtása minden esetben kötelező-e (a 22. cikk (3) bekezdésében szereplő „legalább" szó akár erre is utalhat, azonban az sem zárható ki, hogy csak kvázi ajánlás jellege van és a körülmények által indokolt esetben célszerű magyarázatot adni). Álláspontom szerint a jobb átláthatóság biztosítása végett célszerű megadni a magyarázatot, akkor is, ha a 22. cikk ilyen előírást nem tartalmaz.

Profilozás, illetve automatizált döntéshozatal esetén kiemelt jelentősége van a diszkrimináció mentesség biztosításának és ezért is fontos lehet, hogy MI-alapú automatizált döntéshozatal esetén legyen érdemi emberi felülvizsgálat beépítve a rendszerbe és folyamatosan ellenőrzött legyen a modell működése. Például, ha egy bank egy személy hitelképességét minősítő szoftvert használ és a működése során világossá válik, hogy az algoritmus a női hitelkérelmezőkhöz valamiért következetesen alacsonyabb pontszámot rendel, akkor a szoftver diszkriminál (pl. azért, mert jóval kevesebb adatot adtak meg nőkről és az algoritmus nem megfelelően súlyoz vagy a nők esetében olyan előítéletet alkalmaz, hogy ők többször esnek fizetési késedelembe)[36]. Ilyen esetben javítani kell az adatbevitel minőségén, arányán, illetve az adatok, a tanítás folyamatának és/vagy a modell módosításával kell biztosítani, hogy az algoritmus ne előítéletek alapján dolgozzon.

[32] GDPR 22. cikk (1) bekezdés.

[33] Lényeges, hogy ne szakembereknek, hanem az átlagember számára érthető legyen a magyarázat.

[34] GDPR 13. cikk (2) bekezdés f) pontja és 14. cikk (2) bekezdés g) pontja.

[35] GDPR 22. cikk (3) bekezdés.

[36] Information Commissioner's Office, op. cit., 54-55. o.

Arra vonatkozóan is intézkedéseket kell tenni (belső szabályzatok és oktatás révén), hogy emberi döntést támogató MI használata esetében ne forduljon elő az, hogy a gépet felügyelni hivatott, döntési pozícióban lévő személy fenntartás nélkül elfogadja a gép javaslatát, hiszen ilyen esetben nincs érdemi emberi elem a döntéshozatalban és éppen azt a kockázatot nem sikerül kiküszöbölni, ami a gép esetleges hibás működéséből adódik, így végső soron egy teljesen automatizált döntéshozatalról van szó, amely esetben alkalmazandó a 22. cikk.

Az alábbi 4. pontban két jogesetben foglalkozom röviden az automatizált döntéshozatallal kapcsolatban ott felmerült kérdésekkel.

3.5 A statisztikai és tudományos célú adatkezelés

A GDPR (162) Preambulumbekezdése szerint statisztikai célú adatkezelés a személyes adatok statisztikai eredmények kiszámításának céljából történő gyűjtése és kezelése, amely eredményeket a későbbiekben többféle célra is fel lehet használni, többek között tudományos kutatás céljára is, egyben az eredményt nem használhatják fel konkrét természetes személyekre vonatkozó intézkedések vagy döntések alátámasztására. A 89. cikk (2) bekezdés pedig felhatalmazza a tagállamokat arra, hogy garanciák mentén eltérést állapítsanak meg a 15., 16., 18. és 21. cikkben említett jogokat illetően, ha e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják az adott célok elérését, és azok megvalósításához szükség van ilyen eltérésre.

Erre való tekintettel a lehetőség adott arra, hogy például az MI modell tanításához begyűjtött adatok statisztikai, illetve tudományos feldolgozása tekintetében a tagállamok speciális szabályokat fogadjanak el, amelyek nem módosítják, hanem kiegészítik a GDPR-t.

3.6 Előzetesen felteendő kérdések

A GDPR 25. cikke és a jelen pontban írtak alapján arra a következtetésre lehet jutni, hogy az adatkezelőnek[37] egy mesterséges intelligencián alapuló szoftver használatának megtervezésekor bizonyos kérdéseket fel kell tennie magának, amelyeket az alábbiakban foglalok össze:

[37] Helyzettől függően felmerülhet a közös adatkezelői státusz, illetve az is lehetséges, hogy az MI-t fejlesztő cég adatfeldolgozói pozícióban lesz, így az is szükséges, hogy az adott személy/szervezet a tervezett adatkezelés fényében előzetesen átgondolja és pontosan meghatározza a saját pozícióját.

a) Mi az adatkezelés legitim célja? Figyelemmel kell lenni arra is, hogy a használat ne forduljon át olyan célból történő adatkezelésbe, amely az adatkezelés eredeti céljával nem összeegyeztethető.

b) Mi az adatkezelés jogalapja?

c) Hogyan biztosított az adatok pontossága már az adatgyűjtési fázisától kezdődően? Ennek hiányában téves döntéseket fog hozni még egy egyébként kiváló algoritmussal működő szoftver is, így a torzítások elkerülése érdekében fontos megfelelő intézkedéseket tenni, megbízható információkat tartalmazó forrásokat használni. Külön kiemelendő, hogy az adatkezelési célhoz mérten relevánsnak és reprezentatívnak kell lennie az adatoknak, amelyeket betáplálnak a szoftverbe.

d) Hogyan felelek meg a célhoz kötöttség elvének? Kizárólag azon adatok kezelésére kerülhet sor, amelyek kezelése a jogszerű cél eléréséhez szükséges, figyelmet fordítva a gyűjtött személyes adatok mennyiségén túl a személyes adatok típusára is.

e) Hogyan biztosítom az átláthatóságot? Az érintettek kapjanak megfelelő tájékoztatást a személyes adataik kezelésével kapcsolatban, amelynek azért is van alapvető jelentősége, mert csak megfelelő tájékoztatás esetén van abban a helyzetben az érintett, hogy gyakorolni tudja a jogait.

f) Mennyi ideig kezelem az adatokat? Megfelelő módon határozza meg az adatkezelő az adatok kezelésének időtartamát és integrálja a rendszerbe a törlési, illetve anonimizálási beállításokat, amely anonimizálás tekintetében – a technika gyors fejlődésére is figyelemmel – lényeges, hogy az adatkezelő külön figyelmet fordítson arra, hogy az adatok újra megszemélyesíthetővé vál(hat)nak-e és ha igen, akkor a szükséges intézkedéseket megtegye.

g) Készítettem-e adatvédelmi hatásvizsgálatot? Az adatkezelő az adatkezelés által az érintettek jogaira és szabadságaira gyakorolt kockázatokat tárja fel, elemezze ki és tegye meg azon mindazon intézkedéseket, amelyek az adatkezelés jogszerűségének hatékony és folyamatos biztosításához szükségesek (amely szükségképpen jelenti a szoftver működésének folyamatos figyelemmel kísérését is). Az MI használatát a technológia elérhetősége önmagában nem indokolja, és nem nélkülözhető a szükségesség, arányosság vizsgálata. Előbbi esetében igazolandó, hogy miért nem lehet az adott legitim célt kevésbé invazív eszközökkel elérni, utóbbi tekintetében értékelendő többek között az adatok pontatlanságából, a modell torzításából, esetleges diszkriminatív működéséből adódó kockázat is.

h) Sor került-e tesztelési fázisra? Kiemelten fontos, hogy az éles alkalmazás előtt sor kerüljön tesztelésre, amely során az adatkezelő meg tudja figyelni és kellőképpen ki tudja szűrni a rendszer hiányosságait. Az MI a betáplált adatoktól és a benne futó algoritmus sajátosságaitól függően adott esetben diszkriminálhat bizonyos jellemzőknek meg nem felelő természetes személyeket, amelynek megvalósulása esetén nem beszélhetünk jogszerű adatkezelésről, hiszen az adatkezelés nem felel meg a jogszerűség és tisztességes eljárás elvének (hiába jogszerű az adatkezelés célja, gyűjti be a rendszer csak a szükséges adatokat, pontosak az adatok és megfelelő az őrzési idő).

i) Sor kerül-e kizárólag automatizált döntéshozatalra? Ha igen, akkor a 22. cikk szerinti jogokat is biztosítani kell. Egyebekben érdemes lehet érdemi emberi felügyeletet beiktatni a szoftver működésének folyamatába annak érdekében, hogy egy konkrét személy korrigálni tudjon egy olyan döntést, amely valamilyen okból kifolyólag nem megfelelő, például, ha diszkriminatív döntés lenne (amely esetben az MI az emberi döntéshozatalt segítő, nem azt kiváltó eszköz lenne).

j) Biztosítom-e az érintetti jogokat?

k) Milyen módon tudom biztosítani a modell működésének folyamatos ellenőrzését és javítani az esetleges hibákat?

4. Az MI használatát a GDPR alapján vizsgáló uniós hatósági eljárások

A kutatásaim alapján arra jutottam, hogy a legtöbb MI vonatkozású döntés az olasz adatvédelmi hatósághoz (Garante per la Protezione dei Dati Personali, „Garante") kötődik és olasz kollégákkal konzultálva ennek eredőjét egyfelől magában a Garante tevékenységében látom megnevezhetőnek. Jelesül, a Garante már a GDPR alkalmazandóvá válása előtt is több MI-vel kapcsolatos kérdést vizsgált, illetve intézkedéseket írt elő adatkezelők részére. Például 2013-ban foglalkozott az ún. "redditometro"-val, amely az olasz adóhatóság által jövedelembecslésre használt ellenőrzési eszköz volt. Az olasz adóhatóság olyan módon alkotott adófizetői profilokat, hogy az adófizetők által az adóbevallásukban szereplő adatokat vetette egybe az egyébként máshonnan a kezelésében lévő, valamint bizonyos statisztikákon alapuló feltételezések, becslések alapján kikövetkeztetett adatokkal és ebből vont le következtetést arra nézve, hogy szükséges-e az adott adófizető ellenőrzése adóelkerülési kockázat vélhető fennállása miatt. A Garante különböző intézkedéseket határozott meg, amelyeket a kritikus pontok kezelése érdekében meg kell tenni (többek között azt, hogy gondoskodni kell az adatok minőségéről és pontosságáról, a megfelelő értékelési módszer alkalmazásáról, így arról, hogy az adózó valós jövedelmét csak a tényleges, dokumentált

kiadásokból lehet kiszámítani, és nem lehet a kiadások szintjére vonatkozó, statisztikán alapuló feltételezésekre hagyatkozni, továbbá az adófizetők megfelelő tájékoztatásáról).[38] Úgyszintén 2018. május 25-e előtt, még 2017-ben a "digitális reklámtábla" típusú eszközöknek (ún. totemek) egy vasútállomásra történő telepítésével kapcsolatban vizsgálódott a Garante. Ebben az esetben arról volt szó, hogy a Grandi Stazioni Retail S.p.a. nevű társaság digitális reklámtáblákat helyezett ki a milánói központi pályaudvarra. A reklámtáblákba be volt építve egy arcdetektáló (nem arcfelismerő) kamera. Az eszköz mindössze pár tized másodpercig és kizárólag a RAM-jában tárolta annak a személynek az arcképét, aki elhaladt a reklámtábla előtt, majd a tárolt kép felülíródott a következő felvett képpel (a képet nem továbbították senkinek). A kép alapján az eszköz ezen néhány tized másodperc alatt elvégzett egy elemzést az arckép alapján arról, hogy az illetőnek tetszhetett-e a reklám (mindezt egy 1-től 5-ig terjedő skálán értékelték). Az elemzés adatait (adatcsomag sorszáma, eszköz azonosító száma, rögzítés ideje, tábla előtt eltöltött idő, a nézelődő figyelmének „terjedelme”, az illető neme, korcsoportja, táblától való távolsága, arckifejezése) a reklám közönség általi „elfogadottságára” vonatkozó statisztikai elemzés céljából központilag, titkosítva tárolták. A hatóság a vizsgálata során megfelelőnek ítélte a társaság által megtett intézkedéseket, kiemelve többek között azt, hogy nem arcfelismerő, csupán arcot érzékelő rendszerről van szó, az adatkezelő jogos érdeke szolgálhat az adatkezelés jogalapjaként, egyben előírta az érintettek egyszerűsített helyszíni és részletesebb, honlapon keresztüli tájékoztatását, valamint azt, hogy az adatkezelő legalább hathavonta hajtson végre technikai-biztonsági ellenőrzést a kamera és a helyi memória tekintetében.[39]

Másfelől abban látom a Garante MI vonatkozású aktivitásának okát, hogy a hatóság vezetőségének néhány tagja egyetemi tanár, illetve jogász, akik az MI és így az MI-alapú adatkezelés területén is aktívan tevékenykednek, így minden bizonnyal ezen háttér is indokolhatja, hogy miért tartja kiemelten fontosnak a hatóság, hogy határozottan mutasson irányt az ilyen típusú, megnövekedett kockázatokat jelentő adatkezeléseket végzők számára. Érdemes továbbá azt is hozzáfűzni, hogy a Garante 2022-ben saját féléves ellenőrzési tervében is foglalkozott a mesterséges intelligenciával kapcsolatos tevékenységek ellenőrzésére

[38] Lásd https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf (2023. 09. 02.), 10. o., és https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2765125 (2023. 09. 02.).

[39] Lásd https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252 (2023. 09. 02.).

vonatkozó kötelezettségvállalásokkal, valamint a hatóság elnöke részt vett egy meghallgatáson a hazai parlament előtt, hogy tájékoztatást adjon az EU által tett további lépésekről és a hatóság által biztosított garanciákról, továbbá bejelentést tett arról, hogy a hatóság készséggel integrálná magába az MI monitorozásával kapcsolatos felügyeleti hatásköröket. Összességében valószínűsíthető, hogy a Garante a döntéseivel, kijelentéseivel fel kívánja hívni a figyelmet a magánélet és az MI között meglévő, kétségkívül szoros kapcsolatra és arra, hogy indokolt lenne a hatóságot felruházni az MI felügyeletére vonatkozó jogkörrel és nem egy elkülönült hatóságot létrehozni erre a feladatra.

4.1 A Foodinho ügy[40]

Az olasz adatvédelmi hatóság 2021. júliusában 2.6 millió euró összegű bírságot szabott ki a Foodinho S.r.l. ételfutár hálózatot üzemeltető társaságra, amiért a cég az alkalmazott ételfutárokkal kapcsolatban nem megfelelően használt teljesítmény-értékelő algoritmusokat. Az eljárás tárgyát annak vizsgálata képezte, hogy az adatkezelő által üzemeltetett, a futárok munkavégzését értékelő szoftver jogszerűen működött-e, nem sérti-e az átláthatóság elvét, különös tekintettel a használata révén megvalósuló automatizált döntéshozatalra. Az olasz eljárás idején mintegy 19.000 futárt foglalkoztatott a cég[41].

A hatóság döntése szerint a társaság kétféle rendszert üzemeltetett, az ún. „Kiválósági rendszert" és a „Jarvis rendszert". Előbbi rendszer egy belső pontozásos rendszer, amelyet a szállítási idősávok kiosztására használtak. A cég ezen rendszeren keresztül minden futárhoz egy pontszámot rendel és a magasabb pontszámot elért futárok elsőbbséget élveznek a szállítási idősávok kiosztásakor, így ennek eredményeképpen a "kevésbé kiváló" futárokat kizárják az időpontok kiosztásából, ha az összes rendelkezésre álló szállítási időpontot már elfoglalták a "kiválóbbak". A pontszámot egy automatizált matematikai képlet segítségével osztják ki főként az ügyfelektől és partnerektől érkező visszajelzések és a kézbesítési arányok alapján. A negatív visszajelzések azonban nagyobb súllyal estek latba, mint a pozitívak, és a rendszer büntette a bizonyos szállítási küszöbértékeket el nem érő futárokat. A Jarvis rendszert a megrendelések kiosztásához használták olyan adatok számba vételével, mint a GPS-eszközből származó geolokációs adat, az étel-felvételi hely, a szállítási cím, a megrendelésre vonatkozó különleges

[40] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677611 (2023. 08. 14.).

[41] Lomas, Natasha: Italy's DPA fines Glovo-owned Foodinho $3M, orders changes to algorithmic management of riders, 2021. július 6. (https://techcrunch.com/2021/07/06/italys-dpa-fines-glovo-owned-foodinho-3m-orders-changes-to-algorithmic-management-of-riders/ (2023. 08. 14.)).

követelmények és a jármű típusa. A Jarvis ezeket az adatokat kezelve teljesen automatizáltan osztja ki a megrendeléseket. A cég nem tisztázta a Garante számára, hogy ez az algoritmus pontosan hogyan működik együtt a Kiválósági rendszerrel[42].

A Garante megállapította, hogy az adatkezelő megsértette többek között az átláthatóság, az adattakarékosság és a korlátozott tárolhatóság elvét, a 13. cikket, valamint az alapértelmezett és beépített adatvédelem elvét.

A tájékoztató nem tartalmazott információt az automatizált döntéshozatal tényéről, így az alkalmazott logikáról, sem arról, hogy az adatkezelés milyen jelentőséggel bír és a futárokra nézve milyen következményei lehetnek a döntéshozatalnak.

A Garante a 25. cikk sérelmét abban jelölte meg, hogy sérült az adattakarékosság elve, a hozzáférési jogok pedig egyes esetekben túl széleskörűen kerültek kialakításra.

Sérült továbbá a GDPR 22. cikk (3) bekezdése is, mivel az algoritmus diszkriminatív módon működött és a cég nem tett megfelelő intézkedéseket alkalmazottainak ezen diszkriminatív automatizált döntéshozatallal szembeni védelme érdekében, nem biztosította az emberi beavatkozáshoz való jogot, valamint azt a jogot, hogy a futárok kifejthessék álláspontjukat és kifogást nyújthassanak be az algoritmus által hozott döntésekkel szemben. A döntéshozatal diszkriminatív volta abban nyilvánult meg, hogy a Foodinho S.r.l. kizárólag automatizált döntéshozatalon alapuló döntéseket hozott a futárokról a szakmai teljesítményük, viselkedésük, valamint tartózkodási helyük és mozgásuk elemzése révén és ezen adatok alapján – a negatív értékeléseket felülsúlyozva – hozott döntések révén egyes futárokat kizártak munkalehetőségekből.

A hatóság külön kiemelte, hogy az adatkezelő nem ellenőrizte, hogy a rendszer által használt adatok megfelelőek-e a kitűzött célokhoz képest és nem fogadott el olyan technikai és szervezési intézkedéseket, amelyek a rendszer eredményei pontosságát, torzítás-mentességét lettek volna hivatva biztosítani.

A fentieknek megfelelően a hatóság többek között arra kötelezte az adatkezelőt, hogy (i) adjon megfelelő tájékoztatást az érintettek részére, (ii) tegye meg azon intézkedéseket, amelyek védelmet nyújtanak a rendszerek diszkriminatív működésével szemben, (iii) biztosítsa a 22.

[42] Milner-Smith, Helena–Cooper, Dan: Italian Supervisory Authority Fines Foodinho Over Its Use of Performance Management Algorithms, 2021. július 13. (https://www.insideprivacy.com/gdpr/italian-supervisory-authority-fines-foodinho-over-its-use-of-performance-management-algorithms/) (2023. 08. 14.).

cikk (3) bekezdésében meghatározott érintetti jogokat, (iv) tegye meg azon intézkedéseket, amelyek biztosítják az adatok pontosságát és az adatkezelés céljához mért relevanciáját (azt rendszeresen ellenőrizze), (v) megfelelően határozza meg az őrzési időket.

4.2 A Deliveroo ügy[43]

A Garante egy másik, ugyancsak ételfutárokat foglalkoztató, Deliveroo Italy s.r.l. nevű társaság adatkezelési gyakorlatát is vizsgálta annak kapcsán, hogy a cég a kb. 8.000 futár személyes adatait megfelelően kezeli-e a munkaszervezést és megrendelések futárok közötti kiosztását végző algoritmussal.

Az adatkezelő gyakorlatának vizsgálatát követően a hatóság megállapította, hogy a cég nem nyújtott átlátható tájékoztatást a futároknak a futárok munkabeosztásának kezeléséhez használt algoritmusról. A Garante hozzátette, hogy a Deliveroo szoftvere aránytalanul nagy mennyiségű személyes adatot gyűjtött a futárokról, megsértve ezzel a jogszerűség, az átláthatóság, az adatminimalizálás és a korlátozott tárolhatóság elvét.

A hatóság egyben kötelezte az adatkezelőt, hogy tegyen megfelelő intézkedéseket a futárok jogainak védelme érdekében, biztosítsa az átláthatóságot, valamint az adatok pontosságát az algoritmus használata során és készítsen adatvédelmi hatásvizsgálatot[44], valamint kiszabott a cégre 2.5 millió euró összegű bírságot.

---

[43] Lásd „*Italian Garante Fines Deliveroo 2.5M Euros for Unlawful Processing of Personal Data*" című cikket, 2021. augusztus 5. (https://www.huntonprivacyblog.com/2021/08/05/italian-garante-fines-deliveroo-2-5m-euros-for-unlawful-processing-of-personal-data/) (2023. 08. 15.).

[44] Ettől az ügytől független egy másik, szintén a Garante gyakorlatában előfordult eset, amikor 2022-ben az olasz adóhatóság egy általa készített adatvédelmi hatásvizsgálatot nyújtott be a Garante-hoz véleményezésre. Az adóhatóság célja az volt, hogy az MI segítségével megpróbáljon feltárni arra vonatkozó valószínűségeket a kezelésében lévő egyes adatbázisokban szereplő számos személyes adat elemzése révén, hogy mely jogalany esetében merülhet fel az adóelkerülés, adócsalás kockázata. A Garante engedélyezte az adatkezelést, egyúttal kiemelte, hogy a gépi tanuláson alapuló sztochasztikus modell esetében az egyik fő kockázatot az algoritmusok kialakítása során megjelenő potenciális hibák és torzítások jelentik, ennek megfelelően a végrehajtandó intézkedéseket az adatbázisok jellemzőihez, az elemzési modellekhez kell igazítani. A Garante többek között azt írta elő, hogy az adóhatóság ellenőrizze az analitikus modellek minőségét, és a paramétereket, az elvégzett tevékenységeket, az esetleges kritikus pontokat és az ilyen kritikus pontok kezelése érdekében hozott intézkedéseket rendszeresen dokumentálja az adatvédelmi tisztviselő bevonásával, és szükség szerint frissítse a hatásvizsgálatot. A Garante előírta továbbá, hogy az adóhatóság alkalmazzon hatékony álnevesítést, tegye közzé a hatásvizsgálat kivonatát és gondoskodjon megfelelő emberi beavatkozás elemzési folyamatba történő

Az algoritmus pontozta a futárokat többek között a következő szempontok szerint: (i) péntek, szombat és vasárnap esti elérhetőség, (ii) megbízhatóság, (iii) sebesség. A hatóság megállapítása szerint nem volt átlátható az algoritmus működése, a cég nem tudta igazolni az algoritmus diszkrimináció mentességét, a geolokációs adatok begyűjtése túlzott mértékű volt, egyes adatokat pedig túl sokáig őriztek meg.

4.3 A Clearview AI ügyek

A Clearview AI Inc. nevű egyesült államokbeli, arcfelismerő szoftvert működtető cég az Interneten fellelhető, természetes személyek képmását tartalmazó fotókat és geolokációs adatokat gyűjtötte be nagyon nagy számban[45] és az így összeállított adatbázishoz biztosított hozzáférést különböző nyomozóhatóságok számára.

A társaság ellen több EU országban indult eljárás jogsértő adatkezelés gyanújával, így többek között Olaszországban, Franciaországban és Görögországban[46].

4.3.1 A Clearview AI és az olasz hatóság

A Garante azt követően, hogy a sajtóban hírek jelentek meg a társaság által üzemeltetett szoftverrel kapcsolatban, valamint a hatóság panaszokat, illetve jelzéseket kapott, többek között jogvédő szervezetektől a Clearview AI Inc. által folytatott adatkezelési gyakorlatot illetően, a hatóság az alábbi jogsértéseket állapította meg:

---

beépítéséről és az algoritmussal dolgozó személyzet megfelelő képzéséről annak érdekében, hogy a személyzet tisztában legyen az algoritmikus folyamatok képességeivel és korlátaival, továbbá gondoskodjon arról is, hogy a személyzet indokolt esetben hagyja figyelmen kívül az MI által generált kimeneteket. Lásd https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9808839 (2023. 09. 02.).

[45] Az Interneten elérhető információk alapján jelenleg már több, mint 30 milliárd fotó kezeléséről lehet szó.

[46] Érdekesség, hogy a svéd, bűnügyi adatok kezeléséről szóló törvényben foglaltak megsértése miatt – egyéb intézkedések mellett – 2021-ben 2.5 millió svéd korona (mintegy 250.000 euró) összegű bírságot szabott ki a svéd adatvédelmi hatóság a svéd rendőrségre amiért az jogellenesen használta a Clearview AI szolgáltatását. Lásd https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en (2023. 09. 02.). Lényeges megemlíteni, hogy ebben az ügyben nem a GDPR, hanem a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló 2016/680 EU irányelvet átültető svéd törvény volt alkalmazandó, tekintettel arra, hogy rendőrség általi bűnüldözési célú adatkezelésről van szó.

- a társaság a birtokában lévő személyes adatokat, beleértve a biometrikus és geolokációs információkat is, megfelelő jogalap nélkül kezelte, mivel a társaság jogos érdeke nem szolgál megfelelő jogalapul,
- a Clearview AI Inc. megsértette a GDPR több alapelvét, így például az átláthatóság, a célhoz kötöttség és a korlátozott tárolhatóság elvét,
- az adatkezelő elmulasztotta a GDPR 13-14. cikkeiben meghatározott tájékoztatást megadni az érintettek részére, valamint nem nyújtott tájékoztatást a 15. cikk szerint az érintett kérelmére, és
- a társaság nem jelölt ki képviselőt az EU-ban.

A Garante 2022 februári határozatában a megállapított jogsértésekért 20 millió euró összegű bírságot szabott ki a társaságra, megtiltotta a további adatgyűjtést és adatkezelést, továbbá elrendelte a társaság arcfelismerő rendszere által kezelt adatok – köztük a biometrikus adatok – törlését az Olaszország területén tartózkodó személyek tekintetében, valamint elrendelte egy képviselő kijelölését az Európai Unió területén[47].

A jogalap tekintetében a hatóság úgy érvelt, hogy mivel jelen ügyben nem volt vitatott, hogy az érintettek hozzájárulását nem szerezték be, továbbá tekintettel arra, hogy a 6. cikk (1) bekezdés b), c), d) és e) pontjában említett feltételek kizártak, azt kell megvizsgálni, hogy fennáll-e az adatkezelő jogos érdeke, amelyre a társaság hallgatólagosan hivatkozik, amennyiben tevékenységét a „Google search" által végzett adatkezeléssel teszi egyenlővé[48].

A hatóság felhívja a figyelmet arra, hogy alapvetően nem áll fenn általános felhatalmazás a nyilvánosság számára hozzáférhetővé tett személyes adatok újrafelhasználására és további kezelésére, az adatok nyilvános volta csupán egy olyan körülmény, amely az érdekmérlegelés egyik lehetséges értékelési eleme lehet[49].

A hatóság megállapítása szerint a társaság jogos érdekét a nyereségvágy képezi egy olyan adatkezeléssel szemben, amely különösen invazív jellegű, mivel fényképes adatok gyűjtéséből áll, amelyekhez további, a magánszemélyek magánéletének különböző aspektusait feltárni

[47] https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en (2023. 08. 14.).

[48] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362 (2023. 08. 14.).

[49] 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról (WP217), elérhető: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf (2023. 08. 14.), 16. o.

képes információk kapcsolódnak. Ezek az adatok biometrikus adatok, mert konkrét személy egyedi azonosítását célozzák és különösen nagyszámú személyre vonatkoznak, ráadásul kiskorúakat is érint.

A hatóság külön felhívta a figyelmet arra, hogy a Clearview AI Inc. adatkezelése különleges adatokat is érint (biometrikus adatok), így a 9. cikkben található egyik feltételnek is meg kellene feleljen az adatkezelés. Ezzel kapcsolatban azt hangsúlyozta a hatóság, hogy a 9. cikk (2) bekezdés e) pontja szerinti feltétel[50] önmagában nem elegendő a megfelelés igazolására, hiszen megfelelő érdekmérlegelés végzendő a 6. cikk (1) bekezdés f) pontjára tekintettel.

A Garante véleménye szerint így az adatkezelő jogszerűen nem hivatkozhat a jogos érdekére az adatkezelés jogalapjaként, illetve a 9. cikkben előírtak is sérülnek.

4.3.2 A Clearview AI és a francia adatvédelmi hatóság (CNIL)[51]

2020 májusát követően a CNIL-hez magánszemélyektől érkezett panasz a Clearview AI arcfelismerő szoftverével kapcsolatban, amelyet követően a hatóság vizsgálatot indított. 2021 májusában a Privacy International nevű szervezet szintén figyelmeztette a CNIL-t a társaság gyakorlatára.

A hatóság először felszólította az adatkezelőt, hogy hagyjon fel a jogalap nélküli gyakorlat Franciaország területén történő folytatásával, valamint felhívta az érintetti kérelmek megfelelő kezelésére, amely felszólításra a Clearview AI Inc. nem válaszolt. Ezt követően a CNIL a 2022. októberében hozott határozatában megállapította a személyes adatok jogellenes kezelésének tényét, mivel a biometrikus adatok gyűjtése és felhasználása jogalap nélkül történt, valamint az érintettek jogai sérülését, különösen az adataikhoz való hozzáférés és azok törlése iránti kérelmek esetében (a GDPR 12., 15. és 17. cikke) és ugyancsak 20 millió euró összegű bírságot szabott ki az adatkezelőre, egyidejűleg felszólítva a társaságot arra, hogy két hónapon belül hagyjon fel a jogsértő gyakorlattal, ne gyűjtse és ne kezelje a Franciaországban lakóhellyel rendelkező személyek adatait jogalap nélkül és törölje ezen személyek már begyűjtött adatait.

[50] A 9. cikk (1) bekezdése szerinti tilalom nem áll fenn, ha „*az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott*".

[51] A CNIL 2019 októberében iskolákba telepített arcfelismerős beléptetőrendszert vizsgálva megállapította, hogy annak használata nem felel meg az arányosság, sem az adatminimalizálás elvének. Lásd https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position (2023. 09. 02.).

Egyúttal a két hónapon túli késedelem minden egyes napjára 100.000 euró összegű bírság megfizetését írta elő.[52]

A CNIL a Garante döntésében foglaltakhoz hasonlóan kiemelte, hogy ahhoz, hogy a személyes adatok kezelése jogszerű legyen, az adatkezelésnek a GDPR 6. cikkében megnevezett jogalapok valamelyikén kell alapulnia.

A hatóság megállapította, hogy az adatkezelő nem kéri az érintettek hozzájárulását ahhoz, hogy a fényképeket összegyűjtse és felhasználja a szoftver megalkotásához és működtetéséhez. Jelezte továbbá, hogy a társaságnak nem fűződik jogos érdeke ezen adatok gyűjtéséhez és felhasználásához, különös tekintettel az eljárás tolakodó és tömeges jellegére, amely lehetővé teszi a franciaországi internetezők millióinak Interneten található képeinek lekérdezését. Az érintettek, akiknek a fényképei különböző weboldalakon elérhetők, észszerűen nem számolhatnak azzal, hogy a képeiket a társaság kezeli egy olyan arcfelismerő rendszer kifejlesztése, működtetése céljából, amelyet egyes államok bűnüldözési célokra használhatnak. Mivel a többi jogalap[53] úgyszintén nem jöhet szóba, így a Clearview AI arcfelismerő szoftvere használatának nincs megfelelő jogalapja, ezért a végzett adatkezelés jogellenes.

Az érintetti jogokkal kapcsolatban a CNIL megjegyezte, hogy a társaság nem könnyíti meg az érintett hozzáférési jogának gyakorlását azáltal, hogy

- e jog gyakorolhatóságát a kérelmet megelőző 12 hónapban gyűjtött adatokra korlátozza,
- e jog gyakorolhatóságát indokolás nélkül évente kétszerre korlátozta,
- csak bizonyos megkeresésekre válaszolnak, ha egy személytől túl sok megkeresés érkezik,
- a társaság nem válaszol, vagy csak részleges választ ad a hozzáférési és törlési kérelmekre.

4.3.3 A Clearview AI és a görög adatvédelmi hatóság

A görög adatvédelmi hatóság egy hozzá érkezett panaszbejelentés nyomán induló eljárás során úgyszintén 20 millió euró összegű bírságot szabott ki a Clearview AI társaságra amiért az megsértette a GDPR 5. cikk (1) bekezdésének a) pontját, (2) bekezdését, 6., 9., 12., 14., 15. és

[52] https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai (2023. 08. 04.).

[53] GDPR 6. cikk (1) bekezdés b)-e) pontjai szerinti jogalapok.

27. cikkét. A hatóság egyidejűleg kötelezte a társaságot, hogy tegyen eleget a panaszos hozzáférés iránti kérelmének, valamint megtiltotta a Görögországban található érintettek fényképeinek gyűjtését és kötelezte a céget, hogy törölje a Görögországban található azon érintettek személyes adatait, amelyeket a szolgáltatása nyújtásához gyűjtött[54].

4.4 A Replika ügy[55]

A Luka, Inc. nevű egyesült államokbeli céget, amely a Replika nevű „virtuális barátként" működő chatbot fejlesztője, a Garante 2023. februárjában hozott döntésében felszólította, hogy azonnali hatállyal szüntesse be Olaszország területén a szoftver működtetését, különösen a kiskorúakra és az érzelmileg sebezhető személyekre jelentette kockázatokra tekintettel.

Korábban is merültek fel aggályok az ilyen technológia által gyermekekre jelentette kockázatokkal kapcsolatban, akár a nem megfelelő tartalmaknak kitettségre gondolunk, akár arra, hogy a gyermekekben függőség alakulhat ki az ilyen jellegű szoftverektől, vagy azok arra ösztönözhetik őket, hogy pénzt költsenek például „avatárjuk" egyediesítésére[56].

Az alkalmazás egy mesterséges intelligenciával működő, szöveges és hangalapú interfésszel felszerelt chatbot, amely egy "virtuális barátot" generál, akit a felhasználók barátként vagy partnerként konfigurálhatnak. A Replika a fejlesztő honlapján és a két nagy alkalmazás áruházban olyan chatbotként van feltüntetve, amely javíthatja a felhasználók hangulatát és érzelmi jólétét azáltal, hogy segít nekik megérteni a gondolataikat és érzéseiket, segít a stressz kontrollálásában, szorongásuk enyhítésében és a pozitív gondolkodás kialakításában.

Az olasz hatóság döntését az alábbi hiányosságokkal indokolta:

- az alkalmazásban nem működtetnek megfelelő szűrő rendszert a felhasználók életkorának ellenőrzésére (a weboldalon közzétett adatvédelmi szabályzatban az adatkezelő kijelentette, hogy a 13 év alatti gyermekek személyes adatait nem gyűjtik tudatosan, egyidejűleg a szülőket/gyámokat arra ösztönzik, hogy kövessék nyomon gyermekeik Internet-használatát, és utasítsák a gyermekeket, hogy engedélyük nélkül soha ne adjanak meg személyes adatokat, és lépjenek kapcsolatba a platformmal, ha

[54] https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en (2023. 09. 02.).

[55] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852214#english (2023. 08. 14.).

[56] Lomas, Natasha: Replika, a 'virtual friendship' AI chatbot, hit with data ban in Italy over child safety, 2023. február 3. (https://techcrunch.com/2023/02/03/replika-italy-data-processing-ban/) (2023. 08. 13.).

okuk van azt feltételezni, hogy 13 év alatti gyermek személyes adatokat adott meg, hogy ezeket az adatokat eltávolíthassák az adatbázisokból. Az alkalmazás a két fő alkalmazás áruházban 17 év feletti személyek számára alkalmasnak lett minősítve, miközben a közzétett általános szerződési feltételek megemlítik, hogy 13 év alatti gyermekek nem használhatják az alkalmazást, a 18 év alatti felhasználók esetén pedig előzetesen a szülőknek vagy törvényes képviselőiknek kell engedélyezniük az alkalmazás használatát),

- a program csak a nevük, email fiókjuk és nemük megadására kéri a felhasználókat,
- nem lépnek működésbe blokkoló mechanizmusok akkor sem, ha a felhasználó kifejezetten kijelenti, hogy kiskorú,
- az adatkezelési tájékoztató nem tartalmaz információt az adatkezelés lényeges elemeiről, különösen a gyermekek személyes adatainak kezeléséről, így sérti az átláthatóság elvét,
- az adatkezelés jogalapja nem határozható meg, mivel gyermekek esetében kizárható, hogy az adatkezelés jogalapja az érintettel kötött szerződés teljesítése lenne, mivel a gyermekek az olasz jog szerint nem cselekvőképesek,
- a gyermekek számára a fejlettségi szintjüknek nem megfelelő válaszokat generál a szoftver (pl. szexuális tartalmúak egyes válaszok).

A fentiek alapján a Garante megállapította, hogy az adatkezelő megsértette a GDPR 5., 6., 8., 9. és 25. cikkében foglaltakat.

4.5 A Budapest Bank ügy[57]

A magyar adatvédelmi hatóság (NAIH) ebben az ügyben olyan mesterséges intelligencia segítségével végzett adatkezelést vizsgált, amely adatkezelés a Budapest Bank által hangfelvétel-elemzésre használt gépi tanulással működő MI alapú szoftver használata révén valósult meg. A hatóság több rendelkezés megsértését állapította meg[58] és 250 millió forint[59] összegű bírságot szabott ki az adatkezelőre.

[57] NAIH-85-3/2022, korábbi ügyszám: NAIH-7350/2021.

[58] GDPR 5. cikk (1) bekezdés a) és b) pontja, 6. cikk (1) bekezdése, 6. cikk (4) bekezdése, 12. cikk (1) bekezdése, 13. cikk, 21. cikk (1) és (2) bekezdése, 24. cikk (1) bekezdése, 25. cikk (1) és (2) bekezdése.

[59] Ez az összeg, 383 forintos euró árfolyammal számolva, kerekítve 653.000 eurónak felel meg.

A bank az ügyfélszolgálati hívások rögzített hanganyagát egy MI-alapú szoftver segítségével automatikusan elemezte és az elemzés eredménye alapján állapította meg, hogy melyik elégedetlen ügyfelet szükséges visszahívni. A szoftver automatikusan elemezte mind a telefonáló ügyfél/érdeklődő, mind az ügyfélszolgálati munkavállaló érzelmi állapotát és a beszélgetés egyéb jellemzőit. A hatóság azt vizsgálta, hogy a bank ügyfélszolgálati hívások rögzített hanganyagát automatikusan elemző tevékenységével, a felvételek visszahallgatásával, illetve bizonyos érintettek visszahívásával kapcsolatos adatkezelése megfelelt-e az adatvédelmi követelményeknek, így többek között megfelelő tájékoztatást nyújtott-e az érintetteknek az adatkezelésről.

A bank nyilatkozata szerint a szoftver a beszélgetéseket a beletáplált jellemzők alapján elemezte, rangsorolta, amely jellemzőket a bank nem ismeri[60], a hívások visszahallgatása pedig véletlenszerűen történt. A rendszer működtetésének célja „hívások minőségellenőrzése", a „panasz és ügyfélelvándorlás megelőzése", valamint a „hatékonyság növelése" volt[61].

A hatóság megállapította, hogy a szoftver a hívásokról felállított sorrenddel lényegében javaslatot tett arra, hogy mely személyt lenne célszerű visszahívni. A visszahívásra vonatkozó döntést a bank munkavállalói hozták meg. A visszahívás célja az ügyfél elégedetlenségének kezelése volt, nem az esetleges konkrét panasz kezelése.

A hatóság megállapítása szerint az adatkezelési tájékoztató csupán általános információkat tartalmaz a híváselemzésről[62], nem ismerteti a hangelemzés módszerét, jellemzőit, illetve a tájékoztatóban a minőségbiztosítás és a panasz megelőzés szerepel célként, ez elégedetlenség kezelése nem.

A NAIH megállapította, hogy az adatkezelő nem tájékoztatta az érintetteket arról, hogy milyen adataikat, milyen módon kezelik, továbbá arról, hogy az érzelmi reakcióikat elemzik. A

[60] A bank nyilatkozata szerint „*[…] A szoftver a hangfelvételt […] - a fejlesztő üzleti titkát képező - szempont szerint elemzi. Ezek közül a fejlesztő a beszéd sebességét, hangerejét, hangmagasságát, a beszédszünetek hosszát ismertette példaként. Az elemzés eredményeként nem készül profil, hanem a felvételeket a rendszer napi rangsorba állítja. A sorrend alapja, hogy a vizsgált szempontokból levonható következtetés szerint a telefonáló - bár formális panaszt nem terjesztett elő - elégedetlen volt-e az ügyintézéssel.*"

[61] Lásd határozat 3. o.

[62] A bank *"minőségbiztosítási, panasz megelőzési célból jogos érdeken alapuló profilalkotást végez és automatikus döntés útján választja ki azon hívásokat, melyben magasabban képzett banki dolgozó visszahívás útján hárítja el a telefonbeszélgetésben felmerült problémát, panaszt"*, határozat 20. és 25. o.

hatóság hozzátette, hogy 13. cikk szerint adandó tájékoztatás elemei közül csak a jogalapról adott tájékoztatást az adatkezelő, az adatkezelés célja pedig nem lett teljeskörűen megnevezve.

A hatóság a határozat bank érdekmérlegelésével kapcsolatban írt részében hangsúlyozza, hogy mivel a mesterséges intelligencia használata jellemzően nehezen átlátható, ezért is „*különös odafigyelést igényel – nemcsak papíron leírva, hanem ténylegesen megvalósítva – a mesterséges intelligencia használata az adatkezelés során akkor, ha az általános adatvédelmi rendelet szerinti átláthatósági és elszámoltathatósági feltételeknek meg akar felelni az adatkezelő. Ez túlmutat egy átlagos kockázatú adatkezelés esetén irányadó alapértelmezett elvárhatósági szinttől, és – figyelembe véve az általános adatvédelmi rendelet 24. és 25. cikkei szerinti kockázatalapú megközelítést – ennek a nehézségnek a figyelembevételével kell az adatkezelőnek döntést hoznia arról, hogy mikor és mire használja a mesterséges intelligenciát, és ezzel kapcsolatban hogyan biztosítja az átláthatóságot.*”[63]

Álláspontom szerint az idézett néhány sor a döntés lényege rövid összefoglalásának is tekinthető, mert a 25. cikkből tulajdonképpen „minden” más kötelezettség következik, abból közvetlenül levezethető. A NAIH egyidejűleg utal az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021. sz. közös véleményére[64], amely a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról szól és amely szerint a mesterséges intelligencia természetes személyek érzelmeinek elemzésére való felhasználása nemkívánatos, amelyet bizonyos szűk körű kivételektől eltekintve meg kell tiltani.

A hatóság megállapította, hogy nem áll meg a jogos érdek, mint jogalap, tekintettel arra, hogy az érdekmérlegelés csak azt tartalmazta, hogy a banknak miért szükséges az adatkezelés, azonban az érintetti oldalt nem vizsgálta a bank és így nem is ütköztette az érdekeket, azaz nem végzett valós érdekmérlegelést.

A NAIH az érintetti jogokat vizsgálva megállapította, hogy a tiltakozási jogot a bank nem biztosította az érintettek részére[65]. Úgyszintén a megfelelő tájékoztatás elmaradása

[63] Lásd határozat 26. o.

[64] https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_hu.pdf (2023. 07. 19.).

[65] Az ügy külön érdekessége, hogy a GDPR 22. cikk szerinti automatizált döntéshozatal jelen ügyben nem valósult meg, mert a visszahívásra nem javasolt ügyfelek esetében ugyan teljesen automatizált volt a döntés a vissza nem

következtében a telefonálók nem sejthették, hogy hangjukat elemzésnek veti alá a bank, ami önmagában az érintetti jogok sérülését eredményezi, hiszen, ha az érintett nem tud egy adatkezelésről, akkor a jogait sem tudja gyakorolni azzal kapcsolatban. Másfelől, abból, hogy egy ügyfél felhív egy bankot, nem következik az, hogy számíthat arra, hogy a hangját kielemzik és adott esetben visszahívják azért, mert az elemző szoftver szerint elégedetlen lehetett.

4.6 A ChatGPT ügy

A hírekben számos helyen lehetett olvasni az olasz adatvédelmi hatóság idén márciusban hozott döntéséről, amellyel ideiglenesen betiltotta a ChatGPT Olaszországon belüli használatát, azonban a konkrét részletekről kevesebb szó esett, a sajtó elsősorban azt kapta fel, hogy tilos a ChatGPT használata Olaszországban. Az alábbiakban összefoglalom a „ChatGPT ügy" lényegét.

Az ügy egy idén március 20-án bejelentett adatvédelmi incidensből indult, amely a ChatGPT felhasználók beszélgetéseit és a szolgáltatás előfizetőinek fizetési adatait érintette[66].

A Garante – jelezve, hogy a nagy nyelvi modell alapú mesterséges intelligencia használatán alapuló szoftverekre is vonatkoznak az Európai Unió adatvédelmi jogszabályai – 2023. március 30-án hozott döntésében[67] megállapította, hogy

- a ChatGPT üzemeltetője, az OpenAI, LLC nevű egyesült államokbeli cég nem nyújtott megfelelő tájékoztatást az adatkezeléssel kapcsolatban sem a program felhasználói, sem azon természetes személyek részére, akiknek a személyes adatait az adatkezelő begyűjtötte és a szoftver tanításához felhasználta/felhasználja,
- nincs megfelelő jogalapja a személyes adatok gyűjtésének és azok ChatGPT működésének alapjául szolgáló algoritmusok tanítása céljából történő kezelésének,

hívásról, azonban nem valósult meg a „joghatás vagy jelentős mértékű hatás" a vissza nem hívott ügyfelek vonatkozásában, a visszahívásra javasolt ügyfelek esetében pedig végső soron egy banki személy döntött a visszahívásról, így ezen esetben ezért nem állt fenn a 22. cikk szerinti jogszabályi tényállás. A munkavállaló ellenőrzése ugyancsak emberi döntés esetében történt meg, így az ő esetükben sem került sor a 22. cikk szerinti teljesen automatizált döntéshozatalra.

[66] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english (2023. 08. 04.).

[67] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 (2023. 08. 04.).

- az érintettek személyes adatainak kezelése nem felel meg a pontosság elvének, tekintettel arra, hogy a ChatGPT által közölt információk nem mindig felelnek meg a valóságnak, valamint
- a szolgáltatással kapcsolatban az adatkezelő nem ellenőrzi a felhasználók életkorát, amely szolgáltatás az OpenAI LLC által közzétett általános szerződési feltételek szerint 13 éves vagy annál idősebb személyek számára van fenntartva, jelezve, hogy a 13 éven aluli gyermekek a szűrők hiánya miatt olyan válaszoknak vannak kitéve, amelyek fejlődési szintjükhöz és önismeretükhöz nem megfelelőek.

A Garante döntésében arra tekintettel, hogy a ChatGPT általi adatkezelés sérti a GDPR 5., 6., 8., 13. és 25. cikkeit, azonnali hatállyal elrendelte az adatkezelés átmeneti korlátozását az Olaszország területén élő természetes személyek személyes adatainak kezelése tekintetében. A Garante egyidejűleg felhívta az adatkezelőt, hogy húsz napon belül közölje, hogy milyen intézkedéseket tett az előírtak végrehajtása érdekében, továbbá nyújtson be minden olyan információt, amelyet hasznosnak tart a hatóság által megnevezett jogsértések igazolására.

Az OpenAI LLC nem telepedett le az EU területén, így valamennyi uniós adatvédelmi hatóság jogosult önállóan eljárni az OpenAI LLC céggel szemben, amely aláásható az egységes EU-s gyakorlat kialakulását, hiszen nem kizárt, hogy az egyes uniós adatvédelmi hatóságok nem ugyanolyan módon ítélnék meg a ChatGPT általi adatkezelés egyes aspektusait. A Garante ezt érzékelve kezdeményezte, hogy az Európai Adatvédelmi Testület foglalkozzon a ChatGPT általi adatkezeléssel, amelyet követően külön munkacsoport alakult a Testületen belül. A munkacsoport munkájáról jelenleg nem ismertek a részletek.

A Garante fent hivatkozott végzésének kiadását követően az OpenAI és a hatóság között lezajlott megbeszélés után a Garante április 12-én kiadott egy közleményt[68] azon intézkedésében előírt kötelezettségekről, amelyeket az adatkezelő a tilalom megszüntetése végett köteles teljesíteni. A Garante előírta, hogy

- az adatkezelőnek olyan adatkezelési tájékoztatót kell készítenie és a weboldalán elérhetővé tennie, amely ismerteti a ChatGPT működéséhez szükséges adatkezelés jellemzőit és logikáját, valamint az érintettek (felhasználók és nem felhasználók) jogait,

[68] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751 (2023. 08. 04.).

- a tájékoztatót könnyen hozzáférhetővé kell tenni, és úgy kell elhelyezni, hogy azt a szolgáltatásra való regisztráció előtt el lehessen olvasni,
- a regisztrált felhasználóknak a szolgáltatáshoz való hozzáféréskor, annak újraaktiválása után figyelmeztetést kell kapniuk, amikor egy olyan korhatár szűrőn kell átmenniük, amely a beírt életkor alapján kiszűri a kiskorú felhasználókat,
- a felhasználók személyes adatainak az algoritmusok tanítása céljából történő kezelésének jogalapját illetően a hatóság arra kötelezte az OpenAI LLC-t, hogy törölje a szerződés teljesítésére való valamennyi utalást, és – az elszámoltathatóság elvével összhangban – az érintett hozzájárulására, vagy az adatkezelő (vagy harmadik fél) jogos érdekére alapozza az adatkezelést,
- lehetővé kell tenni az érintettek – köztük a nem felhasználók – számára a szolgáltatás által tévesen előállított személyes adataik helyesbítését, illetve, ha a helyesbítés technikailag kivitelezhetetlen, az adatok törlését. Az adatkezelőnek könnyen hozzáférhető eszközöket kell rendelkezésre bocsátania ahhoz, hogy a nem felhasználók élhessenek az algoritmusok működéséhez felhasznált személyes adataik kezelése elleni tiltakozáshoz való jogukkal, amely jogot a felhasználók részére is biztosítani kell, ha adataik kezelésének jogalapjaként a jogos érdekek szolgál,
- haladéktalanul vezessen be egy életkor-ellenőrzési rendszert a szolgáltatásra való regisztráció során, az erre vonatkozó tervet nyújtsa be és a megoldást 2023. szeptember 30-ig valósítsa meg a 13 év alatti felhasználók, valamint azon 13 és 18 év közötti felhasználók kiszűrésére, akik esetében nem áll rendelkezésre a szülői felügyeletet gyakorló személyek hozzájárulása,
- az OpenAI LLC május 15-ig a hatósággal egyetértésben tájékoztató kampányt kell végezzen a rádióban, a televízióban, az újságokban és az interneten keresztül, hogy tájékoztassa a magánszemélyeket személyes adataiknak az algoritmusok tanításához történő felhasználásáról.

A hatóság hozzátette, hogy folytatja a vizsgálatot a hatályos jogszabályok esetleges megsértésével kapcsolatban és további intézkedések meghozataláról dönthet, amennyiben az szükségesnek bizonyul.

A Garante április 28-i közleményében[69] közzétette, hogy az OpenAI LLC azt jelezte vissza a hatóságnak, hogy (i) elkészítette és a honlapján közzétette a felhasználóknak és a nem felhasználóknak szóló adatkezelési tájékoztatót, amelyben leírja, hogy mely személyes adatokat milyen intézkedések keretében kezelnek az algoritmusok tanításához, és felhívja a figyelmet, hogy mindenkinek joga van kikerülni az adatkezelés hatálya alól, (ii) elkészítette a felhasználóknak szóló adatkezelési tájékoztatót, amit a szolgáltatásba történő regisztrációt megelőzően a regisztrációs oldalon is elérhetővé tett, (iii) minden európai magánszemélynek, beleértve a nem felhasználókat is jogot biztosít arra, hogy egy online, könnyen hozzáférhető űrlapon keresztül jelezze, ha nem kívánja személyes adatainak az algoritmusok tanítása céljából történő kezelését, (iv) bevezetett egy üdvözlő oldalt a szolgáltatás olaszországi újraindításához, amely tartalmaz egy linket a felhasználóknak szóló új adatkezelési tájékoztatóra, valamint a nem felhasználóknak a személyes adataiknak az algoritmusok tanítása céljából történő kezeléséről szóló adatkezelési tájékoztatóra, (v) olyan mechanizmusokat vezetett be, amelyek lehetővé teszik az érintettek számára, hogy kérjék a pontatlannak ítélt információk törlését, ugyanakkor jelezte, hogy a pontatlanságok helyesbítése jelenleg technikailag nem megoldható, (vi) a felhasználóknak szóló tájékoztatóban egyértelművé tette, hogy továbbra is kezel bizonyos személyes adatokat, hogy lehetővé tegye a szolgáltatásainak szerződéses alapon történő teljesítését, valamint a felhasználók személyes adatait az algoritmusok tanítása tekintetében jogos érdeke jogalapján kezeli (azzal, hogy a felhasználók kérhetik, hogy személyes adataikat ne kezeljék az algoritmus tanítása céljából), (vii) az olaszországi regisztrált felhasználók számára fenntartott üdvözlőoldalon egy külön gombot helyezett el, amellyel a felhasználók megerősíthetik, hogy a szolgáltatáshoz való hozzáférés előtt betöltötték 18. életévüket, vagy a 13. életévüket és az adatkezeléshez szüleik vagy gyámjuk hozzájárult, valamint a szolgáltatás regisztrációs oldalán a születési dátum megadására vonatkozó információ kérése beépítésre került a 13 év alatti felhasználók hozzáférésének megakadályozása érdekében, valamint a 13 és 18 év közötti felhasználók esetében a szülők vagy gyámok által adott hozzájárulás megerősítésének kérésére kerül sor.

[69] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490 (2023. 08. 04.).

A ChatGPT felhasználói részére szóló adatkezelési tájékoztatás[70] és a nem felhasználók részére szóló tájékoztatás[71] véleményem szerint több adatvédelmi kérdést felvet:

a) A felhasználóknak szóló adatkezelési tájékoztató az adatok pontossága kapcsán kifejezetten felhívja a figyelmet arra, hogy „*az olyan szolgáltatások, mint a ChatGPT, úgy generálnak válaszokat, hogy elolvassák a felhasználó kérését, és válaszul a kérdésre legvalószínűbben megjelenő szavakat írják meg. Bizonyos esetekben a legvalószínűbben megjelenő szavak nem feltétlenül a legpontosabbak. Ezért kérjük, ne hagyatkozzon a modelljeink kimeneteinek tényszerűen pontos voltára. Ha azt észleli, hogy a ChatGPT válasza tényszerűen pontatlan információkat tartalmaz Önről, és szeretné, ha kijavítanánk a pontatlanságot, akkor a dsar@openai.com címre küldhet helyesbítési kérelmet. Tekintettel a modelljeink működésének technikai összetettségére, előfordulhat, hogy nem minden esetben tudjuk kijavítani a pontatlanságot. Ebben az esetben az alábbi űrlap kitöltésével kérheti, hogy távolítsuk el személyes adatait a ChatGPT kimenetéből.*”[72]

Kérdés, hogy a fentiek szerinti tájékoztatás és a mögötte lévő, bizonyosan fejlett technikai háttér eleget tesz-e a GDPR követelményeinek legfőképpen a pontosság elve, valamint az érintetti jogok – jelen esetben a helyesbítéshez való jog – biztosítása tekintetében. A „*helyesbítéshez való jog a pontosság elvével áll szoros kapcsolatban*”[73] és az „*adatkezelőknek már a személyes adatok felvételekor meg kell tenniük azokat az intézkedéseket, amelyek garantálják, hogy a kezelt információk pontosak lesznek, ezt egészíti ki az érintett joga adatai helyesbítéséhez*”[74].

A GDPR 5. cikk (1) bekezdés d) pontja úgy fogalmaz, hogy „*minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék*”, így álláspontom szerint ennek a fentiek szerinti tájékoztatás eleget tehet, egyidejűleg célszerűnek látszik egy olyan álláspont kialakítása, amely a szabályoknak való megfelelés számonkérésével együtt konstruktív módon

[70] https://openai.com/policies/privacy-policy (2023. 08. 04.).

[71] https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed (2023. 08. 04.).

[72] https://openai.com/policies/privacy-policy (2023. 08. 04.) Lásd az adatkezelési tájékoztató 4. pontját.

[73] Péterfalvi Attila–Révész Balázs–Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2021, elektronikus változat 7.2.1.2 pontja.

[74] Péterfalvi Attila–Révész Balázs–Buzás Péter (szerk.): op. cit., 7.2.1.2 pont.

áll hozzá az MI használatához, azaz a GDPR-beli szabályok kellőképpen flexibilis értelmezését adja olyan módon, hogy egyébként nem sérülnek az adatvédelmi szabályok. Ehelyütt arra gondolok, hogy amennyiben észszerűen indokolható módon valóban nem valósítható meg technikailag a helyesbítés jogának biztosítása[75] (külön vizsgálandó, hogy miért nem valósítható meg), akkor kellő alternatíva lehet az adatok törlésének megfelelő biztosítása.

b) Az adatkezelési tájékoztató 8. pontja szerint az adatokat addig őrzi meg az adatkezelő, amíg arra szüksége van ahhoz, hogy a szolgáltatást az érintett részére nyújtani tudja, vagy egyéb jogos üzleti célokból, például viták rendezése céljából, biztonsági okokból, illetve jogi kötelezettségei teljesítése érdekében. A tájékoztató hozzáteszi, hogy az adatmegőrzés ideje több tényezőtől függ, például az adatok mennyiségétől, jellegétől és érzékenységétől, stb.

Kérdéses, hogy egy ilyen általánosan megfogalmazott tájékoztatás mennyiben felelhet meg az adatvédelmi követelményeknek, különösen az átláthatóság és a korlátozott tárolhatóság elvének. Álláspontom szerint indokolható, hogy ennél konkrétabb és pontosabb tájékoztatás lenne szükséges, így például, amennyiben jogi kötelezettségre hivatkozik az adatkezelő, akkor elvárható, hogy megnevezze a konkrét jogi kötelezettséget, illetve fejtse ki, hogy milyen módon függ az adatmegőrzési ideje az általa felsorolt tényezőktől.

c) Ami talán az egyik legérdekesebb kérdés az az, hogy milyen módon biztosított, hogy az eddig begyűjtött személyes adatok kezelése jogszerű volt a megszerzésük pillanatától kezdve. A nem felhasználóknak szóló tájékoztató[76] szerint a személyes adatok ChatGPT tanítása céljából történő gyűjtésére három forrásból kerül sor, amelyek a következők: (i) a nyilvánosan elérhető Internet tartalom, (ii) harmadik felektől beszerzett adatok és (iii) a felhasználók és az emberi trénerek által megadott adatok. A tájékoztató célja, hogy az Internetről begyűjtött adatokkal kapcsolatosan adjon útmutatást.

A tájékoztató szerint az OpenAI csak az Interneten szabadon elérhető, nyilvánosan hozzáférhető információkat használ – például nem keres „fizetős falak mögötti” vagy a "dark

[75] Álláspontom szerint esetről esetre külön vizsgálandó, hogy miért nem kivitelezhető technikailag az adatok helyesbítése és a választól függően lehetnek olyan helyzetek, amikor elfogadható, hogy az adatkezelő nem tud helyesbítést kezelni, csak törlést.

[76] A dokumentum címe az, hogy „*How ChatGPT and Our Language Models Are Developed*” (azaz „Hogyan fejlesztjük a ChatGPT-t és a nyelvi modelljeinket”).

webről" származó információkat – és szűrőket alkalmaz, továbbá eltávolítja azokat az információkat, amelyekből nem szeretné, hogy a szoftverei tanuljanak, illetve amelyeket nem szeretnének válaszokban viszont látni, amilyen például a gyűlöletbeszéd, a felnőtteknek szóló tartalom, az elsősorban személyes adatokat összesítő oldalak és spamek. Egyebekben az információkat arra használja az adatkezelő, hogy tanítsa a modelljeit. A tájékoztató tartalmazza továbbá, hogy az Interneten található adatok nagy része emberekre vonatkozik, így a tanításra használt adatok mellékesen személyes adatokat is tartalmaznak, egyben hangsúlyozza, hogy az adatkezelő nem keres aktívan személyes adatokat a nyelvi modellek tanításához.

Külön felhívja a figyelmet a tájékoztató arra, hogy az adatkezelő nem használ és nem is fog felhasználni semmilyen, a modell tanításához használt információkban szereplő személyes adatot arra, hogy profilokat készítsen emberekről, kapcsolatba lépjen velük, reklámot küldjön részükre, vagy megpróbáljon eladni nekik valamit.

Ezen túlmenően azt is tartalmazza a tájékoztató, hogy a nagy nyelvi modellek számos olyan felhasználási móddal rendelkeznek, amelyek jelentős előnyökkel járnak, és már most is segítik az embereket például a tartalomkészítésben, az ügyfélszolgálat javításában, a szoftverfejlesztésben, az oktatás igényekre szabásában, a tudományos kutatás támogatásában, és ezek az előnyök nem valósíthatók meg a modellek tanításához szükséges nagy mennyiségű információ felhasználása nélkül. Az adatkezelő egyúttal hangsúlyozza, hogy a modell tanítására használt információk felhasználásának nem célja, hogy negatív hatással legyen az egyénekre, és a tanításra használt információk forrásai egyébként is nyilvánosan elérhetők; és mindezen szempontokra tekintettel a tanításra használt információkban szereplő személyes adatok gyűjtését a GDPR szerinti jogos érdekre alapozza, végül azt is kijelenti az adatkezelő, hogy adatvédelmi hatásvizsgálatot készített a megfelelés biztosítása végett.

Az OpenAI a tájékoztató "*Hogyan felel meg a ChatGPT fejlesztése az adatvédelmi törvényeknek?*" című részében azzal kívánja igazolni, hogy jogszerűen használta fel az emberek adatait, hogy a) a chatbotját hasznos programnak szánta, b) nem volt más választása, mivel az MI-technológia megalkotásához rengeteg adatra volt szükség, és c) nem akarta, hogy bármilyen negatív hatással legyen az egyénekre[77].

[77] Lomas, Natasha: ChatGPT resumes service in Italy after adding privacy disclosures and controls, 2023. április 28. (https://techcrunch.com/2023/04/28/chatgpt-resumes-in-italy/?guccounter=1) (2023. 08. 04.).

Álláspontom szerint nem látható, hogy milyen módon igazolja azt az OpenAI LLC, hogy az Internetről korábban begyűjtött adatok kezelése már a beszerzésük pillanatában jogszerű volt. Ha ezt nem tudja igazolni az adatkezelő, akkor végső esetben az adatok törlése is elrendelhető lehet, ami önmagában igencsak komoly szankció, hiszen a nyelvi modell lényege, hogy az az abba betáplált adatokból tanul és fejlődik. Ha újra kellene kezdeni a tanítást, az komoly nehézségeket okozhat az OpenAI számára és bizonyosan sok értékes tanulási tapasztalat is megsemmisülne.

4.6.1 A ChatGPT ügy eddigi tapasztalatai

A ChatGPT esetében álláspontom szerint felmerül annak lehetősége, hogy az adatkezelő feltehetően nem vagy nem megfelelően alkalmazta a beépített és alapértelmezett adatvédelem elvét akkor, amikor megkezdte az Interneten nyilvánosan elérhető információk (köztük számos személyes adat) gyűjtését és azok mesterséges intelligencia alapú nagy nyelvi modell tanítására történő felhasználását.

Nem kétségesen szükséges, hogy az adatkezelőt, a szoftver fejlesztőjét a jószándék vezérelje egy-egy adatkezelési tevékenység körülményeinek kialakításakor, azonban ez önmagában nem elégséges ahhoz, hogy az adatkezelés jogszerű legyen. A beépített és alapértelmezett adatvédelem elve nem vitatható módon megkívánja az alapelveknek és a GDPR előírásainak való megfelelést már az adatkezelés megtervezésének fázisában, beleértve a kockázatok azonosítását és kiértékelését, a kockázatokkal arányos megfelelő technikai és szervezési intézkedések megtételét, az érintettek jogainak folyamatos és hatékony megóvását szolgáló garanciák adatkezelésbe való beépítését; mindennek pedig annyival minden bizonnyal nem lehet megfelelni, hogy az adatkezelő kijelenti, hogy nem akart rosszat és csakis a jószándék vezette.

A fenti 3.6 pont a)-j) pontjaiban írt feltételek figyelembe vétele még inkább fontos egy olyan adatkezelés esetén, mint, amilyen például egy nagy nyelvi modell használatával megvalósuló adatkezelés, hiszen az olyan kockázatokat is jelenthet, amelyek egy egyszerűbb adatkezelés esetében nem állnak fenn.

A GDPR egyik alapvető követelménye, hogy minden esetben, amikor személyes adatok kezelésére kerül sor, az adatkezelésnek megfelelő jogalapja kell legyen[78]. A megfelelő jogalap biztosítása az adatkezelő kötelezettsége, annak megléte a jogszerű adatkezelés szükséges, de

[78] GDPR 6. cikk.

nem elégséges feltétele. Ez nincs és nem is lehet másként akkor sem, ha mesterséges intelligenciát használnak személyes adatok kezelésére.

Általánosságban megállapítható, hogy egy magán társaság által készített és személyes adatok kezelésére is használt nagy nyelvi modell általi adatkezelés jogalapja nagy valószínűséggel vagy az érintett hozzájárulása lehet, vagy az adatkezelő (és/vagy harmadik fél) jogos érdeke (utóbbi jogalap esetében kivéve, ha például az érintett gyermek). Ezt erősíti meg Lilian Edwards, a Newcastle Egyetem oktatójának véleménye is, aki szerint a ChatGPT esetében lényegében két lehetőség van: beszerezni az érintett hozzájárulását (amit az OpenAI nem tett meg) vagy arra hivatkozni, hogy az adatkezelő jogos érdekében áll az adatok kezelése, ami nagyon nehéz[79].

A Garante fent említett végzésében kötelezte az OpenAI LLC-t, hogy törölje a szerződés teljesítésére való utalást, és az érintett hozzájárulására, vagy a GDPR-ban meghatározott jogos érdekre alapozza az adatkezelést. Utóbbi az adatkezelő, illetve harmadik fél jogos érdekét jelentheti.

Az OpenAI LLC az Internetről begyűjtött, a modell tanítására használt személyes adatok kezelésére vonatkozó tájékoztatójában foglaltak szerint az adatkezelő jogos érdeke a személyes adatoknak a modell tanítására való felhasználása. Érdekesség, hogy a tájékoztató magát a jogos érdeket nem nevezi meg (jóllehet a GDPR szerint meg kellene[80]), csupán arra hivatkozással nevesíti a jogos érdeket, hogy a szoftver hasznos, azzal nem szándékoznak senkinek sem ártani, a begyűjtött adatok a begyűjtésük előtt is nyilvánosak voltak és az adatokat nem használják másra, mint a modell tanítására.

Véleményem szerint erősen kérdéses, hogy mindez elegendő-e a megfelelő jogalap biztosításához, hiszen önmagában az, hogy egy személyes adat nyilvánosan elérhető az Interneten még nem jelenti azt, hogy az szabadon kezelhető a vonatkozó adatvédelmi szabályok betartása nélkül, ahogyan önmagában az sem tűnik elegendőnek a jogszerűség igazolására, hogy az adatkezelésnek nem célja, hogy negatív hatással legyen az érintettekre, továbbá, hogy

[79] Burgess, Matt: ChatGPT Has a Big Privacy Problem, Italy's recent ban of Open AI's generative text tool may just be the beginning of ChatGPT's regulatory woes, 2023. április 4. (https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/) (2023. 08. 14.).

[80] GDPR 13. cikk (1) bekezdés d) pont, illetve 14. cikk (2) bekezdés b) pont. Jelen esetre az utóbbi jogszabályhely vonatkozik, tekintettel arra, hogy a személyes adatokat nem közvetlenül az érintettől szerezték meg, hanem az Internetről.

az adatkezelő nem használja arra az adatokat, hogy például reklám céllal kapcsolatba lépjen az érintett személyekkel, hiszen az önmagában jogellenes adatkezelés lenne és attól, hogy az adatkezelő nem folytat az eredeti céltól eltérő célból jogellenesen adatkezelést, nem következik az, hogy az eredeti célból végzett adatkezelés csakis jogszerű lehet.

A fent jelzettek szerint egyidejűleg az is kérdéses, hogy még ha meg is állna a jogos érdek a jövőre nézve, hogyan igazolja azt az adatkezelő, hogy a korábban – a jogos érdeken alapuló adatkezelés megkezdését megelőzően – begyűjtött személyes adatok tekintetében fennáll a jogszerű adatkezelés.

A norvég adatvédelmi hatóság nemzetközi ügyekért felelős tisztviselője, Tobias Judin megfogalmazása szerint: "*Ha az üzleti modell csupán abból állt, hogy az Internetet átfésülték, csak, hogy minél több adatot találjanak, akkor itt valóban jelentős probléma lehet.*", hozzátéve, hogy ha egy modell olyan adatokra épül, amelyeket esetleg jogellenesen gyűjtöttek, az kérdéseket vet fel azzal kapcsolatban, hogy jogszerűen használhatja-e bárki az ilyen eszközöket[81].

Ehelyütt ismét az látszik beigazolódni, hogy fontos kellő időben, jelesül az adatkezelés megkezdését megelőzően átgondolni és megtervezni magát az adatkezelést, mert egyfelől nem lehet a megtörténteket meg nem történtté tenni, másfelől utólag nem lehetséges jogalapot biztosítani egy eredetileg jogellenesen begyűjtött személyes adat kezeléséhez.

5. Befejezés

A fentebb ismertetett döntések alapján alább összefoglalom az adatkezelők, illetve adatfeldolgozók számára adódó főbb tanulságokat, majd kitérek arra, hogy álláspontom szerint szükséges-e a GDPR módosítása az MI jelentette új és folyamatosan fejlődő technológiákra tekintettel.

5.1 Az MI-re vonatkozó hatósági döntések tanulságai

A GDPR egyes rendelkezései szoros összefüggésben vannak egymással, számos rendelkezés nem különíthető el a többitől, mert együtt alkotnak egy koherens szabályozást. Itt gondolhatunk például arra, amit a fent nevezett ügyek kiválóan megmutattak, jelesül azt, hogy önmagában ezen néhány ügyből levonhatók azok a tanulságok, amelyek bármilyen MI alapú adatkezelés esetén is irányadóak, amelyeket az alábbiak szerint foglalok össze:

[81] Burgess, Matt: op. cit.

- már az algoritmusok fejlesztésénél figyelembe kell venni az alapelveket (pl. átláthatóság, adatminimalizálás, pontosság), gondoskodni kell az érintetti jogok gyakorolhatóságáról, azonosítani kell a kockázatokat és azok kezelésére megfelelő intézkedéseket kell tenni. Amennyiben a fejlesztő adatfeldolgozói pozícióban van, akkor – annak ellenére, hogy a 25. cikk csak az adatkezelőre ír elő kötelezettségeket –, mindenképpen célszerű tekintetbe vennie a beépített és alapértelmezett adatvédelem elvét, mert a termékét megvásárló adatkezelő ügyfele köteles előzetesen tájékozódni a szoftverrel kapcsolatban és csak olyan programot használhat, amely megfelel az alapelveknek (másképpen fogalmazva, prudens módon eljáró adatkezelők esetén csak akkor fogja tudni eladni a szoftvert az adatfeldolgozó fejlesztő, ha igazolni tudja azt, hogy a szoftver eleve úgy lett tervezve, hogy az megfeleljen többek között a 25. cikk szerinti előírásoknak),
- adatvédelmi hatásvizsgálatot kell készíteni, ami önmagában segíthet a kockázatok valószínűségének és súlyosságának/hatásának felmérésében. Jóllehet ez a kötelezettség is az adatkezelőt terheli, a szoftver fejlesztője elkészítheti a termékéhez az adatvédelmi hatásvizsgálatot annak érdekében, hogy igazolni tudja a megfelelést az ügyfelei felé,
- ha gépi tanulásra képes MI tervezett alkalmazásáról van szó, külön figyelmet kell fordítani arra, hogy a gyűjtött adatok pontosak és a célhoz mérten relevánsak legyenek, továbbá, hogy valóban csak a szükséges adatokat szerezzék be és a szükséges ideig kezeljék,
- fontos az érthető tájékoztatás arról (is), hogy hogyan működik az algoritmus (kizárólag automatizált döntéshozatal esetén tájékoztatás szükséges az alkalmazott logikáról, a végzett adatkezelés jelentőségéről, és az érintettre nézve várható következményekről),
- szükséges az algoritmus „kimenetének” folyamatos ellenőrzése annak érdekében, hogy az esetleges hibák, torzítások, diszkriminatív döntések megelőzhetők, illetve kijavíthatók legyenek.

A fenti követelmények mindegyike levezethető a GDPR 25. cikkéből, hiszen az abban megfogalmazott követelmény jelenti többek között az 5., 6-9., 12-22., 24., 32. és 35-36. cikkeknek való megfelelést.

5.2 Következtetések

A mesterséges intelligencia révén megvalósuló adatkezelésnek a GDPR és a gyakorlat szempontjából történő vizsgálata alapján jelen írással célom volt választ adni arra a kérdésre, hogy az MI használatával összeegyeztethető szabályozást tartalmaz-e a GDPR, avagy vannak olyan szabályok, amelyek kiigazítása szükségesnek mutatkozik.

Kétségtelen, hogy érezhető bizonyos feszültség a GDPR előírásai (különösen az átláthatóság, adattakarékosság, pontosság és korlátozott tárolhatóság elvei), az azoknak való megfelelés és az MI modellek működéséből fakadó sajátosságok között, aminek következtében az adatkezelőnek azt megelőzően, hogy MI alapú modell révén történő adatkezelésbe fog, már a tervezés fázisában kiemelt körültekintéssel kell eljárnia.

Ugyanakkor aligha lehet kétséges, hogy bárki azt az álláspontot képviselné, hogy a GDPR alapelveiből részben vagy egészben fel kellene áldozni egyeseket azért, hogy szabadabb teret engedjünk a technológiai fejlődésnek. Ki állítaná azt, hogy legyen kevésbé tisztességes, kevésbé átlátható az adatkezelés, ha MI általi adatkezelésről van szó? Vagy azt, hogy MI általi adatkezelés esetében nem olyan fontos a célhoz kötöttség elve, az adatok lehetnek pontatlanok és a korlátozott tárolhatóságot sem kell annyira komolyan venni, illetve nem kell olyan szintű körültekintéssel eljárni, amilyet a 25. cikk előír? Mindezek önmagukban is feltehető jogos kérdések, azonban, ha azokat abba a kontextusba helyezzük, hogy egy fejlett és kevésbé ismert technológia éppen annak sajátosságai és képességei miatt fokozott kockázatokat jelenthet az érintettekre nézve, akkor még inkább kirajzolódik ezen kérdések aktuális volta, hiszen igenlő válasz esetén egy fokozott kockázattal járó adatkezelésre alkalmaznánk alacsonyabb védelmi szintet, ami álláspontom szerint nem volna helyes[82].

Véleményem szerint inkább a GDPR meglévő szabályainak megfelelő alkalmazására szükséges figyelmet fordítani, főképpen adatkezelői (adatfeldolgozói) oldalon, azonban fontos

[82] Az Európai Bizottság által felállított Mesterséges Intelligencia Magasszintű Szakértői Csoport is hangsúlyozza a következő négy etikai elv kiemelt szerepét megbízható MI használata tekintetében: (i) az emberi autonómia tiszteletben tartása, (ii) sérelem okozásának elkerülése, (iii) tisztességesség, (iv) átláthatóság, megfelelő tájékoztatás nyújtása.
Az Information Commissioner's Office is hangsúlyozza, hogy a technológia lehet új, de az adatkezelés alapelvei maradnak ugyanazok, és a kezdetektől fontos a beépített és alapértelmezett adatvédelem elvének megfelelően eljárni, ami nem választható, mivel a jog maga ezt követeli meg. (https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/ (2023. 08. 19.).

az is, hogy a jogalkalmazó a GDPR által kijelölt keretek között kellő észszerűséggel értelmezze az előírást, ezzel együtt az átláthatóság csökkentése, a kisebb biztonság, „*[a]z érintetti jogok kiüresítése nem lehet célja és eredménye a fejlődésnek*.”[83]

Ahogyan az Európai Parlament Kutatószolgálata is megállapította egy tanulmányában, „*vannak olyan módok az adatvédelmi elvek értelmezésére, alkalmazására és fejlesztésére, amelyek összhangban vannak a mesterséges intelligencia és a nagy adathalmazok előnyös felhasználásával.*”[84].

Egyetértve az Európai Parlament Kutatószolgálatával, kívánatos és fontos, hogy az Európai Adatvédelmi Testület, illetve az egyes hatóságok adjanak ki tájékoztató anyagokat az MI használatával kapcsolatban, amelyek hasznos információkkal szolgálhatnak az adatkezelők, adatfeldolgozók részére és amelyek a GDPR egyes előírásainál konkrétabb információkat adnak arról, hogy hogyan lehet megfelelő módon használni egyes MI technológiákat[85]. Nem vitás, hogy az adatkezelők, adatfeldolgozók felelőssége a megfelelő adatkezelés kialakítása, ugyanakkor az ilyen iránymutatások végső soron mindenki érdekét szolgálnák, beleértve az érintetteket és szélesebb értelemben véve a társadalmat is, figyelembe véve azt is, hogy az MI használatának számos hasznos felhasználási módozata képzelhető el.

Összefoglalva, megítélésem szerint az MI technológiára tekintettel nem szükséges a GDPR módosítása, egyidejűleg célszerűnek látszik a hatósági tájékoztatók kiadása mellett az is, hogy a tagállamok éljenek a fenti 3.5 pontban utalt jogszabályi felhatalmazással az MI modellel begyűjtött adatok tudományos kutatási és statisztikai célú felhasználhatósága vonatkozásában ezzel is segítve a technológiai fejlődést és annak a köz érdekében történő hasznos alkalmazását.

A jelen dolgozat szövegének lezárására 2023. szeptember 8-án került sor, az ezen időpontot követő fejleményekre szükségképpen nem terjed ki.

[83] Lásd Budapest Bank határozat 29. o.

[84] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530 – June 2020, Executive summary, II. o.

[85] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, op. cit., Executive summary, III. o.

Irodalomjegyzék

Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához, WP251.rev.01

Európai Adatvédelmi Testület 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat

Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról, 2021. június 18.

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530 – June 2020

Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, 4 September 2017 (https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf)

Guidance on AI and Data Protection, Information Commissioner's Office 16 March 2023 (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/)

Péterfalvi Attila–Révész Balázs–Buzás Péter (szerk.): Magyarázat a GDPR-ról. Wolters Kluwer, Budapest, 2021

https://openai.com/policies/privacy-policy

https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed

Lomas, Natasha: Italy orders ChatGPT blocked citing data protection concerns, 2023. március 31. (https://techcrunch.com/2023/03/31/chatgpt-blocked-italy/)

Lomas, Natasha: ChatGPT resumes service in Italy after adding privacy disclosures and controls, 2023. április 28. (https://techcrunch.com/2023/04/28/chatgpt-resumes-in-italy/?guccounter=1)

Lomas, Natasha: Replika, a ‘virtual friendship’ AI chatbot, hit with data ban in Italy over child safety, 2023. február 3. (https://techcrunch.com/2023/02/03/replika-italy-data-processing-ban/)

https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

On the Record, Exploring the ethical, technical and legal issues of voice assistants, CNIL (Commission Nationale Informatique et Libertés) (https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_white-paper-on_the_record.pdf)

Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, FRA, European Union Agency for Fundamental Rights, 2019 (https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf)

Think Tank, European Parliament, Artificial Intelligence Act (https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)

Proposal for a Regulation of the European Parliament and of the Council laying down the harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts

Milner-Smith, Helena–Cooper, Dan: Italian Supervisory Authority Fines Foodinho Over Its Use of Performance Management Algorithms, 2021. július 13. (https://www.insideprivacy.com/gdpr/italian-supervisory-authority-fines-foodinho-over-its-use-of-performance-management-algorithms/)

Armstrong, Jonathan–Eyres, Katherine: Client Alert: Italian DPA fines Deliveroo & food delivery start-up over AI algorithm use, 2021. augusztus 4. (https://www.corderycompliance.com/garante-fines-deliveroo/)

Italian Garante Fines Deliveroo 2.5M Euros for Unlawful Processing of Personal Data, 2021. augusztus 5. (https://www.huntonprivacyblog.com/2021/08/05/italian-garante-fines-deliveroo-2-5m-euros-for-unlawful-processing-of-personal-data/)

Lomas, Natasha: Italy's DPA fines Glovo-owned Foodinho $3M, orders changes to algorithmic management of riders, 2021. július 6. (https://techcrunch.com/2021/07/06/italys-dpa-fines-glovo-owned-foodinho-3m-orders-changes-to-algorithmic-management-of-riders/)

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677611

dr. Pók László: Adatvédelmi hatósági eljárások mesterséges intelligencia alkalmazása kapcsán, 2023. május 12. (https://gdpr.blog.hu/2023/05/12/adatvedelmi_hatosagi_eljarasok_mesterseges_intelligencia_alkalmazasa_kapcsan)

dr. Pók László: GDPR bírságok az alkalmazott algoritmusok miatt, 2021. augusztus 27. (https://gdpr.blog.hu/2021/08/27/gdpr_birsagok_az_alkalmazott_algoritmusok_miatt)

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852506

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9808839

Slavova, Dessislava–Kennedy, Alexander–Flakoll, Rita–Orton, Gail–Barbier, Blanche–Negro, Great–Ditri, Ella–Kwiatkowski, Agnes: EU AI Act: Final negotiations can begin after European Parliament vote, 2023. június 23. (https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2023/06/eu-ai-act-final-negotiations-can-begin-after-parliament-vote.html)

Higgins, Tamlin–Jackson, Robin–Korten, Pepijn: The EU AI Act: concerns and criticism, 2023. április 6. (www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2023/04/the-eu-ai-act--concerns-and-criticism.html)

European Parliament Agrees on Position on the AI Act, 2023. június 15. (www.huntonprivacyblog.com/2023/06/15/european-parliament-agrees-on-position-on-the-ai-act/)

A NAIH Budapest Bank ügyben hozott határozata, ügyszám: NAIH-85-3/2022, korábbi ügyszám: NAIH-7350/2021

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2765125

European Digital Rights, Use cases: Impermissible AI and fundamental rights breaches, 2020 augusztus, (https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf)

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252

https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en