ERDÉLYI DÓRA – LEITER MIKLÓS PATRIK

Kérdezz bármit, tudom a választ! – avagy a ChatGPT adatvédelmi kérdései, különös tekintettel a személyes adatok védelmére és a kockázati besorolásra

Ask me anything, I know the answer! – ChatGPT's data protection issues, with a special regard to personal data protection and risk classification

DOI: HTTPS:// DOI.ORG/10.53793/RV.2024.1.4

Absztrakt

Jelen cikkünk témája a ChatGPT, mint nagy nyelvi modell adatvédelmet és kockázati besorolást érintő vizsgálata. Ezen vizsgálódás elengedhetetlen kellékeként először magát a ChatGPT alapjául szolgáló technológiát tekintjük át dióhéjban, beleértve a nagy nyelvi modell működését biztosító és/vagy segítő támogatószolgáltatásokat. Ezen összetett rendszert pedig a GDPR-szabályai segítségével vizsgáljuk, az egyes lényeges adatvédelmi kérdésekre kitérve. Mindezek alapján pedig megkíséreljük behatárolni a kockázati szintet, ami a ChatGPT, mint rendszer veszélyességét jelenti a felhasználókra nézve. Ezután valós jogeseteken keresztül nézzük meg, éles helyzetben, hogy jelen állás szerint milyen megoldásokra lehet számítani a mesterséges intelligencia jogsértő magatartásával szemben. A cikk lényege tehát, hogy szélesebb képet adjon a nagy nyelvi modellek jelenlegi adatvédelmi veszélyeiről, kockázati szintjéről, és azokról a jogi utakról, megoldásokról, amelyek jelen helyzetben a jogalkalmazók kezében vannak a mesterséges intelligencia rendszerekkel szemben. A cikk célja, hogy röviden összefoglalja hol is állunk jelenleg, és egyfajta javaslatot tegyen, merre érdemes tovább haladni.

KULCSSZAVAK: CHATGPT, MESTERSÉGES INTELLIGENCIA, NAGY NYELVI MODELLEK, ADATVÉDELEM, SZEMÉLYES ADAT

Abstract

The topic of this article is the examination of the data protection issues of ChatGPT as a large language model, and its risk classification. Firstly, we are considering an essential accessory to this study that is the underlying technology of ChatGPT itself in its entirety, including the support services that ensure and/or support the functioning of the large language model. Secondly, we are going to look at this complex system through the rules of the GDPR and each of the key data protection issues. Based on all of this, we are trying to narrow down the level of risk chat ChatGPT poses as a system to its users and then we are examining what kind of solutions can we expect from the current state of affairs to deal with the illegal behaviour of artificial intelligence. The purpose of this article is therefore to provide a broader picture of the current data protection threats of the big four models, their level of risk, and the legal avenues and solutions available to law enforcement agencies in the current situation in relation to AI systems.

KEYWORDS: CHATGPT, ARTIFICAL INTELLIGENCE, LARGE LANGUAGE MODELS, DATA PROTECTION, PERSONAL DATA

Bevezetés – A ChatGPT és az adatvédelem

A mai világban is megállja a helyét a mondás, miszerint a tudás hatalom, ezt ChatGPT működése alapján átalakíthatjuk akár arra, hogy az „információ hatalom" vagy „az adat hatalom". A ChatGPT, mint nagy nyelvi modell tanításához felhasznált adatok fellelhetősége, ellenőrzése és azok felhasználása az átlag felhasználó számára nem transzparens. A chatbot használata oly mértékben könnyíti meg a mindennapi

munkát, hogy lassan a már jól megszokott keresőprogramokkal vetekszik népszerűsége. Az előbb említett egyszerűség és népszerűség az egyik legnagyobb veszély akkor, amikor a színfalak mögé nézünk és elolvassuk az „apróbetűs részeket". Felmerülnek olyan kérdések, hogy: „Kinek az adataival dolgozik?" „Meddig tárolja a megszerzett adatokat?" „Az illető hozzájárul-e az adatok megszerzéséhez?" és még sorolhatnánk. Cikkünkben ezen kérdéseket boncolgatjuk. Nem a mindenki számára egységesen elfogadható válasz megtalálásán van a hangsúly, sokkal inkább az egyes problémák bemutatásán, azok technikai és jogi megközelítésén. A cikk egy technológiai és egy jogi-adatvédelmi részből áll. A technológiai áttekintést a mesterséges intelligencia meghatározásával indítjuk, majd pedig ebből kiindulva lépésről lépésre eljutunk a ChatGPT-ig. Ezen lépések során érinteni kívánjuk többek között a gépi tanulást, a mélytanulást, a neurális hálót, a modellt és a különböző tanítási technikákat. A végére pedig maga a GPT, illetve a ChatGPT lehetséges problémái, hibái kerülnek tárgyalásra. Ezt követően a GDPR és a ChatGPT működése során felmerülő jogi kollíziót vesszük górcső alá, kiegészítve az egyes tagállamok ChatGPT által kiváltott reakcióival.

Mi a ChatGPT?

Mesterséges intelligencia és gépi tanulás – mi különbözteti meg őket?

A mesterséges intelligencia fogalmának meghatározását az AI Act módosított változatában használt definícióval határozzuk meg, ami nem más, mint: „*(AI rendszer): olyan gépi alapú rendszer, amelyet úgy terveztek, hogy különböző szintű autonómiával működjön, és amely explicit vagy implicit előrejelzésekre, ajánlásokra vagy döntésekre képes, amelyek befolyásolják a fizikai vagy virtuális környezetet*" (AI Act). A mesterséges intelligencia célját ugyanakkor több vezető mesterséges intelligencia kutató cég szerint az emberi intelligencia kognitív képességekkel bíró gépek létrehozására való törekvése jellemzi. Ezek a képességek az IBM szerint: az arc- és beszédfelismerés, a döntéshozatal, a fordítás; a Google idesorolja még ezen kívül a látást, az adatelemzést, az ajánlások adását. Ezek mind egy-egy területét vagy szeletét adják a mesterséges intelligenciának, mint interdiszciplináris területnek. Ahhoz, hogy ezekkel a képességekkel egy mesterséges intelligencia rendelkezzen, többféle megközelítésre van szükség, ezért a mesterséges intelligencián belül 6 klasszikus területet különböztetünk meg:

1. Gépi tanulás
2. Gépi látás
3. Neurális hálózatok
4. Mélytanulás
5. Természetes nyelvi feldolgozás
6. Kognitív számítástechnika.

A gépi tanulás a mesterséges intelligencia olyan részhalmaza, amely automatikusan képessé tesz egy gépet vagy rendszert arra, hogy tapasztalataiból tanuljon és fejlődni tudjon. A nagymennyiségű adat elemzésére a gépi tanulás explicit programozás helyett algoritmusokat használ a felismerésekből való tanulásra, valamint a döntések meghozatalára. A gépi tanulási algoritmusok idővel javítják teljesítményüket, ahogyan egyre több adatot használnak fel. Ha az emberi kognitív képességekre szeretnénk vele reflektálni, akkor a gépi tanulás egyértelműen megoldással szolgál az adatelemzéshez, ajánlások megtételéhez.

A mesterséges intelligencia alapvető célja, hogy az ember kognitív képességeinek teljes repertoárját a gépi működés által képezze le. Ehhez képest a gépi tanulás egy bizonyos területnek csak egy-egy szeletét képes lehetővé tenni. Ezért a mesterséges intelligencia tágabb fogalom, amelyen belül a gépi tanulás elhelyezkedik.

A gépi tanulás, neurális hálózatok, mélytanulás elhatárolása

A mesterséges intelligencia működésén belül többféle megoldást találunk, amely lehetővé teszi a rendszer működését. Ezeket úgy kell elképzelni, mint egymásba ágyazott megoldásokat, elveket. Az egyik ilyen megoldás a neurális háló. Ez a név akár a biológiából is ismerős lehet, hiszen az emberi agyat, az idegrendszert alapul véve végzi el a szükséges számításokat. Természetesen ezekből a hálókból többféle létezik, amelyeket többek között a felépítés, a mélység, az információ iránya és egyéb tényezők alapján különböztetünk meg. Más neurális hálózat, más megoldást kínál bizonyos problémákra, ezek a megoldások a gépi tanulás és a mélytanulás. A gépi tanuló algoritmusok családján belül helyezkedik el a mélytanulás is, amely egy olyan vállfaja a gépi tanulásnak, ahol az adott mélytanuló mesterséges intelligencia önmagától, külső segítség nélkül fedezi fel a tanulóadatokban lévő különböző mintákat, szabályosságokat. Ez csak bonyolultabb felépítésű, több rétegű neurális hálóval lehetséges, mint a gépi tanulás esetén, ahol a gépi tanuló rendszer címkézés segítségével tanul.

Architechtúrák és modellek – mik ezek?

A mélytanulás – ahogy fent írtuk – neurális hálóból épül fel, ezen neurális hálók építőkövei a következők:

1. bemenet

2. súly
3. átviteli függvény
4. aktiválási függvény
5. torzítás.

Ezekből az építőkövekből többféle felépítésű neurális hálózat (architechtúra) hozható létre attól függően, hogy milyen problémát szeretnénk megoldani, milyen felhasználásban gondolkodunk. Léteznek úgynevezett szabványos neurális hálózat architechtúrák, avagy neurális hálózat felépítési tervek.

A neurális hálózat architechtúráktól részben el kell különíteni a modelleket, hiszen a gépi tanuló modell, már a tanult adatok alapján képes előrejelzést készíteni, döntést hozni új, korábban nem látott adatkészletből. A gépi tanuló modell megalkotása magában foglalja egy neurális hálózat architechtúra elkészítését, majd egy adatkészlet alapján történő betanítását, addig a pontig, ahonnan már önállóan és megbízhatóan el tudja végezni feladatát.

Ezek után rátérhetünk a foundation model, avagy az *alapmodell* kérdésére. Az AI Act módosított változata kitér az alapmodell meghatározására is: *„Az alapmodellek új keletű fejlődés, amelyben a mesterséges intelligenciamodelleket olyan algoritmusokból fejlesztik ki, amelyek célja a kimenet általános és sokoldalúságának optimalizálása. Ezeket a modelleket gyakran adatforrások széles skáláján és nagy mennyiségű adaton képzik ki, hogy a downstream feladatok széles skáláját végezzék el, beleértve olyanokat is, amelyekre nem kifejezetten fejlesztették és képezték ki őket…[…]”* (AI Act. (60e)). Ez alapján elmondhatjuk, hogy az alapmodell olyan neurális hálózat, amelyet általában nyers adatokon képeznek ki, felügyelet nélküli tanulással, és többféle feladat elvégzésére adaptálható, olyanokra is, amelyekre célzottan nem fejlesztették ki őket.

A *transformer modell* egy neurális hálózati architektúra, amely képes automatikusan átalakítani egy adott típusú bemenetet egy másik típusú kimenetté. A kifejezést egy 2017-es Google-dokumentum alkotta meg, amely megtalálta a módját egy neurális hálózat betanításának az angolról franciára való fordításra, és a többi neurális hálózat képzési idejének egynegyedével. A transformer működését néhány mondatban a következőképpen foglalhatjuk össze: a transformer alapfelépítése szerint kódoló, és dekódoló részre bontható. Két alapvető fázisa van a modell tanításának. Az első fázisban egy transformer nagy mennyiségű címkézetlen adatot dolgoz fel, hogy megtanulja a nyelv szerkezetét vagy egy jelenséget. A modell betanítása után hasznos lehet finomhangolni egy adott feladathoz, ez a második fázis.

Az modellek tanítási technikái – hogyan jön létre egy modell?

Láttuk, hogy a neurális hálózat arhcitechtúrát megkell alkotni és be kell tanítani, hogy így már alapmodellként kezelhessük tovább.

Előtanítás

Az előtanítás célja, hogy nagy mennyiségű adat alapján a modell megtanulja megjósolni a következő szót (nagy nyelvi modellek esetében). Ebben a fázisban a modell még nem tanul speciális feladatot, csupán a következő szó megjóslásának módját tanulja meg, egy adott szövegkörnyezetben. Ez a folyamat többféle tanítási mechanizmus szerint történhet, azonban a GPT esetében az autoregresszív tanítási módot használják, vagyis a modellnek úgy kell kitalálnia a következő szót, hogy egy adott mondatban nem látja a szöveg folytatását, így az előző szavakból kell kiindulnia. Például a ChatGPT-nek leírunk egy fél mondatot, majd azt befejezi: „A macska fel van” – a ChatGPT befejezte: „ A macska fel van készülve a kalandra”. Ezzel a fázissal létre lehet hozni a neurális hálóból az alapmodellt, tehát a transformer alapú neurális hálóból itt kapjuk meg a GPT-t, hiszen az előtanítási fázis elegendő, hogy generatív is legyen, de még nem lehet vele „csevegni”.

Finomhangolás

Az előtanítás után a kezünkben van egy úgynevezett PLM (Pre-trained language model), egy általános nyelvi tudással rendelkező modell. Ha konkrét feladatokra szeretnénk használni, akkor finomhangolnunk kell, amihez egyébként már jóval kevesebb adatra van szükség, mint az előtanításhoz. Ennek során egyrészt plusz feladatspecifikus rétegeket adhatnak a modell neurális hálózatához, illetve egy kisebb adatkészlettel betanítják kimondottan egy konkrét feladatra. A GPT így tanult meg kvázi chatbotként beszélgetni, mivel alapjában véve a GPT csak egy szöveggeneráló, szöveg értelmező és fordító modell.

Generatív modell

A generatív modellek lényege, hogy megértsék, rögzítsék a mögöttes minták eloszlását egy adathalmazból, ezután a modell új adatokat generálhat, amelyek hasonló tulajdonsággal rendelkeznek, mint az eredeti adatok. Fontos, hogy a generatív modell egy alapmodell finomhangolása után nyeri el végső „formáját”, tehát azt a feladatot, amit a

modellnek szánnak, csak a finomhangolás után képes megfelelően ellátni.

ChatGPT

Mindezek fényében leránthatjuk a leplet a ChatGPT-ről, amely nem más, mint egy generatív módon működő, előtanított/általános tudással ellátott, transformer modell, chatbot-ként finomhangolva és működtetve.

A transformer modell kockázatai

A transformer modelleknek is megvannak a maguk kockázatai, amivel számolni kell a modell teljes életciklusában, kezdve a fejlesztéstől, egészen a használatig. Három példát említünk, amikről úgy gondoljuk fajsúlyosak a kockázatok között.

Felmerülhet az úgynevezett *„adatmérgezés"* esete, amikor a támadó rosszindulatú példákat helyez el a modell tanítási adatbázisában, amivel hatással tud lenni a modell minden alkalmazására, oly módon, hogy ezzel a modell teljesítményét rombolja.

Ha az alapmodell például egyetlen vállalat *privát adataival van előtanítva*, akkor fennáll a veszélye, hogy az összes downstream[7] alkalmazásra ezen adatokat felfedje. Például, ha valamit kérdezünk a rendszertől, akkor van rá esély, hogy a modell válasza bizalmas információkat fog tartalmazni az adott vállalatról.

Problémát jelenthet még az úgynevezett *kettős felhasználás***.** Ezt a problémát az alapmodellek rugalmassága adja, vagyis ezek a modellek több feladathoz is viszonylag könnyen alkalmazkodnak. Ez viszont lehetővé teszi, hogy eredeti céljuktól eltérően használják őket. Például egy modell, amely eredetileg kép-szöveg párok előrejelzésével foglalkozott, egy idő után képes volt nagy részletességgel felismerni az arcvonásokat. Az alapmodellek könnyű adaptálhatósága tehát lehetőséget teremthet akár a visszaélésszerű használatra is.

A ChatGPT adatvédelmi vonatkozásairól, figyelembevéve az egyéb ún. támogatószolgáltatásokat

Az előzőleg tárgyalt technikai részben a GPT modell-re helyeztük a hangsúlyt. A modellek neurális háló alapján működnek, amelyeknek nincs a klasszikus értelemben vett memóriájuk. Így máshol kell keresni azt a rendszert, ahol az adatokat tárolják és feldolgozzák, éppen ezért ebben a fejezetben először a ChatGPT működését elősegítő egyéb rendszerekről lesz szó első körben, majd rátérünk jogi értékelésére.

Az OpenAI honlapján öt olyan szereplőt találhatunk (URL1), akiket a cég úgynevezett alfeldolgozókként tüntet fel, azonban ezen öt vállalat tevékenysége nagyon eltér, így adatvédelmi kérdésekben sem lesznek egységesen relevánsak:

- Cloudflare: ezen vállalat az úgynevezett CDN-szolgáltatással segíti az OpenAI-t, vagyis segít a tartalomszolgáltatásában
- Microsoft: a Microsoft az Azure felhőszolgáltatással csatlakozik be az OpenAI szolgáltatási körébe
- OpenAI affilates: szolgáltatások és támogatások
- Snowflake: a Data Lake és a Data Warehousing szolgáltatásokkal támogatja az OpenAI szolgáltatásait
- TaskUS: felhasználói támogatás és felügyelet.

Egyéb közreműködő szolgáltatások

- *Cloudflare:* mint említettük, az OpenAI a Cloudflare egy konkrét szolgáltatását, a CDN-t nevezi meg. A CDN nem más, mint egy szerverhálózat, amelynek célja, hogy a lehető leggyorsabban, megbízhatóbban és biztonságosabban szállítsa a tartalmat az eredeti szervertől a felhasználókhoz. Előnye, hogy az oldalak betöltési idejének gyorsaságát ez biztosítja, ezáltal a világ különböző pontjain sem kell perceket várni a weboldalra míg betölt. Működése lényegében abból áll, hogy bár a weblap tartalmát eredetileg a szolgáltató tárolja, a weboldal tartalmait mégis több szerveren gyorsítótárazzák, vagyis lemásolják és különböző szervereken tárolják. Ezek a szerverek tartalmazhatnak személyes adatot is.
- *Microsoft Azure:* a Microsoft Azure szolgáltatásain keresztül is elérhető az OpenAI több modellje, többek között a GPT 4, GPT – 35 – Turbo, DALL-E. Ezen modellekhez az Azure úgynevezett REST API-val biztosít hozzáférést. Elmondhatjuk, hogy REST API-n keresztül nem tárolódik információ az Azure-szerverein, viszont az OpenAI mégis alfeldolgozóként kezeli, vagyis más módon juthat adat, információ a Microsoft birtokába. Jó példa erre, ha egy felhasználó finomhangolni szeretne egy modellt, akkor a saját adatbázisát az Azure rendszere fogja tárolni. Ebben az adatbázisban nem szükségszerű személyes adat szerepeltetése, de mivel ennek semmi akadálya nincs, így számolni kell vele.

[7] feladat specifikus alkalmazás, egy chatbot esetében „beszélgetés"

- *Snowflake:* ehhez először két fogalmat kell tisztáznunk, az első a Data Lake (magyarosan „adattó"), második a Data Warehouse (magyarosan „adattárház"). Data Lake alatt olyan adattárolót értünk, amely nagymennyiségű nyers adatot tárol, annak eredeti formájában. Itt strukturált, nem strukturált és félig strukturált adatok is vegyesen előfordulhatnak, képi, szöveges és hang adatok is tárolhatók ezen rendszeren belül. Azon vállalatok számára előnyös, amelyek bár sok adatot gyűjtenek, de ezeket nem kell azonnal feldolgozniuk. Data Warehouse esetén már strukturáltabb adatbázisban dolgozhatják fel és kezelhetik adataikat a vállalatok. Az OpenAI a Snowflake szolgáltatását használja, vagyis adatait a Snowflake szerverein tárolja. Minden bizonnyal kombinálják a Data Lake és a Data Warehouse előnyeit, vagyis a nyers, feldolgozatlak adatokat a Data Lake-ben tárolják, majd ezeket egy Data Warehouseban feldolgozzák és előkészítik az elemzéshez vagy a további felhasználáshoz.
- *OpenAI affilates:* jelenleg nincs tudomásunk arról, hogy az OpenAI hirdetett volna meg efféle programot, így ennek most nincs relevanciája, ezért az adatvédelmi vizsgálatból kihagyhatónak ítéljük.
- *TaskUS:* a TaskUS esetében felmerült a kérdés: „mire gondolhatott a költő?", mivel az OpenAI felhasználói támogatást említ, biztonsággal és felügyelettel. A vállalat oldalát böngészve olyan szolgáltatásra bukkantunk, név szerint: Digital Costumer Experience, amelyben a TaskUS az ügyfél-vállalat ügyfeleivel kommunikál, lényegében ügyfélszolgálatként működik. Az oldalon azt írják, hogy hangalapon, e-mail-en, chaten és technikai támogatással lépnek kapcsolatba az ügyfelek ügyfeleivel. Illetve van egy másik szolgáltatás Securing your Content elnevezéssel, ahol többek között felhasználó által generált tartalmak moderálását lehet igénybe venni, de vállalják még a generatív AI által kreált tartalmak moderálását is.

Adatvédelem (GDPR)

Elkezdjük a vizsgálódást az adatvédelem, pontosabban *Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 Rendelete* (URL2) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, a továbbiakban: GDPR szemüvegén keresztül.

Személyes adat

A GDPR 4. cikkének (1) értelmében személyes adatnak csak természetes személlyel összefüggő adatok minősülnek, a szervezetek adatai nem tartoznak a szabályozás alá. Fontosnak tartjuk kiemelni, hogy adatvédelmi jogi szempontból az egyéni vállalkozó is természetes személynek minősül, tehát az egyéni vállalkozóval kapcsolatba hozható adat személyes adat. A személyes adat GDPR szerinti fogalma így hangzik: *„azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható".*

Ha olyan módon kezeljük az adatokat, amelyek megakadályozzák, hogy ezen adatok a természetes személlyel kapcsolatba hozhatók legyenek, úgy megvalósul a GDPR 4. cikkének (5) bekezdése: „álnevesítés": a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

Mindezek alapján az OpenAI esetét megkíséreljük értelmezni, vagyis tárol-e személyes adatot, és melyek azok a vállalatok, amelyek az OpenAI által begyűjtött személyes adatokat tárolják. Fontos azzal kezdeni, hogy az OpenAI honnan és miként gyűjti be a személyes adatokat. Ilyen adatokként azonosíthatók:

a) felhasználói fiók információk
b) felhasználói tartalom
c) kommunikációs információk
d) közösségi média információk
e) tanulóadatok.

Az OpenAI szerverei nyilvánvalóan megkapják ezen adatokat, amennyiben a szolgáltatást használjuk, akár webes felületen, akár applikáción keresztül, hiszen, ha csak a felületet megnézzük, egyfajta történeti sávot találunk, ahol a rendszerrel folytatott, több korábbi kommunikációnk található meg. Így pedig az OpenAI képes a tartalmat személyhez kötni, ezzel személyes adatkezelés folyik.

Úgy gondoljuk logikus lenne, ha ezek a Snowflake szervereire kerülnének, hiszen az OpenAI részére biztosít Data Lake és Data Warehouse szolgáltatást egyaránt. Amint láttuk, a Data Lake-ben lényegében bármilyen adat, bármilyen strukturálatlanul is

eltárolható, így mivel kvázi nincs kezelve, a személyes adat jellegét nem veszíti el, bár ez a szolgáltatás akár több szerveren is megvalósulhat, mégis egyetlen összekapcsolt rendszerként létezik. A feloldást talán a Data Warehouse adhatja, ahol már az adatok egy begyűjtési és tisztítási, feldolgozási szakaszon mennek keresztül, így talán elérhetik az álnevesítési szintet – mivel külön szerveren, szűrve, más rendszerektől elkülönülten léteznek –, ha az érintettel csak további információk birtokában kapcsolható össze. Amennyiben, ezeket a már szűrt, tisztított és külön szerveren tárolt adatokat előtanításhoz használják fel, kérdés, hogy a modell rengeteg adat alapján mennyire képes összekapcsolni a természetes személyekkel, hiszen mint látjuk, a transformer modellek rendkívül jól képesek a szöveg-kontextusokat azonosítani.

A következő a Cloudflare esete, ahol a CDN szolgáltatás kap központi szerepet. A Cloudflare szerverei lépnek elsősorban kapcsolatba a felhasználó eszközével, ezáltal biztos, hogy IP-címeket és egyéb azonosítókat tároljanak a felhasználó eszközéről. Mindemellett azt a felületet is eltárolja, amit a felhasználó előzőleg megtekintett, annak érdekében, hogy legközelebb gyorsabb adatátvitelt tegyen lehetővé. Mondhatjuk, hogy a Cloudflare szintén személyes adatot tárol.

A Microsoft esete egyszerűbb, hiszen a bemenetet nem tárolja a rendszer, mivel csupán REST API hozzáférést biztosít a modellekhez, azonban a felhasználói fiók adatait, illetve a felhasználó által feltöltött adatokat egy az egyben tárolják az Azure szerverei.

A TaskUS esetében e-mail cím, név, egyéb adatok azok, amik a megkeresésben (akár e-mail, akár chat vagy más) szerepelnek, minimum ennyi adatot tárol és kezel.

Álnevesítésről óvatosan beszélnénk ezen támogatószolgáltatások esetén, mivel bár biztosak lehetünk benne, hogy kódolják, titkosítják az adatokat, de egyazon adat egyszerre több helyen is előfordulhat, például az IP-cím, eszköz, név bemenet akár az OpenAI, akár a Cloudflare, akár a Microsoft, de talán még a Snowflake szerverein is megtalálható. Ezért az álnevesítés tökéletes megvalósításához erős kételyek fűződnek.

Az adatkezelés jogalapja

A jogalap kérdésében a GPDR 6. cikke rendelkezik, melyekből – véleményünk szerint – az OpenAI adatvédelmi szabályzata alapján leginkább az első teljesül a vállalat részéről: a) *„az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez”*.

Az érintett hozzájárulásnak GDPR szerinti definíciója: „az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez” Ebből a definícióból néhány fontos és lényeges pont emelhető ki, amelyek a hozzájárulás kellékeit adják: önkéntesség, konkrét mivolt, megfelelő tájékoztatáson alapuló jelleg, és egyértelműség. Maga a hozzájárulás is meghatározott fogalom, amely 95/46/EK irányelv 2. cikkének h) pontja szerint: „az érintett kívánságának kinyilvánítása, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához”.

Adatkezelő és adatfeldolgozó

Az adatkezelőt a GDPR 4. cikkének 7. pontja a következőképpen határozza meg: „az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja”.

Ez alapján egyértelmű az OpenAI adatkezelői minősége, ahogy az is, hogy a TaskUS, a Snowflake és a Cloudflare adatfeldolgozónak minősül. Mivel mind a három szereplő az OpenAI megrendelésére végez műveletet a rábízott adatokkal, semmilyen célt, és eszközt nem határoznak meg az adatkezelésre-feldolgozásra vonatkozóan. Viszont van egy kakukktojás, ez pedig a Microsoft Azure, mivel az OpenAI ez esetben nem megrendelőként, az Azure pedig nem szolgáltatóként vesz részt, hanem partnerségi viszony van a két fél között. Tehát az Azure infrastruktúráján keresztül a felhasználók hozzáférhetnek az OpenAI modelljeihez, ez pedig azzal jár, hogy az Azure adatkezelési politikája alatt állnak azon adatok, amelyek az Azure OpenAI Services szolgáltatásának használata során az Azure birtokába kerülnek. Így maga a Microsoft fogja meghatározni az adatkezelés célját és eszközeit a saját adatkezelési szabályzata alapján, a Microsoft szolgáltatását veszik igénybe a felhasználók, és csak közvetítéssel érhetik el az OpenAI modelljeit. Tehát ebben a relációban a Microsoft is adatkezelőnek minősül.

Adatvédelmi incidensek

Az adatvédelmi incidens fogalmát a GDPR 4. cikkének 12. pontja írja le: „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását,

jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi". Ezen rendelkezés jellemzően az automatizált adatkezelés esetére vonatkozik, vagy olyan manuális adatkezelésekre értelmezhető, amelyek egy nyilvántartás részét képezik vagy annak létrehozását szolgálják.

Fontos fogalom a „biztonság sérülése", amely esetében a biztonsági követelményeket a GDPR 32. cikke határozza meg: „Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja [...]". Vagyis az adatvédelmi incidens az adatbiztonság sérülését jelenti, ez pedig komoly veszélyekkel fenyeget, úgymint a személyes adatok:

a) megsemmisülésével
b) elvesztésével
c) megváltoztatásával
d) jogosulatlan közlésével
e) jogosulatlan hozzáférésével.

Adatvédelmi incidensnek minősül, ha ezek közül minimum egy bekövetkezik, de semmi nem zárja ki, hogy több is párhuzamosan bekövetkezzen.

Az OpenAI esetében az adatok jogosulatlan közlésére reális esély mutatkozik, illetve a megváltoztatás és a jogosulatlan hozzáférés is szintén valós veszéllyel fenyeget. Úgy gondoljuk, mindezen veszélyek egyrészt a modell tulajdonságaiból, másrészt az adatkezelés módjából adódhatnak. Amennyiben a modell tanulóadatait nem megfelelően szűrik ki, tartalmazhat személyes adatot, így fennáll a veszélye annak, hogy a modell akár egy felhasználóval jogsértő módon közöljön információkat. Továbbá a cég szerverein tárolt adatok akár egy kibertámadás esetén, akár egy „jogosultsággal nem rendelkező kolléga" jóvoltából jogosulatlanul hozzáférhetővé válhatnak. Nem biztos, hogy ezek szükségszerűen bekövetkeznek, de ha már matematikai esély adódik rá, akkor az eset veszélyessége okán a jognak már foglalkoznia kell vele.

OpenAI (ChatGPT) és a GDPR kollíziója

Kérdezz bármit, tudom a választ! – ez lehetne a ChatGPT mottója is. Alapvetően ezen találmány, amelynek alapját a mesterséges intelligencia különböző algoritmusai adják, hatalmas lépcső az emberiség és a technológia történetében, amely nemcsak megadja a keresési paraméterek által kiadott találatokat, mint a Google, hanem elbeszélget a felhasználóval, mondhatni interakciót folytat. Azonban felmerül a kérdés: miért tudja mindenre a választ? A válaszok helyességét itt most nem vizsgáljuk, hiszen arra az adatmennyiségre szeretnék összpontosítani, ami lehetővé teszi a chatbot számára, hogy „mindentudó" legyen. Egyértelmű, hogy az OpenAI chatbotjának hatalmas mennyiségű adatra van szüksége, amely egy újabb kérdést vet fel: honnan szerzi az adatokat? Milyen adatokat szerez? Hol tárolja? és még sorolhatnánk.

Az OpenAI algoritmusa és annak működése az egyszerű, földi halandóknak átláthatatlan, azonban tudjuk, hogy végez adatkezelést és profilalkotást is. Ha figyelembe vesszük, hogy egyre többször találkozunk olyan cikkekkel, amelyek az OpenAI adatvédelmi mulasztásaival és a vállalat ellen irányuló észrevételekkel foglalkoznak, egyértelmű, hogy nem minden olyan tökéletes, mint amilyennek lennie kellene. Az alábbiakban olasz és spanyol adatvédelmi hatóságok intézkedéseinek bevonásával zajló jogesetek mentén vizsgáljuk meg a GDPR azon rendelkezéseit, amelyet a ChatGPT figyelmen kívül hagyott.

Alapvetően a legtöbb OpenAI elleni jogeset kiindulópontja az, hogy a vállalat nem rendelkezik az Európai Unión belül székhellyel, ill. adatvédelmi gyakorlata a GDPR rendelkezéseibe ütközik. Az OpenAI egyik európai uniós tagállamban sem rendelkezik fióktelepével, így nem tartja szükségesnek, hogy a GDPR felügyelete alá vonja magát. Ettől függetlenül szembe kell néznie a nemzeti adatvédelmi hatóságokkal, hiszen, ha az egyén a ChatGPT szolgáltatás használata során az Európai Unió területén tartózkodik, az említett hatóságok az egyén panasza alapján eljárhatnak.

Az olasz adatvédelmi hatóság

Az olasz adatvédelmi felügyelet, a Garante 2023. március végén felszólította az OpenAI-t, hogy állítsa le a helyi (olaszországi) adatfeldolgozást, emellett megkérte az amerikai székhelyű vállalatot, hogy tisztázza az általuk megjelölt, az adatkezelés során felmerült problémákat. *„A Garante kérte, hogy az OpenAI tegye közzé átláthatóan az adatkezelést részletező tájékoztatóját, vezessen be korhatárkorlátozást és térjen át szigorúbb korellenőrzési intézkedésekre azért, hogy megakadályozza a kiskorúak hozzáférését ezen technológiához. Emellett az OpenAI-nak az egyének adatai kezelésének jogalapját, lehetőséget kell biztosítania a felhasználók számára a személyes adataik feletti rendelkezésre, ideértve a ChatGPT által róluk generált hibás adat helyesbítéséhez vagy törléséhez való jogot, valamint lehetővé kell tennie, hogy az egyének tiltakozhassanak személyes adataik OpenAI általi feldolgozásával szemben (amelyeket a vállalat az algoritmus betanítására használna fel) és tájékoztatnia kell az olasz*

társadalmat arról, hogy adataik feldolgozásra kerülnek egy mesterséges intelligencia-rendszer képzése érdekében" (Lomas 2023). Az OpenAI válaszul korlátozta a ChatGPT használatát Olaszországban (területi alapú tartalomkorlátozás), a többi felmerült probléma megoldására 2023. április 30-ig, a korhatárkorlátozás bevezetésére május végéig, illetve ennek tökéletesítésére szeptember végéig kapott határidőt. Az OpenAI már április végén folytatni tudta a szolgáltatásnyújtást Olaszországban, miután módosította beállításait. Az olasz adatvédelmi hatóság vizsgálata azonban folytatódik és még várni kell arra, hogy az értékelés befejezése után milyen megfelelőségi következtetések születnek.

A spanyol adatvédelmi hatóság

A spanyol adatvédelmi hatóság (AEPD) követte Olaszország példáját és 2023 áprilisában bejelentette, hogy hivatalos, előzetes vizsgálatot indít az OpenAI ellen a GDPR feltételezett megsértése miatt. Mivel a hatóság nem adott ki az adatok feldolgozásának felfüggesztésére vonatkozó felhívást, a vizsgálat időtartama alatt a ChatGPT továbbra is elérhető spanyol IP-címekről. Az AEPD volt az a hatóság, amely felkérte az Európai Adatvédelmi Testületet (EDPB), hogy a ChatGPT legyen az egyik plenáris ülés vitatárgya. Ezen kezdeményezését azzal indokolta, hogy a ChatGPT globális adatfeldolgozási műveletei jelentős hatással lehetnek az egyének jogaira, amely megelőzésére „európai szintű harmonizált és összehangolt fellépések szükségesek". Az EDPB munkacsoport létrehozásáról döntött az adatvédelmi hatóságok által végrehajtott intézkedésekkel kapcsolatos együttműködés és információcsere előmozdítása érdekében. Ebből adódóan bárki, aki úgy érzi, hogy személyes adataihoz fűződő jogait sérti a mesterséges intelligencia és olyan technológiát használ, amellyel észrevétlenül jut hozzá személyes adataihoz, aggodalmát fejezheti ki az adatvédelmi hatóságnál és kérheti ügye vizsgálatát. Az EDPB munkacsoportja párhuzamosan jár el az egyes nemzeti adatvédelmi hatóságokkal, és célja, hogy összehangolja a generatív MI technológiára vonatkozó adatvédelmi kérdéseket.

Ki van a vonal másik végén?

A mesterséges intelligencia és a nagy nyelvi modellek lehetővé teszik, hogy az eddiginél sokkal fejlettebb módon kommunikáljunk a gépekkel, azonban a ChatGPT esetén ez már kétoldalúvá válik, vagyis egyre jobban hasonlít az emberek közötti beszélgetésre. Képzeljük el egy hetünket úgy, hogy a ChatGPT velünk van minden egyes pillanatban, elemzi szokásainkat, viselkedésünket, majd egy idő után kitanulja életritmusunkat. Ennek következtében megfelelő algoritmusok kidolgozásával olyan „tanácsokkal" tud minket ellátni és olyan információkat közöl velünk, amelyek az addigi „tapasztalata" alapján fontos és érdekel minket. Az MI sajátos jellemzője a gépi tanulás, amelynek lényege, hogy *„a rendszer tapasztalatokból generál önálló tudást. A rendszer példa-adatok, minták alapján képes önállóan, vagy emberi segítséggel szabályszerűségeket, szabályokat felismerni és meghatározni, majd az elsajátított tudásbázisban felfedezett szabályszerűségek alapján döntéseket hozni"* (Eszteri 2022).

A gépi tanulásra képes MI-rendszereket már elkezdték használni bizonyos, személyes adatokkal kapcsolatos döntések meghozatalára is. A GDPR megközelítése alapján a mesteréges intelligencia úgy írható le, hogy *„bizonyos eszközök szoftver támogatásával képesek érzékelni környezetüket és algoritmusok szerint cselekedni. A mesterséges intelligencia kifejezést akkor használjuk, amikor a gépek utánozzák az emberi „kognitív" funkciókat - például a tanulást és problémamegoldást -, amelyeket normális esetben természetes személyeknek tulajdonítunk"* (Buzás–Péterfalvi–Révész 2021). Vagyis ezen eszközök képesek mind automatikus döntéshozatalra, mind profilalkotásra. Annak ellenére, hogy a GDPR közös rendelkezéseket tartalmaz az automatikus döntéshozatallal és a profilalkotással kapcsolatban, fontos megjegyezni, hogy a két fogalom nem fedi egymást, vagyis lehet szó olyan automatikus döntéshozatalról, ami nem minősül profilalkotásnak és fordítva. *„A kizárólag automatizált döntéshozatalban nincs emberi részvétel a döntési folyamatban, a profilalkotás azonban egy olyan folyamat, amely az automatizált döntéshozatalra támaszkodik előre meghatározott sémák vagy tényezők alapján"* (Buzás–Péterfalvi–Révész 2021). *„A profilalkotás célja a természetes személyekre vonatkozó személyes jellemzők bármilyen automatizált személyes adatok kezelése keretében történő kiértékelése, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők elemzésére és előrejelzésére, ha az az érintettre nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti"* (GDPR). *„Az érintett alapvetően jogosult arra, hogy az automatizált döntéshozatalon alapuló döntés hatálya ne terjedjen ki rá, azonban, ha azon uniós vagy tagállami jog kifejezetten megengedi, amelynek hatálya alá az adatkezelő tartozik és az adott személy kifejezett hozzájárulását adta, a művelethez megengedhető az ilyen adatkezelésen alapuló döntéshozatal. Az ilyen adatkezelés mindazonáltal csakis megfelelő garanciák mellett végezhető, amelybe beletartozik az érintett külön tájékoztatása és az ahhoz való joga, hogy emberi beavatkozást kérjen és kapjon, különösen, hogy kifejtse álláspontját, hogy magyarázatot kapjon az ilyen értékelés alapján hozott döntésről és hogy*

megtámadja a döntést. Az ilyen intézkedés gyermekre nem vonatkozhat" (GDPR).

A profilalkotás során az adatkezelőnek tájékoztatási kötelezettsége áll fenn, amely során közölnie kell az érintettet az ilyen típusú adatkezelés tényéről, érdemi tájékoztatást kell adnia az alkalmazott logikáról, valamint arról, hogy az adatkezelés milyen jelentőséggel és milyen várható következményekkel bír az érintettre nézve. Ezen hármas felsorolás talán legnagyobb problémát jelentő eleme az adatkezelés logikájáról való tájékoztatás. Ezen pont egy MI rendszer által történő adatkezelés esetén előtérbe helyezi az úgynevezett „fekete-doboz" hatást. A fekete doboz itt azt érzékelteti, hogy ismerjük a bemeneti értékeket és a kimeneti értékeket, de ami közben történik, vagyis a folyamat „oroszlánrésze" ismeretlen, átláthatatlan. Ezen átláthatatlanság a technológiai újdonságok megjelenése és elterjedése óta – véleményünk szerint – csak tovább nőtt, és az egyszerű felhasználók számára egyre zavarosabb az ilyen eszközök működésének háttere.

Összefoglalás, konklúzió

Az adatvédelemmel, ezen belül a személyes adatok védelmével foglalkozik a tanulmány, így javaslatainkat, észrevételeinket e mentén szeretnénk megtenni.

Ahogy a technikai részben említettük, maga a GPT modell a szó hétköznapi értelmében véve nem tárol adatot, információt. Ehelyett, ha úgy tetszik, a tanuló adatbázis alapján egyfajta mintát fedez fel az adatok között, ez alapján a minta alapján pedig új tartalmakat képes generálni. Ezek a generált új tartalmak nagyrészt a tanulóadatokra támaszkodnak. Tegyük fel, hogy értelmes mondatokat akarunk kreálni a rendszerrel, ezért értelmes mondatokat viszünk bele, majd megtanulja milyenek ezek az értelmes mondatok. Néhány ilyen értelmes mondat tartalmaz egy nevet, egy címet és egy telefonszámot, ezt a rendszer értelmes mondatként értelmezi, és ha megfelelő bemenetet kap, válaszként is elküldheti. Az előtanítási fázisban bevitt tanulóadatok esetében ezért fennáll az esélye, hogy ezeket egy másik felhasználónak válaszként elküldi.

Innen érkeztünk a tanuló adatbázis kérdésköréhez. Ezeket az adatbázisokat a Snowflake szervere tárolja és dolgozza fel, itt véleményünk szerint rendkívül fontos, hogy ezen adatbázis semmilyen módon ne tartalmazzon személyhez köthető adatokat.

Ebből látszik, hogy az adatvédelem három fronton kell, hogy jelen legyen a modellek esetében. Az információtároló, feldolgozó és az alapján tanuló neurális háló modell esetében szükséges. A mi meglátásunk, hogy amennyiben az információkat tároló szerver tartalmaz személyes adatokat, úgy szükséges lehet ezeket a feldolgozó fázisban kiszűrni, és ezek nélkül használni az adatbázist a modell előtanításához. A feldolgozó fázisban az adott természetes személyhez tartozó adatokat a rendszer bár szétszortírozza és külön helyezi el az adatbázisban, a modell – rendeltetéséből fakadóan – a kvázi szétszórt adatokban újra meg tudja találni a kontextust és összerakni, vagyis a személyes adatokat „újra létrehozza" az adathalmazból, ha úgy tetszik visszaállítja. A tanulóadatok kapcsán felmerül egy másik probléma, az „adatmérgezés" esete, amikor a tanulóadatokat szándékosan eltorzítják, ezzel rontva a modell teljesítményét és fals válaszok visszaadását. Mindez alapvetően nagy kockázatot jelent, mivel az OpenAI a tanulóadatok nagy részét az internetről szerzi, ahol ilyen torzított adatok gyakran előfordulnak. Ezek alapján javasoljuk, hogy szabályozott adatbázisból történjen a modellek tanítása, szűrjék ki az olyan források használatát, ahol fals adatok vagy jelentős mennyiségben személyes adatok találhatók, és talán ezeket még tovább lehetne szűrni.

Következő javaslatunk az új funkciókkal kapcsolatos, konkrétabban a kép- és hangfeldolgozással. Az alapmodellek – akkor is, ha specializálták őket – működésüket tekintve rugalmasak és jól használhatók különböző feladatokra. Így pedig hang és kép alapján félő, hogy a rendszer többlet információt is képes lesz leszűrni egy adott személyhez kötődő felvételből. Ilyen például a hangulat, érzelmek, arcvonások stb. Ezek miatt szükséges lenne, hogy az OpenAI folyamatosan monitorozza rendszereik felhasználhatóságát, a kettős felhasználásra vonatkozó kockázatokat és emellett igyekezzen moderálni, ill. kiszűrni azon válaszokat, melyek ilyesmire irányulnak.

Az internetre vonatkozó kereséssel kapcsolatban szintén kerülnie kell a személyes adatokat, így például a közösségi média profilra és a nem közszereplő személyekre való keresés korlátozott vagy tiltott legyen.

Személyes adat a GDPR szerint az *„azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ"*. A technológiai újdonságok miatt az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek elérhetővé személyes adatokat, ami gyökeresen átalakította a gazdasági és társadalmi életet. Ezek az egymásra is ható jelenségek egyre inkább szükségessé teszik és elősegítik a személyes adatok Európai Unión belüli szabad áramlását, valamint a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását. A személyes adatok kezelése azonban csak akkor lehet jogszerű, ha egyúttal biztosított azok magas szintű védelme is. Alapvetően négy uniós szabadságjogról beszélhetünk (tőke, áru és szolgáltatások, valamint személyek szabad mozgása), de véleményünk szerint az adat/információ lehet az ötödik elem ebben a felsorolásban.

Az OpenAI 2023 szeptemberében bejelentett néhány újdonságot szolgáltatásaival kapcsolatban, immár képes szöveg mellett kép és hangbemenetet is kezelnek.

Ezekkel az újításokkal még jobban kinyílik az az olló, amennyi adatot ki lehet nyerni a felhasználók által bevitt bemenetekből. Mivel nem csak a szöveges bemenetet lehet értelmezni GPT-vel, így felmerül többek között az érzelemfelismerő AI problematikája. A technológiai részben itt jelenik meg erőteljesen a kettős felhasználás valószínűsége, ti. a rendszer – eleget tanulva a képi adatokból – egy ember érzelmi állapotát is megtanulhatja felismerni, mivel az alapmodellek rendkívül könnyen alkalmazkodnak különböző feladatokhoz.

2023. szeptember 27-től a GPT-4 felhasználóinak lehetősége nyílik olyan ChatGPT-t használni, ami már nem korlátozódik a 2021. szeptembere előtti adatokra, hanem valós időben az interneten képes böngészni. A ChatGPT a Microsoft Bing keresőmotorját használja, hogy a felhasználóknak valós idejű, releváns információt tudjon adni. A két rendszer együttműködésének pontos módját még nem ismerjük, de valószínűsíthető, hogy a felhasználó által bevitt bemenet először a Bing rendszerébe kerül, a Bing az interneten releváns információkat keres, amelyet feldolgozva a ChatGPT választ küld. Azt nem tudni, hogy a Bing miként szűri a weboldalakat, illetve, hogy a GPT-4, amely ezek tartalmát dolgozza fel, milyen adatbázisból lett előtanítva, így egyelőre kérdés, milyen veszélyeket rejthet magában.

Irodalomjegyzék

Buzás, P.–Péterfalvi, A.–Révész Balázs (2021) *Magyarázat a GDPR-ról*. Wolters Kluwer Kiadó.

Eszteri, D. (2022) Elosztott adatbázisok, okoseszközök, automatikus döntések és a GDPR: adatvédelmi kapcsolódási pontok néhány új technológia vizsgálata kapcsán. *Magyar Jog*, 2022/9. pp. 505-515.

Eszteri, D. (2023) Hogyan tanítsuk jogszerűen a mesterséges intelligenciát? *Magyar Jog*, 66 (12). pp. 669-682.

Jóri, A.–Soós, A. K.–Bártfai, Zs.–Hári, A. (2018) *A GDPR magyarázata*. I. Fejezet: A személyes adat, Az érintett „azonosítható vagy azonosított" személy. pp. 61-68.; II. Fejezet: Az adatkezelés. pp. 86-87.; III. Fejezet: Az adatkezelők, közös adatkezelők, adatvédelmi vállalatcsoportok. pp. 91-92.; IV. Fejezet: Az adatkezelés jogalapja, Egy vagy több jogalap. pp. 124.; V. Fejezet: Az adatkezelés jogalapja, Egy vagy több jogalap. pp. 134-135.; V. Fejezet: Az adatkezelés jogalapja, Egy vagy több jogalap. pp. 140-141.; VII. Fejezet: Az adatfeldolgozó, adatfeldolgozás. pp. 91-92.; XI. Fejezet: Az adatvédelmi incidensek és kezelésük. pp. 328-333. HVG Orac Lap- és Könyvkiadó Kft.

Internetes hivatkozások

Abid Ali Awan (2023) *What is Generative Model?* https://www.datacamp.com/blog/what-is-a-generative-model [Letöltve: 2023.09.25.].

Akamai: *What is a CDN (Content Delivery Network)?* https://www.akamai.com/glossary/what-is-a-cdn [Letöltve: 2023.09.25.].

Akshita Kumawat (2023) *Geeks for Geeks*. https://www.geeksforgeeks.org/what-is-an-api/ [Letöltve: 2023.09.26.].

BigCommerce: Articles, Ecommerce, Affilate marketing, Affilate marketing 101: *What it is and how to get started?* https://www.bigcommerce.com/articles/ecommerce/affiliate-marketing/ [Letöltve: 2023.09.25.].

Bullwinkel, M.–Urban, E.–Farley, P.–aahil–ChrisHMSFT (2023) *Microsoft Learn, Data, privacy, and security for Azure OpenAI Service.* https://learn.microsoft.com/hu-hu/legal/cognitive-services/openai/data-privacy?context=%2Fazure%2Fai-services%2Fopenai%2Fcontext%2Fcontext#what-data-does-the-azure-openai-service-process [Letöltve: 2023.09.25.].

Cloudflare: Learning Center, What is a content delivery network (CDN)? | How do CDNs work? https://www.cloudflare.com/learning/cdn/what-is-a-cdn/ [Letöltve: 2023.09.22.].

Databricks: *Machine Learning Models*. https://www.databricks.com/glossary/machine-learning-models [Letöltve: 2023.09.23.].

Garling Wu (2023) *8 Big problem with OpenAI's ChatGPT*. https://www.makeuseof.com/openai-chatgpt-biggest-probelms/ [Letöltve: 2023.09.24.].

Google Cloud: Learn, Artificial intelligence (AI) vs Machine Learning (ML). https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning [Letöltve: 2023.09.25.].

H2O Wiki: What is Neural Network Architecture? https://h2o.ai/wiki/neural-network-architectures/ [Letöltve: 2023.09.25.].

IBM: Topics, What is an REST API. https://www.ibm.com/topics/rest-apis [Letöltve: 2023.09.25.].

IBM: Data and AI Team (2023) AI vs Machine Learning vs Deep Learning vs Neural Networks. IBM Blog. https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/ [Letöltve: 2023. 09. 25.].

IBM: Topics: What is Deep Learning? https://www.ibm.com/topics/deep-learning [Letöltve: 2023.09.24.].

Lawton, G. (2023) Transformer model.

https://www.techtarget.com/searchenterpriseai/definition/transformer-model [Letöltve: 2023.09.22.].
Lomas, N. (2023) *Italy gives OpenAI initial to-do list for lifting ChatGPT suspension order*. Techcrunch. https://techcrunch.com/2023/04/12/chatgpt-italy-gdpr-order/ [Letöltve: 2023.09.26.].
Lomas, N. (2023) Spain's privacy watchdog says it's probing ChatGPT too. Techcrunch. https://techcrunch.com/2023/04/13/chatgpt-spain-gdpr/ [Letöltve: 2023.09.25.].
Lomas, N. (2023) *ChatGPT-maker OpenAI accused of string of data protection breaches in GDPR complaint filed by privacy researcher*. Techcrunch. https://techcrunch.com/2023/08/30/chatgpt-maker-openai-accused-of-string-of-data-protection-breaches-in-gdpr-complaint-filed-by-privacy-researcher [Letöltve: 2023.09.25.].
Lomas, N. (2023) Poland opens privacy probe of ChatGPT folliwing GDPR complaint. Techcrunch. https://techcrunch.com/2023/09/21/poland-chatgpt-gdpr-complaint-probe [Letöltve: 2023.09.25.].
Madhavan, S.–Jones, M. T. (2017) *Deep learning architectures*. https://developer.ibm.com/articles/cc-machine-learning-deep-learning-architectures/ [Letöltve: 2023.09.24.].
Merritt, R. (2023) What are foundation models? https://blogs.nvidia.com/blog/2023/03/13/what-are-foundation-models/ [Letöltve: 2023.09.23.].
Natalie (2023) ChatGPT – Release Notes. https://help.openai.com/en/articles/6825453-chatgpt-release-notes [Letöltve: 2023.09.28.].
OpenAI: 4. Your rights; 6. Children. https://openai.com/policies/privacy-policy [Letöltve: 2023.09.25.].
Open AI (2023) Introducing OpenAI Dublin. https://openai.com/blog/introducing-openai-dublin [Letöltve: 2023.09.26.].
Pequeño, A. IV (2023) Major ChatGPT Update: AI Program No Longer Restricted To Sept. 2021 Knowledge Cutoff After Internet Browser Revamp https://www.forbes.com/sites/antoniopequenoiv/2023/09/27/major-chatgpt-update-ai-program-no-longer-restricted-to-sept-2021-knowledge-cutoff-after-internet-browser-revamp/ [Letöltve: 2023.09.28.].
Rancho Labs (2021) 6 major sub-field of Artificial Intelligence. https://rancholabs.medium.com/6-major-sub-fields-of-artificial-intelligence-77f6a5b28109 [Letöltve: 2023.09.25.].
Shah, K. (2022) Pre-training, fine-tuning, and in-context learning in Large Language Models (LLMs). https://medium.com/@atmabodha/pre-training-fine-tuning-and-in-context-learning-in-large-language-models-llms-dd483707b122 [Letöltve: 2023.09.21.].
Snowflake: Aticles, Data Lake vs Data Warehouse. https://www.snowflake.com/trending/data-lake-vs-data-warehouse [Letöltve: 2023.09.25.].
Stanford University (2022) *On the Opportunities and Risks of Foundation Models Center for Research on Foundation Models (CRFM)*. Stanford Institute for Human-Centered Artificial Intelligence (HAI), pp. 105.-106. https://crfm.stanford.edu/assets/report.pdf [Letöltve: 2023.09.25.].
TaskUS: Digital Customer Experience, Services. https://www.taskus.com/services/digital-cx/ [Letöltve: 2023.09.25.].
TaskUS: *Trust and Safety*, Services. https://www.taskus.com/services/trust-and-safety/ [Letöltve: 2023.09.25.].
Turing: Understanding Transformer Neural Network Model in Deep Learning and NLP. https://www.turing.com/kb/brief-introduction-to-transformers-and-their-power [Letöltve: 2023.09.24.].
UODO: Urzad Ochrony Danych Osobowych (2023) https://uodo.gov.pl/en/553/1567 [Letöltve: 2023.09.26.].
URL1: *OpenAI, OpenAI Subprocessor List*. https://platform.openai.com/subprocessors [Letöltve: 2023.09.25.].
Verma, P.–Oremus, W. (2023) ChatGPT invented a sexual harassment scandal and named a real law prof as the accused. The Washington Post. https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/?fbclid=IwAR3zhAoIErWHsKEXSsGFgyP1dzZrY4e4MMjP287nh2DEFJHgn5sAP_P93_M [Letöltve: 2023.09.25.].
Wollacott, E. (2023) *OpenAI hit with new lawsuit over ChatGPT training data*. Forbes. https://www.forbes.com/sites/emmawoollacott/2023/09/01/openai-hit-with-new-lawsuit-over-chatgpt-training-data/?sh=6d49f2456d84 [Letöltve: 2023.09.24.].

Hivatkozott jogszabályok

EDPB-EDPS (2021) Joint Opinion 5/2021, on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en [Letöltve: 2023.09.25.].
European Data Protection Borad (2023) Guidelines 3/2022 on, Deceptive design patterns in social media platform interfaces: how to recognise and aovid them.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en [Letöltve: 2023.09.26].

COM (2021) 206 Regulation of the European Parliament and of the Council laying down harmonised ruled on artifical intelligence (Artifical Intelligence Act) and amending certain union legislative acts. 3. cikk 33) bekezdés; 3. cikk 34) bekezdés; 52. cikk 2) bekezdés. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF [Letöltve: 2023.09.28.].

COM(2017)10 Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 [Letöltve: 2023.09.24.].

URL2: Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46=EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). (6) preambulumbekezdés; (71) preambulumbekezdés; 3. cikk 1)-2) bekezdés; 4. cikk 7. pont; 4. cikk 14. pont; 5. cikk (1) bekezdés a) pont; 12. cikk (1) bekezdés; 13. cikk 2 bekezdés f) pont; 15. cikk (1) bekezdés. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679 [Letöltve: 2023.09.27.].