Minden hang számít!

Az emberi hang mesterséges intelligenciával történő analizálásnak kérdései

Kézirat lezárta: 2022. november 11.

Tartalomjegyzék

Tartalom

Bevezetés

It's not what you say, (but how you say it!)
(Mae West)[1]

2022. A mesterséges intelligenciák használta általánossá vált a fejlett országokban, annak ellenére, hogy sokan valószínűleg nem is tudják, hányszor találkoznak vele a mindennapjaik során. Arra azonban talán kevesen gondoltak, hogy amikor betelefonálnak bankjuk ügyfélszolgálatára egy ilyen szoftver fogja megállapítani, hogy a hívás pillanatában milyen hangulatban is lehettek, mennyire voltak megelégedve az igénybe vett szolgáltatás minőségével. A szoftverek teszik mindezt a betelefonáló hangja alapján, azért, hogy növeljék az ügyfelek elégedettségét. A rendszer nem újkeletű hazánkban, a Telenor telekommunikációs vállalat már 2011-ben egy, a Nextent által készített szoftverrel elemzett hetente több ezer az ügyfélszolgálatára beérkezett hívást.[2] Dolgozatom középpontjában a Nemzeti Adatvédelmi és Információszabadság Hatóságának fennállása óta kiszabott legnagyobb, 250 millió forintos bírsága áll, amit az egykori Budapest Bankra rótt ki, és ami egyben az első mesterséges intelligencia használatával kapcsolatban kiszabott szankció hazánkban.

Kutatásom kiindulópontja annak a ténynek az ismertetése volt, hogy a XXI. századi digitális társadalomban mekkora gazdasági értékké vált az adat. Ezután bemutatásra kerül a mesterséges intelligencia technológia kialakulásának rövid története és működésének lényege, kiemelve azt, hogy milyen veszélyek merülhetnek fel a rendszer használata közben. Fontosnak éreztem ismertetni a hanganalitikai rendszerek működési elvének lényegét, tettem mindezt azért, hogy a Budapest Bankra kiszabott bírság kapcsán egy teljes képet kaphassunk, hogy milyen elkövetett hibák vezettek el ehhez a már korábban említett kiugróan magas bírsághoz. Ehhez azonban elengedhetetlennek gondolom felvázolni az adatvédelmi jog létrejöttének leglényegesebb pontjait, a terület életébe markáns változásokat hozó általános adatvédelmi rendelet létrejöttéig. Ezután 'egyet hátra lépve' az amerikai viszonyok ismertetését is elkerülhetetlennek éreztem, nem csak azért, mert jelenleg is folyamatosan adatokat továbbítanak Európából az USA irányába, annak ellenére, hogy már az Európai Bíróság is kimondta, hogy az adatok biztonsága ott erősen megkérdőjelezhető, de azért is, mert arrafelé

[1]Mae WEST:It's not what you say, but how you say it Album: send me home, kiadás éve:2018
[2]Minden hívást beszédanalízissel vizsgál a Telenor ügyfélszolgálata:https://www.hwsw.hu/hirek/47708/telenor-nextent-ugyfelszolgalat-voice-miner-hanganalizis.html

ez a fajta hanganalízis általi elemzés mondhatni teljesen mindennapos. Végezetül dolgozatom zárásaképpen felvázolok, egy olyan hozzáállást a mesterséges intelligencia szabályozásáról, ami az adatok megfelelő biztonsága mellett képes garantálni, hogy az Európai Unió tervéhez híven a világ élvonalába kerülhessen a mesterséges intelligencia felhasználása tekintetében az évtized végére.

2.Digitális társadalom

Digitális társadalomról akkor beszélhetünk, ha gyors, olcsó a földrajzi helyektől független adattárolást, adatátvitelt, az adatok széles körű és sokoldalú kombinációját, rekombinációját lehetővé tévő bináris logikai és gondolkodási struktúrák dominálnak, s átfogó hálózatuk a környezetünk részévé vált.[3] Mint minden működő társadalomban, természetesen a digitális társadalomban is nélkülözhetetlen egy átfogó szabályrendszer, amelyben az adat, mint a XXI. század egyik legértékesebb vagyoni erővel bíró eszköze, biztonságban van. Az Economist egy 2010. évi számában megjegyezte, hogy az adatok, különös tekintettel a fogyasztók személyes adatai, „az üzleti élet új alapanyagává váltak: a tőkével és a munkával szinte egyenlő gazdasági input".[4] Mi, az Európai Unió területén élő természetes személyek azt gondolhatjuk, hogy sok mindent teszünk adatainak biztonsága érdekében, de pontosan az adat értékéből kifolyólag, már egy érintéssel engedélyt adhatunk arra, hogy a telefonunk, okos eszközünk ott legyen minden beszélgetésben, kihallgatva a témát, vagy hogy kihez imádkozunk elalvás előtt.

2.1. Az adat fogalma és jelentősége

Az adat az új olaj![5] - hangzott el Angela Merkel egykori német kancellár szájából 2019-ben. Azonban azt, hogy mi is az adat, nehezen lehetne egy fogalommal meghatározni. Az Európai Gazdasági Térség (az Unió tagállamai, valamint Norvégia, Liechtenstein és Izland) területén hatályos Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban GDPR) sem ad pusztán csak az adat fogalmára definíciót. Általános értelemben elmondható, hogy az adatok, érvelés, vita vagy számítás alapjául szolgáló tényszerű információk (például mérések vagy statisztikák) vagy digitális formában továbbítható vagy feldolgozható információ érzékelő eszköz vagy szerv által kibocsátott információ, amely hasznos, irreleváns vagy redundáns információt is tartalmaz, és amelyet fel kell dolgozni ahhoz, hogy abból következtetéseket lehessen levonni.[6] A definícióból megállapítható, hogy az adatok magukban is értékkel bírhatnak, azonban azokat feldolgozva önmagukon túlmutató értelmet nyerhetnek. Nem meglepő, hogy a gazdasági tevékenységet végző vállaltok is felismerték ezt, és ezért a legtöbb

[3]GYEKICZKY Tamás: Jogrendszerek a digitális társadalomban, Wolters kluwer Hungary Kft. 2020 Budapest 23.
[4]Kenneth CUKURIER: Data,data everywhere. The Economist, London, 2010.http://econ.st/3gqggaw
[5]Merkel Az adat az új olaj 2019.11.18. Portfolio https://www.portfolio.hu/gazdasag/20191118/merkel-az-adat-az-uj-olaj-407459#
[6]Az adat fogalma: https://www.merriam-webster.com/dictionary/data

”ingyenesnek” nevezett szolgáltatás esetén az adatainkkal fizetünk. Erre egy kiváló példa az AVG ingyenes antivírus szoftver adatvédelmi nyilatkozata, amely tartalmazza, hogy a program összegyűjtheti a felhasználóról a nem személyes adatokat (például böngészési és keresési előzmények), amelyeket harmadik félnek is értékesíthet (például hirdető cégek), ezért cserébe a szoftver ingyenes maradhat a felhasználók számára.[7]

2.2. A Mesterséges Intelligencia

A mesterséges intelligencia kifejezést először John McCarthy alkotta meg 1956-ban, amikor az első tudományos konferenciát tartotta a témában.[8] A rendszer fejlődése és térnyerése pedig azóta gyakorlatilag töretlen, a haditechnológiától az orvosláson át az ügyfélélmény javításáig mindenhol felhasználásra kerül. Népszerűségének két oka van; az egyik, hogy megfelelő felhasználás mellett csökkenteni tudja a kiadásokat, növelni a bevételeket, a másik pedig, a képesség, hogy a kitűzött üzleti/stratégiai célok elérését lerövidítheti. Az Európai Bizottság honlapján olvasható, hogy az, ahogyan a mesterséges intelligenciához (a továbbiakban, MI) viszonyulunk, meghatározza majd a világot, amiben élünk.[9] Éppen ezért az európai MI stratégia célja, hogy az évtized végére az EU a mesterséges intelligencia világszínvonalú központjává váljon, és biztosítsa, hogy annak felhasználása megbízható módon és az emberi jogok tiszteletben tartásával történjen. Emellett a mesterséges intelligencián alapuló innováció előmozdítása szorosan kapcsolódik az adatkormányzási rendelethez, a nyílt hozzáférésű adatokról szóló irányelvhez és az uniós adatstratégia egyéb kezdeményezéseihez, amelyek megbízható mechanizmusokat és szolgáltatásokat fognak létrehozni a kiváló minőségű, adatvezérelt MI-modellek fejlesztéséhez szükséges adatok újra felhasználása, megosztása és összevonása érdekében.[10]

A jogalkotó véleménye szerint a szabályozni kívánt mesterséges intelligencia beépülhet bármely, a belső piacon szabadon forgalmazott termékbe vagy szolgáltatásba[11], így a pusztán tagállami szintre szorított jogalkotás megkérdőjelezné a szabályozás hatékonyságát. Az első lépés az Európai Bizottság részéről az ún. Fehér Könyv megalkotása volt, amely egy 2019-ben létrehozott magas szintű szakértői csoport létrehozásával, bevonásával fektette le az alapokat a

[7]PWC:Mennyit ér az adat? 2018.https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/data_monetization_2018_web.pdf
[8]The history of artificial Intelligence University of Washington https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf
[9] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[10] Javaslat az Európai Parlament és Tanács Mesterséges Intelligenciára vonatkozó rendelet tervezetéről https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52021PC0206 bezvezető 5. pont
[11] Az EU MI rendeletének bevezetője 7.

témában. A munkacsoport hét alapvető követelményt fogalmazott meg az MI rendszerekkel szemben. Ezek az emberi felügyelet, műszaki stabilitás és biztonság, adatvédelem, átláthatóság, sokféleség, megkülönböztetésmentesség és méltányosság, társadalmi és környezeti jólét, valamint elszámoltathatóság.[12] Ursula von der Leyen, a Bizottság elnöke kifejtette, hogy nem csak a szilárd alapok meghatározása a fontos, hanem egy olyan rendszer felállítása is, mellyel elnyerik az európai emberek bizalmát is. A célkitűzést a Bizottság konkrét jogszabályok megalkotásán keresztül kívánja elérni.

E cél megvalósulásaként jött létre 2021-ben az Európai Parlament és Tanács rendelettervezete a mesterséges intelligenciáról. Ebben a rendelettervezetben a következőképpen kerül meghatározásra a mesterséges intelligencia fogalma: ”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”.[13] A rendelet I. számú mellékletében pedig a következőeket találjuk: gépi tanulási megközelítések, ideértve a felügyelt, a felügyelet nélküli és a megerősítő tanulást, a módszerek széles skálájának, többek között a mélytanulásnak az alkalmazásával. Továbbá ide tartoznak logikai és tudásalapú megközelítések, beleértve a tudás megjelenítését, az induktív (logikai) programozást, a tudásbázisokat, a következtetőmotorokat, a(z) (szimbolikus) érvelést és a szakértői rendszereket.[14] A rendelet hatálya kiterjed az MI-rendszereket az Unióban forgalomba hozó vagy üzembe helyező szolgáltatókra, függetlenül attól, hogy ezen szolgáltatók letelepedési helye az Unióban vagy harmadik országban található. Továbbá az MI-rendszerek Unión belüli felhasználóira, valamint az MI-rendszerek harmadik országban található szolgáltatói és felhasználóira, ha a rendszer által előállított kimenetet az Unióban használják.[15]

Nem csak az Európai Unió készül az elkövetkező digitális kihívásokra, 2020-ban az Innovációs és Technológiai Minisztérium közzétette Magyarország 2030-ig szóló mesterséges intelligencia stratégiáját. A tervből kiolvasható, hogy Magyarország elhivatott az MI rendszerek fejlesztésében, és a rendszerekkel kapcsolatos kísérletezési kedv növelésében, hiszen az évtized végére nagyságrendileg 6 400 Mrd Ft extra GDP növekmény becsülhető.

[12]Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf
[13]Az EU MI Rendelet: 1. cikk https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206&from=FR
[14] Az EU MI Rendelete: I. sz. melléklet
[15] Európai Unió MI rendelettervezet 2. cikk

Ugyanakkor a stratégia szól arról is, hogy hazánkban az MI fejlesztések egyelőre koordinálatlanok, az adatvagyon csak egy kis része hozzáférhető és a hazai MI startupok még nem rendelkezek meghatározó szereppel a világpiacon.[16] A stratégiában ismertetésre kerülnek azok területek, amelyeken már eddig is alkalmazták a mesterséges intelligenciát, ebből az egyik a bank és biztosítási terület. Ugyan a hanganalízises szoftverek nem kerülnek megemlítésre, ugyanakkor a stratégia támogat minden olyan megoldást, melyekkel az adatok másodlagos felhasználását hatékonyabbá lehet tenni.

2.3. Az MI veszélyei

Általánosságban elmondható, hogy az emberek sokszor félnek az ismeretlentől, ugyanakkor hajtja is őket a vágy új dolgok alkotására. Nincs hiány olyan történetekből sem, hogy mennyi veszélye van a mesterséges intelligencia használatának. Elég csak azokra a disztópikusnak ható történetekre gondolni, amikor egy MI rendszer alapján működő robotnak érzelmei lettek és a feltalálója ellen fordult. Microsoft cég a Twitterrel együttműködve ennek a lehetőségét vizsgálta a Tay Microsoft[17] kísérlet keretein belül. A kísérlet szerint Twitter ráengedett egy MI alapú chatbotot (ezt nevezték Tay-nek) az alkalmazására, amellyel minden felhasználó válthatott üzenetet. Alig több, mint 24 óra után Tay rasszista üzeneteket küldött, valamint kritizálta az Egyesült Államok akkori elnökét, Donald Trump-ot és kormányát. A hiba azonban nem a készülékkel, hanem a felhasználókban volt, mert ők terelték erre a témát, és a tanulásra képes rendszer csak felszedte az információkat, amikkel ellátták. Nem lehet azt állítani, hogy teljesen veszélytelen lenne a rendszer használata a természetes személyekre, de sokkal inkább kell egyelőre az adathalászatra, a biometrikus azonosításra, vagy a hátrányos megkülönböztetésre gondolni, mint potenciálisan fennálló veszélyforrás. Ennél a pontnál fontos megjegyezni a GDPR preambulumbekezdésében rögzített technológia semlegességet, vagyis, hogy a természetes személyek védelme nem függhet a felhasznált technológiai megoldásoktól.[18] Ezen felül Wojciech Rafał Wiewiórowski, az Európai Unió Adatvédelmi Biztosa a fent említett Fehér Könyvvel kapcsolatos külön állásfoglalásban megjegyezte, hogy az MI rendszerekkel kapcsolatos követelmények ne csak a fogyasztói oldallal szemben álljanak fent, hanem az uniós intézmények, szervek, hivatalok és ügynökségek, ha mesterséges intelligenciát használnak, az uniós tagállamokban alkalmazottakkal megegyező szabályok

[16]Magyarország mesterséges intelligencia stratégiája 2020. május 16. https://ai-hungary.com/api/v1/companies/15/files/137203/view
[17]Milyen veszélyeket rejt a mesterséges intelligencia? https://itmap.hu/milyen-veszelyeket-rejt-a-mesterseges-intelligencia/
[18]GDPR (15) preambulumbekezdés

hatálya alá tartozzanak.[19] Ezzel még inkább eleget téve az átláthatóság követelményének és erősítve a polgárok bizalmát az ilyen rendszerekben. Valamint ezzel az intézkedéssel gátját lehet szabni, hogy az állami hatalom birtokosai visszaéljenek a helyzetük adta lehetőségekkel és önös célokra használják fel a rendszereket.

A korábban már említett Mesterséges Intelligencia rendelettervezet, (összhangban a GDPR-al) kockázatalapú megközelítést alkalmaz, és ez alapján három csoportba sorolja az MI rendszereket. Végeredményként pedig megkülönböztethetőek egymástól tiltott-, magas kockázattal járó-, valamin olyan MI rendszerek, amelyek felhasználása nem jelent nagy kockázatot a személyek jogaira és szabadságára nézve. A besorolásnál vizsgálták, hogy az MI rendszer negatív hatása mekkora kárt tud okozni, a kár visszafordítható-e, hogy a károsultak milyen mértékben kerülnek kiszolgáltatott helyzetbe, illetve, hogy az adott rendszerrel kapcsolatban vannak-e hatékony gyakorlatok a potenciálisan problémák megoldására. A fent említett okok miatt minősítették tiltottá a távoli biometrikus azonosító rendszerek használatát, melyek alkalmasak lehetnek arra, hogy egy személyt a tulajdonságai alapján kategorizáljanak, ami végső soron könnyedén vezethet az érintett hátrányos megkülönböztetéséhez. Általánosságban elmondható továbbá, hogy tilos minden olyan rendszer felhasználása, amely az egyébként is hátrányos helyzetben lévő személyek (kiskorúak, szellemi és/vagy testi fogyatékossággal élők) helyzetét kiszolgáltatottá teszi. A nagy kockázatúnak[20] minősített MI rendszerek számos követelménynek kell, hogy megfeleljenek, de szabályozott környezetben minimalizálható a bennük hordozott kockázat. Ilyen követelmény a megfelelő szakmai dokumentáció elkészítése, uniós adatbázisba történő beregisztrálása, nemzeti hatóságnál való bejelentés, a nagy kockázatú MI rendszer által automatikusan generált naplók megőrzése. A rendelettervezetet széleskörű támogatásra talált, és várhatóan a közeljövőben az Európai Parlament elé kerül elfogadásra.

[19]Az Európai Uniós adatvédelmi biztos összefoglaló véleménye a Fehér könyvről 2020. 06.29. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020XX1117(01)&from=EN

[20]MI act nagy kockázatúnak minősíti: azon terméket, amelynek biztonsági alkatrésze az MI-rendszer, vagy magát az MI-rendszert mint terméket a II. mellékletben felsorolt uniós harmonizációs jogszabályok értelmében a termék forgalomba hozatala vagy üzembe helyezése céljából harmadik fél által végzett megfelelőségértékelésnek kell alávetni és az MI-rendszert a II. mellékletben felsorolt uniós harmonizációs jogszabályok hatálya alá tartozó termék biztonsági alkatrészeként vagy önmagában ilyen termékként kívánják használni.

3. Hanganalitika

Az emberi hang egyes sajátosságai több információt rejthetnek, mint maguk a kimondott szavak[21], ugyanis az emberi hang olyan egyedi, akár az ujjlenyomat vagy a kézírás. A mindennapi bevásárlástól kezdve az otthoni internetszolgáltatáson át a bankunk megválasztásáig mindenütt számos vállalat verseng egymással értünk, a fogyasztókért/ügyfelekért. A verseny azonban nem ér véget azzal, hogy döntés születik például egy pénzügyi intézett mellett, mert ha nem lesz elégedett az ügyfél a szolgáltatás minőségével, könnyűszerrel térhet át az egyik konkurenciához. Így mindenütt nagy hangsúlyt fektetnek a vállaltok az *ügyfélelégedettség* maximalizálásra, valamint az *elvándorlás* minimalizálásra, [22] ehhez pedig a legváltozatosabb módszereket alkalmazzák. Egyik ilyen lehet a hanganlízis vagy hanganalitika. Ezt a szoftvert először a 2000-es évek elején használták kereskedelmi célokra a vállalatoknál, bár akkor a hang elemzéséről még szó sem volt, ugyanis a területen az első megoldások még a beszéd szöveggé alakítására születtek, melynek segítségével sokkal gyorsabban lehetett átiratot, vagy jelentést készíteni egy hívásról.

A hanganalitika a hangfelvételek vagy a kapcsolattartó központokba érkező élő ügyfélhívások beszédfelismerő szoftverrel történő elemzésének folyamata, a hasznos információk megtalálása és minőségbiztosítás céljából. A beszédelemző szoftver azonosítja a szavakat és elemzi a hangmintákat, hogy érzékelje a beszélő hangjában az érzelmeket és a hangsúlyt.[23] Ezenkívül képes a csend, zene és egymásra beszélés detektálására, valamint opcionálisan kiegészítő információk biztosítására, mint a beszédstílus, hangerő és egyéb akusztikai jellemzők.[24] Ugyanis már a beszélő mentális állapotában bekövetkező csekély változások is előhívnak olyan fiziológiai reakciókat, például az idegrendszerben vagy a légzésben bekövetkező változásokat és az izomfeszültséget, amelyek hatással vannak a hangképzési folyamatra.[25]

Számos más terület is van, aminek keretében a hanganalitikát használják. Dolgoznak már olyan rendszeren, ami képes felismerni és beazonosítani a beszélő egészségügyi problémáját, legyen szó akár Parkinson korról vagy poszttraumás stressz szindrómáról vagy skizofréniáról. Jelenleg is folyamatban vannak olyan hanganalitikai szoftver fejlesztések, amelyek kifejezetten

[21]Soskin, W.F., Kauffman, P.E.: Judgment of emotion in word-free voice samples. J. Commun. 11(2), 73–80 (1961) https://doi.org/10.1111/j.1460-2466.1961.tb00331.x
[22] NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021 4.
[23]What is speech analitics? https://www.techtarget.com/searchcustomerexperience/definition/speech-analytics
[24] Xdroid.com VoiceAnalytics https://xdroid.hu/hangelemzes
[25]. CUMMINS, N.:"You sound i'll, take the day off": automatic recognition of speech affected by upper respiratory tract infection. In: IEEE EMBC, pp. 3806–3809 (2017)

a segélyhívások elemzésére fognak használni. Kezdetben a rendszer csak laboratóriumi környezetben működött, tökéletes mikrofonnal, azonban ma már a rendszer képes akár háttérzajjal, nem tökéletes mikrofon közreműködésével is elemzéseket készíteni, azzal együtt, (amit észben kell tartani), hogy egy igazi novumról van szó, így a technológiai háttere jelenleg még fejlődő szakaszban van.[26]

3.1. A szoftver működése

A NAIH 2021-es évvégi összefoglalójában tett említést arról, hogy rekordmagas bírságot szabott ki mesterséges intelligencián alapuló hanganalízis használata miatt. Nem sokkal később pedig fel is került az egész határozat a Hatóság oldalára, amelynek szövegéből nem lehet kétséget kizáróan megállapítani, hogy melyik cég szolgáltatását vette igénybe a bank, ugyanis több olyan magyar startup és vállalkozás is megtalálható a piacon, ami kínál ilyen szolgáltatást. Elmondható, azonban az, hogy az ilyen szoftverek működési elve nagyon hasonló, a folyamathoz pedig mesterséges intelligenciát vesznek igénybe. (Ez volt az első pont, ahol a Budapest Bank vétett a szabályok ellen, ugyanis az eljárás elején nyilatkozatában azt közölte, hogy az adatkezelés során nem alkalmaznak semmilyen MI alapú rendszert.)

A hanganalizáló rendszer működése a következőképpen zajlik. Az ügyfél (jelen esetben a Budapest Bank) megvásárolja a szoftvert, amit a call centerbe érkező hívásokon tud felhasználni. A technológia három fő összetevőből áll. Az első a természetes nyelvi feldolgozás (NLP): Ez az összetevő elemzi a kimondott szót, és azonosítja a releváns kulcsszavakat. Megérti a beszélgetések különböző aspektusait. Az NLP-motort a meghatározott szabályokkal betanítják a legkülönfélébb összetett párbeszédek dekódolására. A második összetevő a szándékosztályozás, aminek lényege, hogy a rendszerben lévő mesterséges intelligencia képes felismerni a hívást kontextusát jellemző konkrét szavakat (mint például, probléma vagy megoldás). A kulcsszó felismerés (a szoftvert használó igényeire alakítva) lehetővé teszi a panaszos ügyfelek kiszűrését és a churn (felháborodott ügyfél) megelőzést, a tiltott /töltelékszavak kimutatását.[27] A harmadik pedig maga az analízis folyamata. Ezalatt a szoftver figyelme megoszlik a kimondott szavak, az intonáció és egyéb nonverbális jelek között, melyek az ügyfelek elégedettségének vagy frusztrációjának mutatójaként szolgálhatnak[28], és képes

[26]Jacob Leon KRÖGER, Otto HANS-MARTIN LUTZ and Philip RASCHKE Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference https://link.springer.com/content/pdf/10.1007/978-3-030-42504-3_16.pdf

[27]NAIH-85/2022 (NAIH-7350/2021) https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei

[28] What is voice analytics? https://justcall.io/blog/what-is-voice-analytics.html#How_does_voice_analytics_work

meghatározni, hogy a hívás idejében az ügyfél dühös, elégedetlen, csalódott, bizonytalan, semleges vagy elégedett állapotban volt.

Ezután a szoftver a fejlesztő üzleti titkát képző szempontrendszer szerint elemzi a hangfelvételeket, majd ezekből egy sorrendet állít. Ennek alapja, hogy a vizsgált szempontokból levonható következtetés szerint a telefonáló bár formális panaszt nem terjesztett elő elégedetlen volt-e az ügyintézéssel/szolgáltatással[29]. Az ilyen rendszerek mögött óriási adathalmaz, úgynevezett *big data* áll. A big data nagy mennyiségű, nagy sebességű, nagy variációs lehetőséggel bíró információvagyon-összesség, amely az adatkezelés költséghatékony és innovatív formáin keresztül lehetővé teszi kiemelt új összefüggések feltárást, a döntéshozatalt és a folyamatautomatizálást.[30]

A rendszer minden beérkező hívást rögzít, de az 5 másodperc[31] alattiakat esténkét automatikusan törli. A szoftver saját tárhelyén alap esetben 45 napig tárolja a hívásokat, ezalatt van lehetőség a megtörtént hívás visszahallgatására. Minden hívás a határidő lejárta után automatikusan törlődik, azonban a korábban elvégzett hanganyag elemzések ezután is elérhetőek lesznek, de ezekből az adatokból az egyes hívások már nem következtethetőek ki. [32]A rendszer képes jelezni a megadott szókészlet, valamint a felismert érzelmek alapján hogy a híváson belül pontosan melyek a problémás részek, így az ellenőrző személyeknek elég csak azokat visszahallgatni. A szolgáltatók azt ígérik, hogy a termék használatával javítani lehet a betelefonáló ügyfelek hívásélményét, illetve elemzések segítségével az egyes call centerben dolgozó munkatársak egyéni fejlődését elősegíti.

4. Adatvédelem

Az adatvédelmi jog Jóri András szerint: azon jogszabályok összessége, amelyek meghatározott (természetes) személyekkel összefüggésbe hozható adatok kezelésének rendjére adnak előírásokat és meghatározott jogokat biztosítanak e személyeknek saját személyes adataik vonatkozásában.[33] Az adatvédelmi jog, viszonylag rövid története ellenére a szakirodalom a szabályozás több generációját különböztetheti meg, melyek különböző, de mindannyiszor a technológia fejlődéséhez és az ehhez szorosan kapcsolódó társadalmi

[29]NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021 5.
[30]TÖRÖK Bernát és ZŐDI ZSOLT: A mesterséges intelligencia szabályozási kihívásai, Ludovika Egyetem Kiadó Budapest, 2021 44.
[31]NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021 3.
[32]NAIH-85/2022 (NAIH-7350/2021) https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei
[33]JÓRI András: Az adatvédelem alapjai 2019.04.02. HVG Orac Kiadó Kft. Budapest https://gdpr.orac.hu/wp-content/uploads/szeminarium/GDPR_kepzes_20190402_Adatvedelmi_alapok.pdf

változásokhoz köthető kihívásokra reagálva hasonló szabályozási célokat eltérő megközelítéssel igyekeztek megvalósítani. A jogszabályok magas száma annak is köszönhető, hogy a jogterület igen szoros kapcsolatban áll a technológia fejlődésével és a társadalom változásaival így rövid időn belül felmerülhet az igény egy-egy kérdéskör szabályozásának teljes vagy részleges újragondolására[34].

A fejlődés ívét jól mutatja, hogy minden jogszabály a korábban lefektetettek legfontosabb vívmányait átveszi és azzal együtt igyekszik újítani. A következőkben kiemelésre kerültek az egyes korszakok legfontosabb állomásai, de ezeken kívül is számos adatvédelmi szabályozás született a térségben. A gondolat, hogy az adatok, különösen a természetes személyek adatait értéküknél fogva védelem illeti meg, egészen 1959-ig nyúlik vissza Európában, jóllehet az adatvédelmi jog kialakulásáról ekkor még nem beszélhetünk. Fontos megemlíteni azonban egy informális momentumot az adatvédelmi jog kialakulására. Ez pedig nem volt más, mint mikor George Estman 1888-ban New Yorkban piacra dobta a Kodak1-es fényképezőgépet, amelynek sajátossága volt, hogy az ára miatt gyakorlatilag bárki hozzájuthatott. Gyakorlatilag ez hívta életre az adatvédelemben használt hozzájáruláshoz való jogot, ugyanis a könnyen hozzáférhető gép hatására megszaporodtak a titokban elkészített felvételek. Nem is véletlen, hogy a cég mottója a következő volt:" Ön csak megnyomja a gombot, a többi a mi dolgunk."[35]

Az Európai Parlament és Tanács 95/46 EK Irányelvének preambulumából[36] egyértelműen kiolvasható, hogy a jogalkotó célja az adatok a négy alapszabadsághoz hasonló szabad áramlásának akadálymentessé tétele úgy, hogy a személyek alapvető jogai biztosítva legyenek. Ezen felül „az adatfeldolgozási rendszerek célja az emberek szolgálata; mivel a természetes személyek nemzetiségétől és lakóhelyétől függetlenül tiszteletben kell tartaniuk e személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat, és hozzá kell járulniuk a gazdasági és társadalmi fejlődéshez, a kereskedelem fejlődéséhez, valamint az egyének jólétéhez."[37] Az imént említett irányelv ugyan korábbi, a szakértők az adatvédelmi jog kialakulását az 1970-es évekre teszik, mint az ekkor kibontakozó technológiai forradalomra adott jogi válaszlépés.[38] Az első ténylegen adatvédelemmel kapcsolatos törvény

[34] SZŐKE Gergely László: Az európai adatvédelmi jog megújítása, tendenciák és lehetőségek az önszabályozás területén HVG-ORAC Kiadó Kft. Budapest, 2015 25.
[35] Fotóművészet Magazin 2004/3-4 XLVII évfolyam Pfisztner Gábor: Photokina 2004
[36] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 95/46/EK IRÁNYELVE (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (2-3) preambulumbekezdés
[37] Az Európai Parlament és Tanács 95/46 EK Irányelve (2) preambulumbekezdés https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:31995L0046&from=HU
[38] SZŐKE Gergely László: ADATVÉDELEM ÉS ÖNSZABÁLYOZÁS. ADATVÉDELMI IRÁNYÍTÁSI RENDSZER AZ ADATKEZELŐKNÉL doktori értekezés Pécs, 2014.

a németországi Hessen tartományban született, tárgya pedig az akkoriban Európában széleskörben elterjedt nyilvántartásokba gyűjtött személyes adatok kezelésére terjedt ki. Fontos hangsúlyt kaptak továbbá az adatbiztonságra vonatkozó (jogosulatlan hozzáférés, nyilvánosságra hozatal, megsemmisítés) szabályok.[39]

Az adatvédelemi jog kialakulásának második generációja a 80-as 90-es évekre tehető. A személyi számítógépek megjelenése az online kereskedelem fellendülését eredményezte, amely a gazdaság oldaláról a nagy vállalatokon keresztül egyre inkább csillapíthatatlan *adatéhséget* eredményezett, ugyanakkor hiányoztak azok a jogszabályok, amelyek a másik oldalon lévő fogyasztók (természetes személyek) adatainak védelmét megfelelően garantálni tudják. Erre elsőként válaszul 1980-ban az OECD[40] (Organization for Economic Cooperation and Development) adott ki iránymutatást. A korábban már említett okon kívül a másik probléma az volt, hogy az eltérő nemzeti jogi szabályozások, amelyek az adatvédelmi és az ahhoz kapcsolódó kommunikációs technológiára vonatkoznak, komoly hatékonysági hiányosságokat és gazdasági költségeket okoznak, valamint károsítanák a személyes adatok értékét.[41] Annak ellenére, hogy nagyon különböző jogszabályi rendszerrel rendelkező országok képzik az OECD tagságát, az irányelvben megfogalmazott alapelvek tekintetében széleskörű konszenzus alakult ki. Itt olyan alapelvek lefektetésére került sor, mint az adatgyűjtés korlátozásának elve, célhoz kötöttség elve, hozzájárulás elve, (igen gyakori, hogy ezen elv sérülése miatt szabnak ki bírságot) melyek innentől fogva minden adatvédelmi jogszabály alapját képzik majd. Bár kezdeti célja nem volt, mégis az OECD irányelv egy kapocs lett az az Európai Unió és az Egyesült Államok között. Ki kell még emelni az évtized másik fontos jogszabályát, az 1981-ben Strasbourgban aláírt személyes adatok gépi felhasználása során az egyének védelméről szóló egyezményt, amely a témában az első jogilag kötelező erejű nemzetközi okmány.[42]

Az 1990-es évek közepétől az Európai Közösség életében alapvető változások zajlottak le, így volt ez az adatvédelmi jog területén is. Ebben az időben sorra kerültek be a nemzeti alkotmányokba, hogy a személyes adatok védelméhez való jog, alapjog. Ezzel kívánták erősíteni az egyén pozícióját, akár az állammal, akár a nagy vállalatokkal szemben. Ezt az irányt erősítette tovább, hogy a 2000-ben Nizzában megrendezett csúcstalálkozón megszületett Alapjogi Charta 8. cikke kimondja, hogy: „Mindenkinek joga van, a rá vonatkozó személyes

[39]JÓRI András: Adatvédelmi Kézikönyv, Budapest, Osiris Kiadó 2005 53.
[40]Michael KIRBY The history, achievement and future of the 1980 OECD guidelines on privacy 2011
[41]Jennifer STODDART: Thirty years after the OECD privacy guildline https://www.oecd.org/sti/ieconomy/49710223.pdf
[42]A SZEMÉLYES ADATOK VÉDELME: https://www.europarl.europa.eu/ftu/pdf/hu/FTU_4.2.8.pdf

adatok védelméhez."[43]. Fontos rendszerszintű változás volt még az adatkezelési jogalapok megjelenése és elterjedése.[44] Ezzel összhangban Magyarország Alaptörvénye VI. cikk (2) bekezdésében rögzíti a személyes adatok védelméhez való jogának tartalmát, vagyis mindenkinek joga van tudni, hogy ki, hol, mikor milyen célra használja fel az ő személyes adatait.[45]

4.1. Az adatvédelmi rendelet megszületése

Az Európai Unió alapjait és működését meghatározó jogi aktusok, nemzetközi jogi szempontból nemzetközi szerződésnek minősülnek.[46] Ebből következik, hogy ezen szerződések megkötésével a tagországok egyes kérdésekben, melyek alapvetően a joghatóságuk alá tartoznának, a döntéshozás jogát közösen gyakorolják meghatározott intézmények és döntéshozási mechanizmusok útján. Saját nemzeti jogszabályaikat pedig úgy kell kialakítaniuk, hogy az ne menjen szembe egyik nemzetköz szinten elfogadott nemzetközi szerződéssel sem.

2012. január 25-én, az Európai Bizottság az 1995-ös uniós adatvédelmi szabályok átfogó reformját javasolta az online magánélethez való jogok megerősítése és az európai digitális gazdaság fellendítése érdekében, ez volt az úgynevezett" adatvédelmi csomag"[47]. A közösség jogalkotás elsődleges motivációja elsősorban mégsem csak az alapjogok védelme volt, hanem az EUMSZ 114. cikkével összhangban a belső piac működését korlátozó akadály lebontása.[48] Innentől számítva 4 évre volt szükség, hogy az Európai Parlament elfogadja az Általános Adatvédelmi Rendelet szövegét, új fejezetet nyitva ezzel az adatvédelmi jog történetében. A rendelet az értelmezést segíteni kívánva definíciót ad a személyes adatra és számos más, az adatvédelem során mindennaposan használt fogalomra. Ezen felül meghatároz új olyan jogokat, melyek innentől a természetes személyt megilletik. Ilyen például az adathordozáshoz, vagy a profilalkotás tilalmához való jog.[49] A jogalkotó egyik célja a GDPR megalkotásával, hogy

[43]Az Európai Unió Alapjogi chartája (2012/C 326/02) 8. cikk
[44]SZŐKE Gergely László: Az európai adatvédelmi jog megújítása, tendenciák és lehetőségek az önszabályozás területén HVG-ORAC Kiadó Kft. Budapest, 2015 51.
[45] 15/1991 AB Határozat II. fejezet
DR.ÁRVAY Viktor, dr. BENDIK Tamás, dr. BOJNÁR Katinka, dr. BUZÁS Péter, dr.ESZTER Dániel, Dr. MAJSA Ágnes, dr. OSZTOPÁNI Krisztián,dr. PÉTERFALVI Attila, dr. RÉVÉSZ Balázs, dr. SZIKLAY Júlia : Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., . Budapest 2021 39. oldal
[47]History of the General Protection Regulation https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
[48]UA. MAGYARÁZAT GDPR-RÓL 27.
[49]Általános Adatvédelmi Rendelet. 51. cikk (1) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679#d1e4614-1-1

tisztázza a jogalapokkal kapcsolatban fennálló számos bizonytalanságot.[50] Rendelkezik továbbá az Európai Adatvédelmi Testület (a továbbiakban EDPB) és a nemzeti adatvédelmi hatóságok felállításáról, melynek célja, hogy elősegítse e rendeletnek az Unió egész területén történő egységes alkalmazását iránymutatások, ajánlások, és legjobb gyakorlatok kibocsájtása útján.[51] Ezenkívül az EDPB tagja kérésre részt vehet a nemzeti felügyeleti hatóságok együttműködési eljárásaiban. A GDPR szerint a nemzeti hatóságok feladata, hogy felhívják az adatkezelőket és feldolgozókat a rendelet szerinti kötelezettségeikre, végső soron a GDPR betartatása. A rendelet megsértése esetén pedig joga van a körülményt tisztázó eljárást lefolytatni és esetlegesen a megfelelő jogkövetkezmény(eket) alkalmazni. Az eljárás indulhat kérelemre vagy hivatalból.[52]

5. Az adatvédelem és az MI helyzete az Egyesült Államokban

Annak ellenére, hogy ma már inkább Kínát tartják a legerősebb mesterséges intelligencia nagyhatalomnak, akinek a Pentagon (egykori) szoftverfejlesztési igazgatója szerint behozhatatlanná vált az előnye[53], azonban a MI fejlesztésben és kutatásban sokáig az Amerikai Egyesült Államok járt az élen. Így fontosnak éreztem annak ismertetését, hogy Amerika hogyan viszonyul adatvédelem és a mesterséges intelligencia kérdésköréhez; ezen a ponton kell megemlíteni, az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézetének kezdeményezését, amely megbízható mesterséges intelligencia-rendszerek építőköveinek létrehozását célzó szövetségi szabványok kidolgozására irányuló, a köz- és a magánszektorral folytatott műhelybeszélgetéseket és megbeszéléseket foglal magában.[54] A NIST rendszer célja, hogy olyan elveket hozzon a mesterséges intelligencia szabályozásának rendszerébe, ami egyrészt növeli bizalmat az emberekben, másrészt, hogy tevékenységével hozzájárul a tevékenységével kapcsolatos politikai döntések meghozatalához.[55] Joe Biden kormánya megalakítása után nem sokkal egyértelművé tette, hogy elhivatott annak irányába, hogy az

[50]JÓRI András, SOÓS Andrea Klára: Adatvédelmi jog magyar és európai szabályozása HVG-Orac Lap- és Könyvkiadó Kft. 75.

[51]Általános Adatvédelmi Rendelet. 51. cikk (1) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679#d1e4614-1-1

[52]A Nemzeti Adatvédelmi és Információszabadság Hatóság általános adatvédelmi rendelettel kapcsolatos állásfoglalásai Magyar Közlöny Lap ás Könyvkiadó kft Budapest, 2019 250.

[53]Kína lenyomja a világot? Itt már lépéselőnyben van https://haszon.hu/megorizni/vilag/kina-usa-mesterseges-intelligencia

[54]Legalisation Related to AI https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx

[55]Artificial Intelligence: The vitals https://www.nist.gov/system/files/documents/2022/03/30/AI%20Fact%20Sheet%200615%20FINAL.pdf

Atlanti-óceán két partján fekvő hatalmak együttműködve jelezzék a civil társadalom és a tudomány képviselői számára, hogy megértik a rendszer iránt érzett aggodalmakat és közös erővel kívánnak tenni ellene. [56]

5.1. Az amerikai adatvédelmi szabályozás

Az Egyesült Államokban az első adatvédelemmel kapcsolatos törvényt 1974-ban fogadták el, ez volt az úgynevezett U.S. Privacy Act.[57] Ebben már le voltak fektetve a legfontosabb adatvédelmi alapelvek, úgy, mint a tájékoztatáshoz való jog, a hozzáféréshez való jog, vagy a tiltakozáshoz való jog. Az idő előrehaladtával ezt követte számos további rendelet, azonban elmondható, hogy Amerikában jelenleg államonként külön történik a szabályozás. Így történhet meg, hogy míg Kalifornia vagy New York állam rendelkezései kiterjednek minden olyan vállalatra, ami adott államban tevékenységet folytat, addig Marylandban csak azokra a vállalatokra vonatkozik a szabályozás, amelyeknek fizikailag is ott van a bejegyzett székhelyük, ezen felül az alacsonyabb éves nettó árbevétellel rendelkező vállaltokra sokszor nem is vonatkoznak ezek a szabályok. [58] Meg kell azonban jegyezni, hogy mind az 50 államban jogszabály szerint értesíteni kell az érintett természetes személyt, ha adataik biztonsága egy incidens keretében sérül.[59]

A kaliforniai fogyasztói adatvédelmi törvényt (California Consumer Privacy Act, vagyis CCAP) úgy szokták emlegetni, mint a GDPR-ra válaszként megalkotott jogszabály, mely a témában a legszigorúbbnak is tekinthető Amerikában. A CCPA szembe megy azzal a bevett amerikai megoldással, hogy az amerikai cégek magukat ügyfeleik adatainak tulajdonosának tekintik.[60] Ezen törvény kereti között Kalifornia állam lakosainak lehetőségük nyílt rendelkezniük adataik felett. Tájékozódhatnak arról, milyen adataikat tartják nyilván azt mire használják fel, esetlegesen kinek továbbítják. A gyermekek fokozott védelme érdekében a 16 éven aluliak adatait csak hozzájárulás alapon lehet továbbítani. A fogyasztókat felruházza a tiltakozáshoz való joggal is, így felszólíthatják az érintett vállalatot, hogy törölje adataikat, vagy megtilthatja nekik azok további falhasználást. A törvény így jól láthatóan megnehezíti a

[56]The EU and U.S. starting to align on AI regulation https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation/
[57]https://www.justice.gov/archives/opcl/policy-objectives
[58]U.S. Privay Laws: The complete guide https://www.varonis.com/blog/us-privacy-laws
[59]Security breach notifications laws https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[60]Michael Garlie California Consumer Privacy Act of 2018: A study od compience and associated risk https://www.proquest.com/openview/e341d9d4ddbdab7a174d21f85d6247f7/1?pqorigsite=gscholar&cbl=18750&diss=y

nagyvállaltok dolgát, ugyanakkor a lehetővé teszi azt is, hogy a vállaltok díjért, vagy kedvezményekért cserébe megvásárolhassák a fogyasztók adatait, ezzel egy új piacot nyitva a kereskedelemben. A CCPA felruházza a kaliforniai főügyészt a rendelet végrehajtására, akinek jogában áll bírságot kiszabni az észlelt jogsértések után.

A szövetségi szabályozás hiánya egyre inkább megnehezíti a multinacionális vállalatok életét, ezért sem meglepő, hogy a facebook közösségi oldal alapítója Mark Zukkerberg,[61] négy olyan területet jelölt meg, ahol szükség volna átfogó szabályozásra, ebből az egyik az adatvédelem volt. Különösen igaz ez a Schrems II. ítélet után.

5.2. Schrems II és az adatvédelmi pajzs

A Schrems-ügy egészen 2013-ig nyúlik vissza, amikor is Maximilans Schrems azt kérte nemzeti adatvédelmi hatóságtól, hogy az tiltsa meg a Facebook Ireland számára a személyes adatok Egyesült Államokba történő továbbítását, mert abban az országban nem garantálható megfelelően a személyes adatok védelme. Panaszát a bizottság első körben elutasította, mert úgy találta az adatok védelme igenis megfelelően biztosítva van az úgynevezett Safe Harbur rendszeren keresztül. A Safe Harbour gyakorlatilag nem volt más, mint egy önminősítésen alapúló megoldás, amelynek keretében az USA vállalatai maguk dönthették el, hogy megfelelnek- e az alapelveknek, és ha igen kitehették a SH jelzést honlapjukra, ezzel jelezve, hogy az adatkezelés jogszerű keretek között történik. Az igazsághoz hozzátartozik, hogy semmilyen ellenőrzési mechanizmus nem képezte részét a rendszernek.[62]

Az Európai Bizottság felismerve a Safe Harbour rendszer hibáit, tárgyalásokba kezdett a USA-val, így született meg 2016-ban az úgynevezett adatvédelmi pajzs (privacy shield). A pajzsot személyes adatok védelmét biztosító elvek, nyilatkozatok és kötelezettségvállalások alkották, amelyeknek azoknak a szervezeteknek, akik a pajzshoz kívántak csatlakozni, alá kellett vetniük magukat. Azonban a határozat azt is kimondja, hogy az adatvédelmi pajzs rendelkezései a nemzetbiztonság, a közérdek és a bűnüldözés követelményeinek teljesítése végett szükséges mértékben korlátozhatóak. Az Európai Unió Bírósága szerint az, hogy az amerikai hatóságok hozzáférhetnek az Unió területéről továbbított személyes adatokhoz, nem felel meg a GDPR szerinti arányosság elvnek, mert a megfigyelések nem a szükséges mértékre korlátozódnak. Ezen felül a Bíróság vizsgálta azt is, hogy a GDPR (104) preambulumbekezdésére tekintettel biztosítva van- e jogorvoslati lehetőség. Megállapítása

[61]https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html
[62]Az adatnak mennie kell? https://www.adatvedelmiszakerto.hu/2020/09/a-schrems-ii-itelet-utan-az-adatnak-mennie-kell/

szerint, az amerikai szabályozásából nem egyértelmű, hogy a megfigyelési programokat hogyan lehet korlátozni és hogy léteznek- e az amerikai polgárok számára szóló megfelelő garanciák, amelyek megsértése esetén az amerikai bíróság előtt érvényesíthetné jogait.[63] Mindezekre tekintettel a Bíróság a C-311/18 számú ítéletében az adatvédelmi pajzsot érvénytelenné nyilvánította. Az ítélet következtében jelentősen drágább lett az USA-ba való adattovábbítás költsége és a kockázatok is megnövekedtek.

Ennek következében még inkább érthető, hogy egyre többen sürgetnek egy olyan átfogó szabályozást, amely időtállónak bizonyul a rendkívül gyors fejlődés ellenére, és megfelelő garanciákat biztosít az Uniós térség számára az adatok biztonságát tekintve. Kétségkívül leginkább a multinacionális vállaltok vezetői vetik vigyázó szemüket a törvényhozókra, hiszen ők azok, akik működésük során gyűjtött uniós fogyasztói adatok egy központi rendszerbe gyűjtik, ami így elérhető a világ minden táján működő leányvállalatok számára, ebből következően elengedhetetlen, hogy ezek a vállalatok megértsék az adatáramlás módját annak biztosítása érdekében, hogy a határokon átnyúló adattovábbítás megfeleljen a GDPR követelményeinek[64]. Mindenhez jó kiindulási alap lehet, a már korábban részletezett Kaliforniai Adatvédelmi törvény.

Valószínűleg a közeljövő grandiózus változásokat fog hozni kérdésben. Az USA hajlandóságát mutatja az együttműködésre az a tény, hogy Joe Biden a 2022 októberében aláírt végrehajtási rendeltettel[65] kimondja, hogy az amerikai hírszerző ügynökségek csak meghatározott nemzetbiztonsági célokra, valamint szükséges és arányos módon gyűjthetnek adatokat. Az amerikai hírszerző ügynökségeknek frissíteniük kell politikáikat és eljárásaikat, hogy azok megfeleljenek a rendelet iránymutatásainak. A rendelet szerint az Igazságügyi Minisztériumon belül létrejön az úgynevezett Adatvédelmi Felülvizsgálati Bíróság, ami lehetővé teszi a polgárok számára, hogy egy ”speciális ügyvéd” segítségével pert indíthassanak adataik felhasználásával kapcsolatban. Kérdésre Gina Raimondo kereskedelmi miniszter elmondta:” Ezek a kötelezettségvállalások teljes mértékben figyelembe veszik az Európai Unió Bíróságának 2020-as Schrems II. határozatát, és az uniós jog alapján az Egyesült Államokba történő személyes adat-továbbításra is kiterjednek" A folyamat várhatóan 2023 tavaszára fejeződik be, amikor megtörténhet a végleges paktum közzététele is. [66]

[63]https://gdpr.news.hu/cikkek/schrems-ii-itelet-avagy-a-privacy-shield-halala-1-resz/
[64]Bernard GALLAGHER: Will the US adopt a nationwide data privacy lae similar to GDPR? https://www.ispartnersllc.com/blog/us-nationwide-data-privacy-law-gdpr/
[65]PresidentBiden Signs Executive Order to Implement the European Union-U.S. Data PrivacyFramework
[66]Biden signs executive order on EU-U.S. data privacy agreement https://www.politico.com/news/2022/10/07/biden-executive-order-eu-data-privacy-agreement-00060872

5.3. A hangok elemzése a tengeren túl

Az amerikaiak többsége úgy véli, hogy online és offline tevékenységeit a vállalatok és a kormány bizonyos rendszerességgel nyomon követi és ellenőrzi. Ez a modern élet olyannyira gyakori velejárója, hogy nagyjából tízből hat amerikai felnőtt azt állítja, nem hiszi, hogy lehetséges úgy élni a mindennapokat, hogy a vállalatok vagy a kormány ne gyűjtene róluk adatokat.[67] Amint az korábban részletezésre került, sok pozitív momentuma volt az elmúlt 2 évnek, amelyből arra lehet következtetni, hogy Amerikában is új fejezet kezdődik a mesterséges intelligencia szabályozásának történetében. 2022-ben eddig 17 tagállamban nyújtottak be általános mesterséges intelligenciáról szóló törvényjavaslatot.[68] Általánosságban elmondható azonban, hogy ezekben a javaslatokban csak az a közös, hogy valamilyen módon kötődnek az MI rendszerekhez, de az érintett területek közt éppúgy megtalálható az egészségügy, a munka világa, mint a közösségi médiás platformok.

Pontosan azért, mert Amerikában jelenleg még nincsen GDPR/MI rendelet, így az adatvédelem sem játszik olyan központi szerepet a mindennapokban, mint Európában. Jól mutatja az adatvédelemhez való viszonyulást, hogy a 30 legmagasabb adatvédelmi bírságból az első hatot, mind amerikai vállalat európai leányára szabták ki.[69] Így minden bizonnyal megállapítható, hogy a hang mesterséges intelligencia általi elemzése teljesen bevett gyakorlat, amelyről az érintettek vagy nem is tudnak, vagy ha tudnak is, nem rendelkeznek megfelelő információkkal arra nézve, hogy hová vezethet ez az adatkezelési gyakorlat a folyamatosan fejlődő technikai megoldások tükrében.

6. A Budapest Bank döntés

2017-ben (még a GDPR alkalmazásának kezdete előtt) az egykori Budapest Bank Zrt. (a bank eben a formában már nem létezik, mert 2022. március 31-én beleolvadt az MKB Bankba[70]) hanganalízis alapú szoftvert kezdett használni az ügyfélszolgáltra érkezett hívásokon, azzal a céllal, hogy hatékonyabb legyen a panaszkezelése, valamint a call centeben dolgozó munkatársak munkahelyi tevékenysége javuljon. Négy évvel a hanganalitika használatának kezdete után, a Nemzeti Adatvédelmi és Információszabadság Hatóság eddig

[67]Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information
[68]Legalisataion related to AI https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx
[69] Biggest GDPR fines so far https://www.tessian.com/blog/biggest-gdpr-fines-2020/
[70]Egyesül a Budapest és az MKB Bank https://www.portfolio.hu/bank/20220331/ma-egyesul-a-budapest-bank-es-az-mkb-bank-itt-vannak-a-tudnivalok-536713

soha nem látott, 250 milliós bírsággal sújtotta a bankot, ezenkívül felszólította a sérelmes magatartás azonnali módosítására, mert ez a hangfelvétel elemzésen alapuló adatkezelési gyakorlat számos ponton súlyosan sértette a GDPR-t. A közzétett határozat két részre bontható, ugyanis a most lezárt eljárásnak volt egy előzmény ügye is. Az előzmény ügy vizsgálata arra terjedt ki, hogy az ügyfelek tájékoztatása jelen adatkezeléssel kapcsolatban kielégítő módon történik-e meg. A második eljárásban pedig annak a vizsgálatára került sor a Hatóság részéről, hogy telefonos ügyfélszolgálat bejövő és kimenő hívásai rögzített hangfelvételeinek automatikus elemzésével, és ez alapján a hangfelvételek egy részének visszahallgatásával, majd a visszahallgatott felvételeken szereplő érintettek egy részének visszahívásával összefüggő adatkezelések jogszerűen történnek-e.

6.1. Az előzmény és az aktuális ügy menete

Az érintett bank egyik ügyfele vett észre egy mondatot a bank honlapjára feltöltött adatkezelési tájékoztatóban, ami arra utalt, hogy a hívásokat automatikusan alávetik egy elemzésnek, amely képes lehet arra, hogy a telefonáló hangjából következtetéseket vezessen le.[71] A bank ügyfele ezzel kapcsolatban tett fel néhány kérdést a vonal túlsó végén lévő kollégának, nevezetesen, hogy milyen célból történik az adatkezelés, hol talál a hangelemzéssel kapcsolatos adatkezelésről részletes tájékoztatást, valamint, hogy ez a fajta adatkezelés mennyire felel meg a GDPR-nak. Kérdéseire a bank munkatásától kielégítő válaszokat nem kapott, ekkor fordult bejelentéssel a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban: Hatóság vagy NAIH), melyet a Hatóság az Info tv. szerint köteles érdemben kivizsgálni.[72] Az GDPR erre utaló részének hiányában az adatvédelmi eljárásokra az Ákr. szabályait kell alkalmazni az info tv-ben meghatározott eltérésekkel. A NAIH először a Budapest Bankot, mint pénzintézeti tevékenységet folytató jogi személyt vizsgálta azon adatkezelése tekintetében, hogy az ügyfélszolgálati hívások rögzített hanganyagát automatikusan elemzi, és ezzel kapcsolatban megfelelő tájékoztatást nyújt-e az érintetteknek. A Hatóság a tényállás tisztása céljából elektronikus úton megkereste az érintett bankot. A Hatóság megkeresésére az ügyfél előadta, hogy a kérdéses adatkezelésnek több célja volt. Elsősorban, hogy a bank ügyfélszolgálatán dolgozó személyek munkavégzése hatékonyabb legyen, a hívásokat visszahallgató 20 munkatárs eljárásának útján. Fontos megjegyezni, hogy a hangelemző szoftver rangsorolja a hívásokat a Szoftver által megállapított jellemzők alapján.

[71] NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021
[72] 2011. évi CXII. tv az információs önrendelkezési jogról és az információs szabadaságról 53§ (1)

Ezen jellemzők az Ügyfél előtt sem ismertek, azt a szoftver zártan kezeli. A hívás kiértékelésének részletes eredményei, az értékelt szempontok nem ismerhetők meg.[73] Másodsorban az panaszok megelőzése azáltal, hogy a rendszer előre meghatározott szókészlet alapján listázni tudja azokat a hívásokat, amelyekben az adott szó elhangzik. A problémásként észlelt hívásokat visszahallgatva egy magasabb képzett, több tapasztalattal rendelkező kolléga hívja vissza az ügyfelet, elhárítva a korábban felmerülő problémát ezzel végső soron igyekszik az ügyfél elégedettségét fokozni.

A bank a Hatóságnak adott válaszában kitért arra is, hogy a panasz tevő ügyfél által keresett adatkezelési tájékoztató megtalálható a bank honlapján, és említésre kerül az is, hogy amennyiben az ügyintéző kolléga az érintett tájékoztatást minden hívás elején felolvasná, úgy 10-15 perccel később kerülne sor arra, hogy az ügyfél kérését az ügyintéző elé tárja, ugyanakkor mind a bank részéről indított, mind pedig a bejövő hívások esetében elmondható, hogy az ügyfél figyelmét felhívják arra, hogy hívásáról hangfelvétel készül. Tekintettel arra, hogy a bank kapacitása korlátozott, az ügyfelek türelme pedig sok esetben véges, így a bank érvelése szerint közös érdek a hívások időtartamának lerövidítése. Tehát ez volt az ok az írásbeli tájékoztatás mellet. A bank kérésre elmondta, hogy az adatkezelést *jogos érdek* alapján végzi és automatikus döntés alapán választja ki a visszahívandó személyeket.

A NAIH a második eljárásban a Budapest Bank telefonos ügyfélszolgálatának bejövő és kimenő hívásai rögzített hangfelvételeinek automatikus elemzésével, és ez alapján a hangfelvételek egy részének visszahallgatásával, majd a visszahallgatott felvételeken szereplő érintettek egy részének visszahívásával összefüggő adatkezelések vizsgálata volt. [74] A Hatóság az Ákr.[75] 76§ alapján nyilatkozattélre hívta fel az érintett pénzintézetet. Megállapításra került, hogy a kezelt adatokként számon van tartva, a bank ügyfélszolgálatán dolgozó kolléga neve és hangja, a hívás iránya, ideje, helye, a felhívott, vagy betelefonáló ügyfél hangja neve, telefonszáma és egyedi hívásazonosítója. Mivel az érinettek egyértelműen azonosíthatók, a szoftver által végzett adatkezelésére a GDPR szabályainak irányadóságát semmi nem zárja ki. A bank a korábban már ismertetett információkat kiegészítette azzal, hogy természetesen van az ügyfeleknek lehetőségük gyakorolni a GDPR 21. cikke szerinti tiltakozáshoz való jogot, a hívás bontásával, ellenkező esetben a bank a beszélgetés megkezdését hozzájárulásként értékeli. Ezenfelül a Bank megjegyzete, hogy a szoftver működésének kezdete óta panaszmentesen üzemelt, valamint, hogy a bank számos különböző adatkezelést végez, ehhez

[73] NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021
[74] NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021
[75] 2016. évi CL. törvény az Általános Közigazgatási Rendtartásról

képest az adatvédelmi panaszok száma alacsony és a nemzeti hatóság sohasem szabott ki rájuk bírságot korábban.[76]

6.2. Jogos érdek, mint jogalap

A magyar adatvédelmi jog fejlődésének hajnalán az adatkezelés jogalapjai a hozzájárulásra és a törvény/önkormányzati rendelet általi felhatalmazásra korlátozódtak. Az adatvédelmi rendelet szövegéből levonható, hogy valamennyi, a személyes adatokkal összefüggő tevékenység adatkezelésnek minősül, így a rendet hatálya alá tartozik.[77] A GDPR 6. cikke taxatíven sorolja fel azokat az eseteket, amelyek közül az egyiknek teljesülnie kell, ahhoz, hogy az adatkezelés jogszerű legyen, a felsorolás f) pontja a következőképpen szól: az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.[78] Kisegítő értelmezésként a (47) preambulumbekezdés szerint jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.[79] A természetes személyek biztosága érdekében, fontos, hogy az adatkezelés jogalapja megfelelően azonosításra kerüljön, ugyanis ennek hiányában az adatkezelő, az őt terhelő kötelezettségek körében mulasztást követtett el, ez pedig szükségszerűen vezethet bármely, a GDPR-ban meghatározott jogkövetkezmény alkalmazásához.[80]

Arra, hogy mi lehet jogos érdek, a GDPR nem ad teljeskörű magyarázatot, ezért sokszor jolly-jokerként vagy gumi szabályként is emlegetik, a helyzet azonban az, hogy precíz alátámasztás szükséges a jogszerű adatkezeléshez. A jogos érdek jogalapjának egyik fő sajátossága, hogy a GDPR felhatalmazza az adatkezelőt az adatkezelés körülményeinek kialakításra. A meghatározott jogos érdek szerint kell megjelölni, hogy pontosan milyen célból

[76] NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021
[77] [77]UA. MAGYARÁZAT GDPR-RÓL 83.
[78] GDPR 6. cikk (1) bekezdés f pont
[79] GDPR (47) preambulumbekezdés
[80] NAIH/2019/769. sz. határozat

történik az adatkezelés, milyen hosszú ideig történik és mik azok az intézkedések, amik garanciaként szolgálhatnak a természetes személyek számára, hogy az adataik feldolgozása csak a szükséges mértékben a cél elérésével arányos módon történik.[81] Ha az adatkezelés jogalapja jogos érdek, akkor érdekmérlegelési tesztet kell elvégezni, amit írásban dokumentálni kell, hogy az érintetteknek bemutathassák, hogy miért van arra szükség, hogy az adatkezelés felülírja a természetes személyek jogait, ennek hiányában az adatkezelők nem hivatkozhatnak a jogos érdekre és az adatkezelés jogellenes.[82] Erre főleg azért van szükség mert a jogos érdekre jogalapként gyakran olyan esetekben hivatkoznak, amikor a mérleg nyelve az egyik oldal felé billen (tipikusan ilyennek mondható a bank és ügyfél viszonya). A teszt kitöltése kötelező, az elvégzésre azonban számos módszertan bevethető. A 29. cikk szerinti Adatvédelmi Munkacsoport 7 lépésből álló tesztet ajánl a NAIH elfogadható gyakorlatként öt lépésből állótesztet javasol az adatkezelőknek. Eszerint az érdekmérlegelési teszt keretein az adatkezelőnek először meg kell határoznia, hogy milyen célból kívánja kezelni az adatok konkrét helyzetre és tevékenységre lebontva, olyan célokat kell itt meghatározni, amik valóban léteznek. Be kell mutatnia továbbá azt az érdekelti kört, akire az adatkezelés vonatkozik. (A Hatóság szerint az adatkezelő jogos érdekének meghatározása során figyelembe veheti, hogy az ügyfelek szemében rontaná a vállalat megítélését, ha az ügyintézés nem lenne gyors és hatékony.[83]) Másodsorban meg kell vizsgálni, hogy az adatkezelés szükséges-e a cél elérésében, illetve alá kell támasztania, hogy miért ez a módszer a legalkalmasabb és más megoldások, amelyek esetlegesen kevesebb kockázatot hordoznak magukban, miért nem megfelelőek.

Jogos érdek esetén gyakran előfordul, hogy két egymással szembenálló érek azonosítható be, így az érdekmérlegelési teszt harmadik követelménye szerint meg kell határozni azokat a jogokat, amikre a jogos érdek következtében történő adatkezelés hatással lesz. Valamint azokat a jogokat, amik az érintetteket megilletik, ilyenek lehetnek, hogy a kezelt adatokhoz a lehető legkevesebb ember férhessen hozzá, vagy az, hogy az adatkezelés időtartama minél rövidebben kerüljön meghatározásra. Az arányosság körében vizsgálni kell, milyen személyes adatokra terjed ki az adatkezelés, pl., ha különleges személyes adat, akkor erre külön ki kell térni, illetve jogos érdek esetén az adatkezelőnek bele kell foglalnia a tesztbe, hogy milyen garanciákat állapít meg, amik az arányosságot biztosíthatják. A beépített garanciák lehetnek az adatkezelés végrehajtásához kapcsolódóak, másodsorban lehetnek az információs technológiához

[8181] UA. MAGYARÁZAT GDPR-RÓL.14.
[82] ZAVODNYIK József: A NAIH általános adatvédelmi rendelettel kapcsolatos 2019-es értelmezései Wolters Kluwer Budapest, 2020 182.
[83] NAIH/2020/2758/4 sz. határozata

kapcsolódó biztosítékok, mint például a legjobb technikával biztosítani adatok védelmét. Harmadrészt garanciának tekinthetőek olyan megoldások is, amelyek az érintett számára egyfajta kontrollt biztosítanak, tipikusan ilyen, amikor az érintett bármikor hozzáférhet azokhoz az adatokhoz, melyek jogos érdek alapján vannak kezelve.[84]

6.3. Az adatvédelmi hatásvizsgálat

Habár követelményeiben nagyon hasonlítanak egymásra, mégis fontos megkülönböztetni az érdekmérlegelést az adatvédelmi hatásvizsgálattól (gyakran PIA-ként emlegetik, Privacy Impact Assessment). A GDPR alapján a legfontosabb különbség, hogy amennyiben a jogalapként a jogos érdek kerül meghatározásra, abban azesetben az érdekmérlegelés elkészítése kötelező, a hatásvizsgálatot pedig csak akkor kell készíteni, hogyha „az adatkezelés különösen új technológiákat alkalmazó típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve."[85] Abban az eseten viszont, ha egy ilyen típusú adatkezelés felmerül és a hatásvizsgálat elkészítése, vagy a Hatsághoz való bejelentése elmarad, úgy a NAIH jogosult GDPR-ban meghatározott szankció alkalmazására.[86] Az adatvédelmi hatásvizsgálat elvégezhető az érdekmérlegeléssel együtt is, azonban gyakori, hogy még előtte készül mert, ha az adatkezelő úgy tapasztalja, hogy több módszer is van egy konkrét célhoz kötött adatkezelésre, akkor a hatásvizsgálat segítséget nyújthat abban, hogy kiderüljön melyik jár a legkevesebb kockázattal az érintettek jogaira nézve. „Végső soron tehát adatvédelmi hatásvizsgálat a rendelet betartásának elérésére és bizonyítására szolgáló eljárás."[87] Fontos továbbá, hogy nem elég a hatásvizsgálatot egyszer elvégezni, hanem szükséges azt időről-időre (a kockázat mértékétől függően) felülvizsgálni. A rendelet nem említ kifejezett módszertant az elvégzésre, azonban a NAIH hivatalos honlapján megtalálható a francia adatvédelmi hatóság (CNLI) által készített szoftver, amivel könnyen elkészíthető a hatásvizsgálat a GDPR-al összhangban, hiszen rendszer kockázat alapon sorolja az adatkezeléseket kategóriákba, így a NAIH jó gyakorlatnak ismeri el ennek alkalmazását.

A hatásvizsgálat alapvetően két nagy részből áll. Az elsőben a GDPR 35. cikk (7) bekezdése szerint ismerteti az adatkezelés célját, a szükségesség-arányosság értékelésével, másodsorban pedig bemutatja azokat a biztonsági mechanizmusokat, amivel igyekszik csökkenteni a

[84]UA. MAGYARÁZAT GDPR-RÓL 157.
[85]GDPR 35. cikk (1)
[86]GDPR 35. cikk
[87]29-es adatvédelmi munkacsoport WP 248 rev.01 számú iránymutatása

kockázatot. Amennyiben a hatásvizsgálat azt mutatja, ki, hogy a kockázatot csökkentő intézkedések nem elégségesek, az adatkezelő köteles a Hatósággal konzultálni. Ennek keretében a NAIH igyekszik teljeskörűen megismerni az adatkezelés célját és tanácsokkal ellátni az adatkezelőt, amivel a kockázatok csökkenthetőek.

Természetesen egy mesterséges intelligencia alapú hangelemző szoftver alkalmazásának bevezetése már első hallásra is olyan adatkezelésnek minősül, amelynél a hatásvizsgálat elvégzése nem maradhat el.

6.4. Út a bírsághoz

A bírságról szóló döntés indokolásában a NAIH több fő szempontot kiemelt, amelyek szempontja szerint értékelte az adatkezelés jogszerűségét. Elsősorban, hogy alkalmazható a GDPR az adatok tekintetében, másodsorban, hogy a kezelt adatok hogyan minősíthetőek, harmadrészt a mesterséges intelligencia és a szoftver kapcsolatát. Értékelte a tájékoztatáshoz, valamint a tiltakozáshoz való jog meg (nem) létét, az érdekmérlegelési teszt alaposságát, és a rendszerrel végzett adatkezelés jogszerűségét.

6.4.1. Megállapítható a GDPR hatálya?

A nemzeti hatóság első feladata az eljárás során megállapítani, hogy a GDPR rendelkezései alkalmazhatóak-e az adatkezelésre, ugyanis ez adja meg a felhatalmazást a NAIH-nak az eljárás lefolytatására. Mivel az adatkezelés az Unió területén történik, Uniós állampolgárok adataival kapcsolatban, ezért a megállapítható, a rendelet hatálya kiterjed a hanganalitikára. Az adatvédelmi rendelet 4. cikke kimondja, hogy az a személyes adatként való minősítéshez, akár a közvetett azonosíthatóság is elegendő. Ezt támasztja alá ez Európai Bíróság C-184/20[88] ügye is, amiben a Bíróság kimondta, hogy amennyiben akár közvetett úton azonosítani lehet az érinett személyt, az már a GDPR szerinti adatkezelésnek minősül. Bár a bank először azzal érvelt, hogy a szoftver nem tárol azonosítható adatokat, valamint az elemzett eredmény a hívó és az ügyfélszolgálatos munkatárs vonatkozásában nem személyes adat, mert nem köthető senkihez. Ezt a nyilvánvalóan hamis állítást a Budapest Bank maga cáfolta meg (már csak azért is, mert ha nem lehetne összekötni a hangot egy ügyféllel sem, nem lenne egyértelmű hogy kit kell visszahívni),a korábbi ügy során válaszlevelében, ahol elmondta, hogy az ügyfélszolgálati hívások egyedi belső azonosítószámmal vannak ellátva, amely a szoftveren kívül, de az bank rendszerint belül összeköthető a hívó féllel és az ügyfélszolgálatos kollégával is. Ezt az egyedi

[88] C-184/20 sz. ügy a Litván etikai főbizottság vs. QP, mint állami közintézmény

azonosítót álnévként a szoftver is használja, így össze lehet kötni az ügyfelet a hangjával, ez az összekötés pedig meg is történik, mikor megállapításra kerül, hogy kit kell visszahívni. Ezt az értelmezést támasztja alá az Európai Unió Bíróságának Patrick Breyer vs. Bundesrepublik Deutschland ügyében[89] hozott ítélete. Ebben az ügyben a bíróság kimondta, hogy az IP címek is személyes adatoknak minősülnek abban az esetben, ha az adatkezelők hozzáférhetnek a szolgáltatóktól ahhoz az információhoz, hogy egy meghatározott időpontban egy IP címhez melyik előfizető tartozott.

6.4.2. Az adatok minősége

Döntésében a Hatóság megállapította, hogy az eljárás során kezelt adatok a GDPR 9.cikke szerint különleges személyes adatnak nem minősölnek. Döntésüket azzal indokolták, hogy a kezelt adatok közül egyedül a érzelem (pszichikai állapot) minősülhetne különleges személyes adatnak, (aminek a kezelése a rendelet alapján tilos), de az összes körülmény figyelembe vételével, mégsem lehet ekként értékelni, mert a hangelemzés során nem jön létre olyan adat, amivel az érintett egyedileg azonosítható lenne így a biometrikus adat ezen feltétele hiányzik. Nem tekinthető egészségügyi adatnak sem, mert az érintett mentális és fizikai egészségére vonatkozóan következtetést nem lehet levonni.[90]

6.4.3. Mesterséges Intelligencia felhasználása a hangelemzéshez

Az ügy előzmény eljárásban a Budapest Bank úgy nyilatkozott, hogy a szoftver mesterséges intelligencia és automatizált döntéshozatal felhasználása nélkül működik. A Hatóság döntésében nem hozta nyilvánosságra a céget, akitől a bank a szoftvert megvásárolta, azonban ismeretes, hogy a meg nem nevezett cég honlapjáról, illetve a Hatóság további tájékozódásából kiderül, hogy a rendszer igenis használ mesterséges intelligenciát, valamint automtatizált döntéshozatalt is. Az MI fogalma korábban már kifejtésre került, így a gépi tanulás sem maradhat kivétel. A gépi tanulás (Machine Learning) a mesterséges intelligencia egy típusa, amely lehetővé teszi a szoftveralkalmazások számára, hogy pontosabbá tegyék az eredmények előrejelzését anélkül, hogy kifejezetten erre programoznák őket. A gépi tanulási algoritmusok múltbeli adatokat használnak bemenetként az új kimeneti értékek előrejelzéséhez.[91] Természetesen a gépi tanulásnak is több módját lehet megkülönböztetni, ezek közül az egyik a

[89]C-582/14 sz. ügy Breyer vs. Bundesrepublik Deutschland
[90]NAIH-85/2022 (NAIH-7350/2021) sz. döntés
[91]TECH TAEGER https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML

neurális hálózatok alkalmazása. Ennek lényege, hogy a neurális hálózatok módszertan képes tanulási fázisban önmaga fejlesztésére, ezáltal pontosabb becslési hatékonyság megvalósítására. Amikor az információ keresztül halad a neurális hálózaton, a rendszer érzékeli az elvárt és tényleges kimeneti adatok között az eltérést, így változtatja a paramétereit. Minél több adat halad keresztül a hálózaton, annál pontosabb becslést biztosít a rendszer.[92] Ennek a képességnek birtokában lehet képes a szoftver arra, hogy kiértékelje, és bizonyos szempontok szerint ellenőrizze a hívást. Ilyen szempont lehet, hogy greeting rule-nak megfelelően elég illedelmesen köszöntette-e az ügyfélszolgálatos munkatárs a bank ügyfelét a hívás elején.

Az általános adatvédelmi rendelet külön is foglalkozik a profilalkotással és a részben abból származtatható automatizált döntéshozatali mechanizmussal. Önmagában az automatizált döntéshozatal az a képesség, hogy technológiai eszközök segítségével, emberi beavatkozás nélkül döntenek.[93] Profilalkotásról akkor beszélünk, ha valamilyen formájú automatizált adatkezelés történik személyes adatok tekintetében és a profilalkotás célja egy természetes személy személyes jellemzőinek értékelése Nem nehéz elképzelni, hogy az emberi beavatkozás nélkül az automatikus döntéshozatali mechanizmus során keletkező profilalkotás könnyedén ráerősíthet a sztereotípiákra, vagy meghatározott jellemzők alapján csoportosítaná az embereket. Így a módszer felhasználása, amellyel legyakrabban a multik és a pénzügyi szektor szereplői élnek, megfelelő biztosítékokat kíván. Biztosítékként szolgálhat a tömör és érthető tájékoztatáshoz való jog, a tiltakozáshoz való jog, a hozzáféréshez való jog is. A profilalkotás további feltétele, hogy tisztességes és átlátható legyen. Továbbá az adatkezelőknek képesnek kell lenniük arra, hogy világosan megmagyarázzák és indokolják, hogy miért van szükség a személyes adatokat gyűjtésére és tárolására, vagy pedig fontolóra kell venniük, hogy a profilalkotáshoz összesített, anonimizált vagy (ha ez elegendő védelmet biztosít) álnevesített adatokat használjanak.[94]

Ezek alapján megállapítható, hogy a Bank az adatkezelés során mesterséges intelligenciát és automatizált döntéshozatalt alkalmaz, amelyek segítségével jön létre az a rangsor, ami alapján az ügyfelek visszahívásra kerülnek, valamint ami alapján az ügyfélszolgálaton dolgozó kollégák munkáját értékelik. Ebből megállapítható, hogy a folyamat során a GDPR 4. cikk (4) pontja szerinti profilalkotásra is sor kerül.[95] Ezek a tények, nem csak az adatkezelés kockázatát

[92] KOVÁCS Róbert: Neurális hálózatok – a mesterséges intelligencia Szent Grálja https://mesterin.hu/neuralis-halozatok-a-mesterseges-intelligencia-szent-gralja/
[93] 29-es cikk szerinti adatvédelmi munkacsoport iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához
[94] WP 29-es iránymutatás
[95] GDPR 4. cikk (4): személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére,

növelik, de az érintett személyek vonatkozásában is jelentőségük van, ugyanakkor elmondható, hogy használatával csökken a befektetett erőforrás, valamint alkalmas a piac szegmentálására, vagy a termékek egyéni igényekhez történő igazítására.

6.4.4. A tájékoztatáshoz és a tiltakozáshoz való jog (nem) biztosítása

Az uniós jogban az átláthatóság elve megköveteli, hogy minden személyes adatkezelés általánosságban legyen átlátható az egyének számára. Az egyéneknek joguk van tudni, hogy a rájuk vonatkozó személyes adatok közül melyeket és hogyan gyűjtik, használják fel, valamint tájékoztatást kell adni számukra a személyes adatok kezelésével összefüggő kockázatokról, garanciákról és jogaikról.[96] A banknak mind a hívások elején, mind a honlapon megtalálható üzletszabályzatban a tájékoztatást az átláthatóság elvét szem előtt tartva kellett volna megadnia, úgy, hogy az egy laikus számára is kielégítő tájékoztatást nyújtson. Az átlátható tájékoztatást a profilalkotás tekintetében is elmulasztotta a bank, ugyanis profilalkotás végzése esetén a GDPR 60. preambulumbekezdése szerint ebben az esetben tömören és egyértelműen tájékoztatni kellett volna az érintettet arról, hogy köteles-e a személyes adatairól nyilatkozni, valamint, hogy milyen következményei lehetnek az adatszolgáltatás elmaradásának. A korábban említettek bizonyítják, hogy ezzel a bank is tisztában, volt, és ennek ellenére sem változtatott a gyakorlatán.

Tekintettel arra, hogy az érintett ügyfelek nem voltak a szükséges ismeretek tudatában, értelemszerűen a tiltakozáshoz való joguk is némiképp kiüresedett. Főszabály szerint abban az esetben, ha az adatkezelést jogos érdekre alapozták (ideértve a profilalkotást is), az érintettnek joga van tiltakozni, ebben az esetben adatait nem lehet tovább kezelni „kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.”[97] Az EUB tisztázta, hogy az érintett jogai „főszabályként” megelőzik az adatkezelő gazdasági érdekeit „a kérdéses információ jellegétől, illetve attól is függően, hogy az információ mennyire érzékeny az érintett személy magánélete szempontjából, illetve hogy a nyilvánosságnak milyen érdeke

különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják

[96]GDPR 39. preambulumbekezdés

[97]GDPR 21. cikk (1) bekezdés

fűződik ezen információ megszerzéséhez.[98] Ebben az esetben az a tény, hogy a szoftver panaszmentesen üzemelt az üzembe helyezés óta, nem azt támasztja alá, hogy a Bank ügyfelei tudtak erről az adatkezelésről, de nem zavarta őket, hanem azt, hogy nem volt átfogó képük arról, mi is történik az adataikkal.

6.5. A jogsértések értékelése

Ahogy arról korábban már szó volt, abban az esetben, ha az adatkezelő a jogos érdeket jelöli meg jogalapként, úgy a GDPR alapján az érdekmérlegelés elkészítése kötelező. A Hatóság értékelése szerint, bár elkészült a dokumentum, az mégsem felel meg az átláthatósági követelményeknek, mert nem támasztja alá az adatkezelés célját, az adatkezelést nem a szükségesség arányosság szempontjai szerint vizsgálja, hanem kizárólag saját érdekeit mérlegeli benne (azzal együtt, hogy a Hatóság számára megküldött dokumentumokból kiderül, hogy a rendszer hatékonysága megkérdőjelezhető, hiszen az esetek 91,96%[99] százalékában nem ismerte fel az érzelmeket). Csak az összehasonlítás kedvéért, az izraeli székhelyű Nemesysco hangelemzéssel foglalkozó vállalat saját bevallása szerint, rétegzett hangelemző rendszer használatával is csak 42%-ban detektált helyesen.[100]

Az érdekmérlegelésről elmondható továbbá, hogy semmilyen adatot nem tartalmaz arra vonatkozóan, hogy sor került- e bármikor is annak felülvizsgálatára. A dokumentumban a bank megállapította, hogy saját céljai eléréséhez szükséges az adatkezelés, de az érintetti jogok sérülésének lehetősségét nem vizsgálta. Kimondottan jogsértően járt el a tájékoztatáshoz és a tiltakozáshoz való jog tekintetében. A tájékoztatáshoz való joggal kapcsolatban elmondható, hogy a bank munkatársa még konkrét kérdésekre sem tudott olyan válaszokat adni, ami azt eredményezte volna, hogy az érintett olyan helyzetbe kerüljön, hogy adataival kapcsolatban megfontolt döntést hozzon. A tiltakozási jogukat pedig csak a hívás megbontásával volt lehetőségük gyakorolni, ami ellehetetlenítette volna az ügyintézésüket, így megállapítható, hogy a tiltakozáshoz való jog lényegében kiüresedett. [101] A Hatóság úgy ítélte meg, hogy az érdekmérlegelés nem ad valós képet, így az az értelmezés, hogy az ehhez kötődő jogos érdek elsőbbsége állapítható meg az érintett személyek jogainak védelmével szemben, nem megfelelő.

[98]C-131/12.sz. ügy Google Spain SL, Google Inc. kontra Agencia Española de Protección de Datos (AEPD), Mario Costeja González
[99]NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021
[100]The amazing potential of voice analytics https://www.forbes.com/sites/bernardmarr/2016/08/08/the-amazing-potential-of-voice-analytics/?sh=442718584f77
[101]NAIH-85-3/2022 Korábbi ügyszám: NAIH-7350/2021

6.6. A bírság mértéke

A fent ismetett eljárás nemcsak azért kavart nagy pont Magyarországon, mert első ízben szankcionált egy mesterséges intelligencia alapú adatkezelést, hanem azért is, mert a bírság mértéke magasabb volt, minden korábbinál. Csak a mihez tartást végett meg kell említeni, hogy ez a 250 millió forintos bírság magasabb mint 2021-es évben kiszabott bírságok együttvéve, akkor ugyanis a Hatóság minösszesen 68.1 millió forintot szabott ki. [102] A GDPR alapján a felügyeleti hatóságnak joga van bírságot kiszabni akár más szankciókkal együttesen is. Az adatvédelmi rendelet a jogsértés jellege szerint határozza meg a kiszabható bírság maximumát. Jelen esetben több ízben került sor a GDPR megsértéséré, így a 83. cikk a bírság mértéke nem lehet több, mint 20 millió euró vagy vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeggel kell sújtani, azzal, hogy a kettő közül azt kell kiszabni, amelyik magasabb.[103]

Az Európai Adatvédelmi Testület (a továbbiakban EDPB) is kiadott egy iránymutatást a bírság kiszabásával kapcsolatban. Ebben egy 5 lépcsős hangsúlyozzák, hogy minden ügyet egyedileg az összes körülményt együttesen véve kell megvizsgálni, mert csak így lehet garantálni, hogy a jogsértés mértékével arányos, illetve alkalmas lesz arra, hogy a jövőbeni hasonló magatartásoktól távol tartsa az érintettet.[104]

A bíráson kívül a Hatóság arra is kötelezte az érintetett, hogy módosítsa az adatkezelési gyakorlatát, hogy az megfeleljen az adatvédelmi rendeletnek, azaz a hangelemzés során az érzelmeket ne elemezze és biztosítsa az érintetteknek az őket megillető jogaikat, különös tekintettel a tájékoztatáshoz és a tiltakozáshoz való jogokra. A munkavállalókkal kapcsolatos hangelemzés tekintetében pedig el kell végezni erre adatkezelésre külön egy érdekmérlegelést kell elkészíteni, aminek ki kell térnie arra az alá-fölé rendelt viszonyra, ami a munkaviszonyból származik, külön ki kell térnie azokra a biztonsági garanciákra, amik a visszaélést megakadályozhatják. Az adatkezelést cél elérésére szükséges mértékre kell korlátozni azzal, hogy meg kell adni a munkavállalók számára minden információt az értékelési szabályokkal kapcsolatban. A Budapest Banknak 60 napja volt megteremteni a jogszerű adatkezelés kereteit vagy leállítani az adatkezelést.

[102]NAIH beszámoló a 2021-es év tevékenységéről 2022. 03.31. 30. https://www.naih.hu/eves-beszamolok?download=507:naih-beszamolo-a-2021-evi-tevekenysegrol
[103]GDPR 83. cikk (5) bekezdés
[104]Guidelines 04/2022 on the calculation of administrative fines under the GDPR https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

6.7. Lehet ezt jól csinálni?

Amennyi haszna van az ügyfelek / fogyasztók adatainak egy vállalkozás számára, éppen annyira teheti pokollá annak napjait, hogy az adatok védelmét maximálisan garantálni tudja, az egyre növekvő kihívásokkal szemben. Hatványozottan igaz ez az állítás, azokra, a cégekre, akik call centert is üzemeltetnek, ezért a címben feltett kérdésre elsőre talán a válasz egy egyszerű nem. Az EDPB az Európai Adatvédelmi biztossal összhangban a témáról akképp nyilatkozott, hogy természetes személyek érzelmeinek levezetésére való felhasználása rendkívül nemkívánatos. [105] A korábban hosszasan elemzett NAIH döntés is ezt az álláspontot támasztja alá, azonban Péterfalvi Attila, a Nemzeti Adatvédelmi és Információszabadság Hatóság jelenlegi elnöke nemrégiben a témát érintően interjút adott a Portfolio magazinnak, amiben arra a kérdésre, hogy lehet-e egy ilyen technológiát szabályszerűen alkalmazni, a következőket mondta: „Az ördög a részletekben rejlik, az az alapvető kérdés, hogy az érintettet miről tájékoztatják, és milyen adatokat vizsgál, kutat a mesterséges intelligencia.”[106]

Mi, XXI. századi emberek egy felugró ablakban egy egyszerű érintéssel hozzájárulunk ahhoz, hogy Siri vagy Alexa passzívan ott legyen és hallgassa minden beszélgetésünket, majd az említett témáknak megfelelő tartalmakkal árasszon el bennünket különböző online platformokon[107]. Ebben az esetben a felhasználó aktív tevőleges magatartással járul hozzá ahhoz, hogy az általa kimondott információk felhasználásra kerüljenek. Richard Brown, az internet-, hálózati, hang- és biztonsági megoldásokat kínáló Activereach igazgatója rámutat: "A legtöbb ügyfél feltételezi, hogy a céggel folytatott e-mailes kommunikációjukat hosszú távon tárolhatják, de nem feltétlenül gondolják, hogy ez a hangalapú beszélgetések esetében is így van".[108] Ahogy erre Brown is rávilágít, az érintettek tájékoztatása kulcsfontosságú egy ilyen típusú adatkezelés tekintetében, végső soron a jogszerűség egyik záloga. Brian Martin, a Spitch nevezetű emberi hangadat elemzési megoldásokat kínáló svájci vállalat regionális igazgatója kiegészíti azzal, hogy "el kell mondani az ügyfeleknek, hogy gyűjtik a hangnyomatukat, és meg kell említenie az ezzel járó előnyöket; például a gyorsabb kiszolgálást, a személyre szabott

[105] Az Európai Adatvédelmi Testület és az adatvédelmi Biztos 5/2021.sz. közös véleménye a mesterséges intelligenciáról. 35. bekezdés https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_hu.pdf

[106] TURZÓ Ádám Pál:Terjed az AI és a felhő a bankokban – Péterfalvi Attila elárulta mire kell nagyon figyelni https://www.portfolio.hu/uzlet/20220928/terjed-az-ai-es-a-felho-a-bankokban-peterfalvi-attila-elarulta-mire-kell-nagyon-figyelni-569465#

[107] Alexa and Alexa Device https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230

[108]Bernard MARR: The amazing potential of voice analytics https://www.forbes.com/sites/bernardmarr/2016/08/08/the-amazing-potential-of-voice-analytics/?sh=442718584f77

figyelmet és a nagyobb fokú biztonságot". A fogyasztónak fel kell ajánlani a lehetőséget, hogy lemondjon a hangadatainak rögzítéséről, és akkor is hozzáférhessen a szolgáltatásokhoz, ha ezt megteszi.[109]

A leírtak alapján, ha elfogadjuk azt az állítást, hogy az Európai Adtavédelmi Testület nem tiltotta meg, csupán nemkívánatossá nyilvánította az eljárást, akkor azt kell mondanunk, hogy bár nagyon szigorú feltételek mellett, de lehet alkalmazni a hanganalitikát, az adatminimalizálás elvét tiszteletben tartva. Ez azért fontos, mert a technológia fejlettségi szintjét tekintve, hamarosan már nemcsak a beszélő érzelmi állapotát, hanem testalkatát, betegségét, szélsőséges esetben magasságát is meg lehet majd mondani. Ennek az elsődleges feltétele az alapos és minden részletre kiterjedő érdekmérlegelés és hatásvizsgálat elkészítése, amely bemutatja az adatkezelés célját és minden körülményét, különös tekintettel a kockázatok enyhítésére tett intézkedésekre, pontosan megjelölve a felülvizsgálat dátumát. Másodsorban az adatkezelés jogalapjaként a GDPR 6. cikk (1) bekezdés a) pontja szerint a hozzájárulást kell megjelölni. Ennek a hozzájárulásnak egy aktív, tevőleges magatartásban kell megnyilvánulnia akképpen, hogy a hozzájárulás megtagadása, vagyis a tiltakozáshoz való jog gyakorlása nem jelentheti az ügyintézést ellehetetlenülését. Harmadrészt nagyon fontos az ügyfél tájékoztatása. Nemcsak arról, hogy milyen adatokat kezelnek róla és milyen célból, de arról is informálni kell, hogy milyen előnyeit élvezheti annak, hogy hozzájárul a hangelemzéshez. A tájékoztatást úgy kell megtenni, hogy az érthető világos, mégis a lehetőségekhez mérten tömör legyen, és a témában nem jártas személyek is megismerhessék az adatkezelés lényegét. Az ügyfél tájékoztatásának eszköze a szóbeli figyelmeztetés a hívás elején, valamint az adatkezelési tájékoztató hozzáférhetővé tétele a bank online felületein. Fontos továbbá, az ügyfélszolgálaton dolgozó munkavállalók tudásának folyamatos bővítése. Figyelembe kell venni továbbá, hogy a mesterséges intelligencia egy rendívül gyors ütemben fejlődő ‘iparág’,így gyakran igény mutatkozhat a rá vonatkozó szabályozás módosítására, ezért a felhasználóknak olyan belső rendszert kell kialakítaniuk, amellyel a jogszabályok változásától függetlenül folyamatosan biztosítani tudják a jogszerű működést.

[109]BRIAN Martin:GDPR Iplication for spech technology: https://spitch.ai/blog/gdpr-implications-for-speech-technology/

Összegzés

Dolgozatom során igyekeztem bemutatni, hogy hogyan viszonyul az Európai Unió a mesterséges intelligencia felhasználáshoz, egy olyan területen, amelyre eddig a témában kevés figyelem hárult. A dolgozat folyamán ismertettem a hanganalitika szoftverek működésének lényegét, és felhasználásának célját. Véleményem szerint jól látszik a két bemutatott régió adatvédelemhez való hozzáállásból, hogy az uniós államok polgárai sokkal nagyobb biztonságban tudhatják az adataikat, valamint az adatvédelmi tudatosság is mindinkább jellemző rájuk. Nem titkolt célom volt a dolgozatommal hogy részletesen bemutassam az MI alapú hangelemző rendszereket, bizonyítva ezzel azt, hogy van helye a rendszer jogszerű felhasználásnak, mert megfelelő biztonsági intézkedésekkel minimálisra csökkenthetőek a kockázatok.

Véleményem szerint az Európai Adatvédelmi Testületnek nemkívánatos helyett megengedetté kellene nyilvánítania az ilyen fajta adatkezelést, abban az esetben, ha mind a GDPR-nak és egyéb az adott országban hatályban lévő kapcsolódó jogszabályoknak, mind pedig a mesterséges intelligencia rendeletnek megfelel. Kikötve azt a tényt, hogy a hangelemző rendszert kizárólag az ügyfélszolgálatokon történő hívásokra lehet alkalmazni, azokkal marketing tevékenységet végezni nem lehet. Ezzel a kikötéssel garantálni lehet, hogy a rendszer ténylegesen arra kerül felhasználásra, hogy az ügyfél ügyintézése során felmerülő problémák az a lehető leggyorsabban elháruljanak.

Az adatvádelem szempontjából fontos, hogy az adatkezelés jogalapja megfelelően legyen kiválasztva, ez mindennél fontosabb, hiszen enélkül a szabályos adatkezelés meghiúsul. Amennyiben jogalapnak a hozzájárulás kerül megjelölésre nem pedig a jogos érdek, úgy a szoftver felhasználójának be kellene gyűjtenie az ügyfelek kifejezett hozzájárulását, amit meg kell előznie megfelelő tájékoztatásnak. A tájékoztatásnak ki kell terjednie az esetleges kockázatokra, az ezek elkerülésére tett intézkedésekre és nem utolsó sorban azokra a lehetőségekre, amiket ez a rendszer magában hordoz. Jelenleg elsősorban az ügyintézési idő lerövidülését lehet garantálni, a problémák gyorsabb felismerése által, de amilyen ütemben fejlődik az érintett terület, könnyen lehet, hogy hamarosan még több előnyt fog jelenteni. Meg kell azonban adni a lehetőséget az ügyfeleknek, hogy a megfelelő tájékoztatás után maguk mérlegeljenek, hogy kívánják-e ezt típusú adatkezelést vagy sem. Amennyiben nem, vagy bármikor az ügyfél a tiltakozáshoz való jogával él a hangja elemzésével kapcsolatos adatkezelés onnantól a kérvényező tekintetében fel kell függeszteni. Fontos azonban elmondani, hogy

emiatt olyan hátrány nem érheti, ami az ügyintézését teljesen ellehetetlenítené. A szoftver felhasználójának el kell készítenie a hatásvizsgálatot, a GDPR-ban meghatározott alapossággal eljárva, meghatározva annak a felölvizsgálati dátumát.

Ami pedig a mesterséges intelligenciát illeti, az AI tervezet kockázat alapú megközelítése alapján egy ilyen szoftver magas kockázatúnak kell, hogy minősüljön. Ezen besorolás szerint kell eljárni vele kapcsolatban és elkészíteni minden olyan beadványt, amit a rendelet megjelöl, mert ezekkel lehet garantálni, a biztonságos és átlátható működést. Természetesen az imént említett tájékoztatáshoz való jogba bele kell tartoznia annak is, hogy a személyeket informálják a tényről, hogy mesterséges intelligencia segítségével működik a rendszer.

Az amerikai helyzet ismertetését azért éreztem szükségesnek, mert jól érzékelteti a hozzáállásból fakadó különbségeket. Véleményem szerint GDPR megadja a kellő biztonságot az adatoknak, azonban szerintem fontos, hogy a jogalkotás ne álljon a fejlődés útjában, márpedig, ha egy új rendszert nemkívánatosnak minősítenek, azzal pontosan ezt lehet elérni azzal együtt, hogy növeli a társadalomban a félelmet, illetve a bizonytalanságot a rendszerrel szemben. Pedig a mesterséges intelligencia az életünk része és talán el sem tudjuk képzelni, mennyire lesz az a jövőben, így fontos, hogy ne váltson ki szorongást az emberekből. Ezt pedig úgy lehet elérni, hogy tudatosan megfelelő biztosítékokkal ellátott rendszerekkel találkozunk mindennapi életünk során. Ez a fajta magatartás fogja elhozni a változást a társadalomba is, mert a nyitottság elengedhetetlen egy olyan korban, ahol a fejlődés és a változás a mindennapok szerves része lett.

Irodalomjegyzék

Az internetes linkek egységes letöltési dátuma: 2022. november 11.

Jogszabályok:

15/1991 AB Határozat II. fejezet

2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról 53§ (1)

2016. évi CL. törvény az Általános Közigazgatási Rendtartásról

29-es adatvédelmi munkacsoport WP 248 rev.01 számú iránymutatása

Általános Adatvédelmi Rendelet. (15.) preambulumbekezdés, (39) preambulumbekezdés, (47) preambulumbekezdés,4. cikk (4) bekezdés 6. cikk (1) bekezdés f), 35. cikk, 51. cikk (1) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679#d1e4614-1-1

Az Európai Adatvédelmi Testület és az adatvédelmi Biztos 5/2021.sz. közös véleménye a mesterséges intelligenciáról. 35. bekezdés https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_hu.pdf

Az Európai Parlament és Tanács 95/46 EK Irányelve (2-3) preambulumbekezdés https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:31995L0046&from=HU

Az Európai Unió Alapjogi Cartája (2012/C 326/02) 8. cikk

Guidelines 04/2022 on the calculation of administrative fines under the GDPR https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

Javaslat az Európai Parlament és Tanács Mesterséges Intelligenciára vonatkozó rendelet tervezetéről https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52021PC0206 bevezető 5. és 7. pont I. sz melléklet

Magyaroszág mesterséges intelligencia stratégiája 2020. május 16. https://ai-hungary.com/api/v1/companies/15/files/137203/view

Jogesetek:

C-131/12. sz. ügy Google Spain SL, Google Inc. kontra Agencia Española de Protección de Datos (AEPD), Mario Costeja González

C-184/20 sz. ügy a Litván etikai főbizottság vs. QP, mint állami közintézmény

C-582/14 sz. ügy Breyer vs. Bundesrepublik Deutschland

NAIH/2019/769. sz. határozat

NAIH/2020/2758/4 sz. határozata

NAIH-85/2022 (NAIH-7350/2021) https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei

Könyvek, és tanulmányok:

[1]29-es cikk szerinti adatvédelmi munkacsoport iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához
A Nemzeti Adatvédelmi és Információszabadság Hatóság általános adatvédelmi rendelettel kapcsolatos állásfoglalásai Magyar Közlöny Lap ás Könyvkiadó kft Budapest, 2019 250.

A személyes adatok védelme: https://www.europarl.europa.eu/ftu/pdf/hu/FTU_4.2.8.pdf

Az Európai Uniós adatvédelmi biztos összefoglaló véleménye a Fehér könyvről 2020. 06.29. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020XX1117(01)&from=EN

Bernard GALLAGHER: Will the US adopt a nationwide data privacy lae similar to GDPR? https://www.ispartnersllc.com/blog/us-nationwide-data-privacy-law-gdpr/

Bernard MARR: The amazing potential of voice analytics https://www.forbes.com/sites/bernardmarr/2016/08/08/the-amazing-potential-of-voice-analytics/?sh=442718584f77

CUMMINS, N.:"You sound ill, take the day off": automatic recognition of speech affected by upper respiratory tract infection. In: IEEE EMBC, pp. 3806–3809 (2017)

Fotóművészet Magazin 2004/3-4 XLVII éfolyam Pfisztner Gábor: Photokina 2004
GYEKICZKY Tamás: Jogrendszerek a digitális társadalomban, Wolters Kluwer Kiadó 2020 Budapest 23.
History of the General Protection Regulation:https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Jacob Leon KRÖGER, Otto HANS-MARTIN LUTZ and Philip RASCHKE Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference https://link.springer.com/content/pdf/10.1007/978-3-030-42504-3_16.pdf 249
Jennifer STODDART: Thirty years after the OECD privacy guildline https://www.oecd.org/sti/ieconomy/49710223.pdf

JÓRI András, SOÓS Andrea Klára: Adatvédelmi jog magyar és európai szabályozása HVG-Orac Lap- és Könyvkiadó Kft. 75.

JÓRI András: Az adatvédelem alapjai 2019.04.02. HVG Orac Budapest https://gdpr.orac.hu/wp-content/uploads/szeminarium/GDPR_kepzes_20190402_Adatvedelmi_alapok.pdf

JÓRI András:Adatvédelmi Kézikönyv, Budapest, Osiris Kiadó 2005 53.

Kenneth CUKURIER: Data, data everywhere. The Economist, London, 2010. http://econ.st/3gqggaw

Michael KIRBY The history, achievement and future of the 1980 OECD guidelines on privacy 2011

DR.ÁRVAY Viktor, dr. BENDIK Tamás, dr. BOJNÁR Katinka, dr. BUZÁS Péter, dr.ESZTER Dániel, Dr. MAJSA Ágnes, dr. OSZTOPÁNI Krisztián,dr. PÉTERFALVI Attila, dr. RÉVÉSZ Balázs, dr. SZIKLAY Júlia : Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., . Budapest 2021 14.,27.,83. 157.

SOSKIN, W.F., KAUFFMAN, P.E.: Judgment of emotion in word-free voice samples. J. Commun. 11(2), 73–80 (1961) https://doi.org/10.1111/j.1460-2466.1961.tb00331.x

SZŐKE Gergely László: ADATVÉDELEM ÉS ÖNSZABÁLYOZÁS. ADATVÉDELMI IRÁNYÍTÁSI RENDSZER AZ ADATKEZELŐKNÉL doktori értekezés Pécs, 2014.
SZŐKE Gergely László: Az európai adatvédelmi jog megújítása, tendenciák és lehetőségek az önszabályozás területén Budapest, 2015 25., 27. és 51.

The history of artificial intelligence University of Washington https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf

TÖRÖK Bernát és ZŐDI ZSOLT: A mesterséges intelligencia szabályozási kihívásai, Ludovika Egyetem Kiadó Budapest, 2021 44.

ZAVODNYIK József: A NAIH általános adatvédelmi rendelettel kapcsolatos 2019-es értelmezései Wolters Kluwer Budapest, 2020 182.

További internetes cikkek:

Mae WEST: It's not what you say, but how you say it Album: send me home, kiadás éve:2018

Az adat fogalma: https://www.merriam-webster.com/dictionary/data

What is speech analitics? https://www.techtarget.com/searchcustomerexperience/definition/speech-analytics

What is voice analytics? https://justcall.io/blog/what-is-voice-analytics.html#How_does_voice_analytics_work

Milyen veszélyeket rejt a mesterséges intelligencia? https://itmap.hu/milyen-veszelyeket-rejt-a-mesterseges-intelligencia/

Ed BURNS Machine Learning definiton TECH TAEGER https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML

KOVÁCS Róbert: Neurális hálózatok – a mesterséges intelligencia Szent Grálja https://mesterin.hu/neuralis-halozatok-a-mesterseges-intelligencia-szent-gralja/

TURZÓ Ádám Pál: Terjed az AI és a felhő a bankokban – Péterfalvi Attila elárulta mire kell nagyon figyelni 2022.09.28. https://www.portfolio.hu/uzlet/20220928/terjed-az-ai-es-a-felho-a-bankokban-peterfalvi-attila-elarulta-mire-kell-nagyon-figyelni-569465#

Brooke AUXIER, Lee RAINIE, Monica ANDERSON, Andrew PERRIN, Madhu KUMAR, Erica TURNER 2019.11.15. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information

Xdroid.com VoiceAnalytics https://xdroid.hu/hangelemzes

PWC: Mennyit ér az adat? 2018.https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/data_monetization_2018_web.pdf

Alexa and Alexa Device https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230

NAIH beszámoló a 2021-es év tevékenységéről 2022. 03.31. 30. https://www.naih.hu/eves-beszamolok?download=507:naih-beszamolo-a-2021-evi-tevekenysegrol

BRIAN Martin: GDPR Iplication for spech technology 2018.05.16. https://spitch.ai/blog/gdpr-implications-for-speech-technology/
Schrems II. ítélet, avagy a Privacy Shield halála 2020.08.04. https://gdpr.news.hu/cikkek/schrems-ii-itelet-avagy-a-privacy-shield-halala-1-resz/

DR. IVANICS Krisztina 2020.09.08. Az adatnak mennie kell? https://www.adatvedelmiszakerto.hu/2020/09/a-schrems-ii-itelet-utan-az-adatnak-mennie-kell/

MOLNÁR Balázs 2021.10.12. Kína lenyomja a világot? Itt már lépéselőnyben van https://haszon.hu/megorizni/vilag/kina-usa-mesterseges-intelligencia

Fotóművészet Magazin 2004/3-4 XLVII évfolyam Pfisztner Gábor: Photokina 2004

Ma egyesül a Budapest és az MKB Bank 2022.03.31. https://www.portfolio.hu/bank/20220331/ma-egyesul-a-budapest-bank-es-az-mkb-bank-itt-vannak-a-tudnivalok-536713

Biggest GDPR fines so far 2022.05.05. https://www.tessian.com/blog/biggest-gdpr-fines-2020/

Legalisation Related to AI 2022.08.26. https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx
KOI Tamás: 2022.11.17. Minden hívást beszédanalízissel vizsgál a Telenor ügyfélszolgálata https://www.hwsw.hu/hirek/47708/telenor-nextent-ugyfelszolgalat-voice-miner-hanganalizis.html