Jelentés

Magyarországon működő bankoknál alkalmazott mesterséges intelligencia (MI) rendszerek személyes adatokat érintő adatkezeléséről

1. ELŐZMÉNYEK

Az Európai Unió mesterséges intelligenciáról szóló rendelete[1] (a továbbiakban: **MI rendelet**) 2024. július 12-én jelent meg. Az MI rendelet 2024. augusztus 1-jén lépett hatályba. Az MI rendelet rendelkezéseit fokozatosan kell alkalmazni a következő években, az MI rendszerek különböző kategóriáihoz meghatározott eltérő határidőkkel.

Magyarországon a 2025. december 1-től hatályos 2025. évi LXXV. törvény valamint az annak végrehajtásáról szóló 344/2025.(X.31.) Korm. rendelet alapján a Magyar Mesterséges Intelligencia Tanács jogosult az MI rendelet végrehajtásával összefüggő iránymutatások, állásfoglalások kiadására. A fenti tagállami jogszabályok alapján a nemzetgazdasági miniszter gondoskodik az MI rendelet 70. cikke szerinti piacfelügyeleti hatósági, valamint az egyedüli kapcsolattartó pont működtetésével kapcsolatos feladatok ellátásáról, továbbá a Nemzeti Akkreditáló Hatóság látja el az MI rendelet 28. cikke szerinti bejelentő hatósági feladatokat

Az Európai Unió Bizottsága 2025. július 07. napján kibocsátott egy iránymutatást a 2024/1689 rendelet (a továbbiakban: **MI rendelet**) által meghatározott mesterségesintelligencia-rendszerek fogalommeghatározásáról.[2] Az MI rendelet 3. cikkének 1. pontja[3] tartalmazza az MI-rendszer fogalmának meghatározásánál az olyan rendszereket, melyek előrejelzéseket generálnak kimenetekként. Az iránymutatás szerint a „*gépi tanulást alkalmazó MI-rendszerek képesek olyan előrejelzéseket generálni, amelyek feltárják az adatok összetett mintázatait, és rendkívül dinamikus és összetett környezetben pontos előrejelzéseket adnak*”, példaként pedig az önvezető autókat és az energiafogyasztási MI-rendszereket mutatja be.[4] Ezzel szemben az egyszerű előrejelző rendszerek *„(…) amelynek teljesítménye egy alapvető statisztikai tanulási szabály segítségével érhető el, bár technikailag besorolható a gépi tanulási*

[1] (EU) 2024/1689 rendelet a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401689

[2] Európai Unió Bizottsága, A Bizottság iránymutatása az (EU) 2024/1689 rendelet (a mesterséges intelligenciáról szóló rendelet) által meghatározott mesterségesintelligencia-rendszerek fogalommeghatározásáról (2025.07.29.) – a továbbiakban: **EB Iránymutatás**

[3] „MI-rendszer”: gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet;

[4] EB Iránymutatás (54)-(55) bekezdések

megközelítésekre támaszkodó rendszerek közé, teljesítménye miatt kívül esik az MI rendszer fogalommeghatározásának hatályán”[5]

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: **Hatóság**) korábban a NAIH-85-3/2022 számú határozatában a Budapest Bank Zrt.-vel szemben szabott ki 250 000 000 Ft bírságot jogellenes adatkezelés miatt, amely mesterséges intelligenciát használt. A Hatóság honlapján magyar[6] és angol[7] nyelven is teljes terjedelemben elérhető határozatában a Hatóság megállapította, hogy a megfelelő tájékoztatás hiányában az érintettek számára az eleve nehezen követhető az MI alkalmazása fokozott kockázatot jelent, ezért több, nem kevesebb erőfeszítést igényel a tájékoztatás megadása az adatkezelő részéről egy korábbi technológián alapuló adatkezeléshez képest. A téma összetettsége nem mentesíti az adatkezelőt a GDPR[8] szerinti kötelezettségei alól, az érintettek tájékoztatása nem hagyható el csak azért, mert az adatkezelő mesterséges intelligenciát is alkalmaz. A tiltakozási jog csak papíron létezése sem felel meg az adatvédelmi szabályoknak. Ha az érintett nem is tud az adatkezelésről, akkor nem is tud ellene tiltakozni, főleg ha semmilyen gyakorlati lehetőséget nem biztosít az adatkezelő erre még az adatkezelés megtörténte előtt. A jogos érdek jogalap alkalmazása esetén a nem megfelelő előzetes érdekmérlegelés – amely ezen esetben sem hagyható el és nem merülhet ki az adatkezelő saját érdekének bemutatásában – az adatkezelés jogszerűségét érinti. Az Európai Adatvédelmi Testület 28/2024 számú véleménye[9] hasznos támpontokat ad az érdekmérlegelés elvégzésére mind az MI tanításával, mind a használatával kapcsolatos adatkezelések esetén.

A Hatóság áttekintést kívánt kapni arról, hogy a magyar bankszektorban 2025-ben az MI rendszerek mely célokból, mely személyes adatokat kezelnek, és ezek jogi megfelelősége miként valósul meg. Ezen típusú adatkezelések a jelenlegi gyors terjedésük és az általuk kezelt személyes adatok mennyisége miatt rendkívüli fontosságúak társadalmi és adatvédelmi szempontból egyaránt. Ennek keretében a Hatóság többek között megkereste a Magyar Nemzeti Bankot, valamint több külön hivatalbóli vizsgálatot indított Magyarországon működő

---

[5] EB Iránymutatás (49) bekezdés

[6] https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei&start=100

[7] https://www.naih.hu/data-protection/decisions?download=522:ai-based-speech-signal-processing-technology-and-data-protection

[8] 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 szóló 2016/679/EU rendelet (a továbbiakban: **GDPR**): https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504#C3-1

[9] https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_hu_0.pdf

bankok adatkezelésével kapcsolatban. A jó gyakorlatok kialakulásának elősegítése érdekében a vizsgálatok eredményét a Hatóság a jelen jelentésben hozza nyilvánosságra. A jelentés a vizsgálatban részt vett bankoknak küldött kérdésekre adott válaszokon alapul. A jelen jelentés célja egy körkép készítése volt, nem adatvédelmi hatósági eljárás lefolytatása a tényállás bizonyítékokon alapuló feltárásával, ezért a Hatóság nem vizsgálta a válaszok pontosságát, és azokat kizárólag a jogszabály által védett információk kiszűrése céljából nézte át a jelen jelentésben történő felhasználás előtt.

2. ÖSSZEGZÉS

A Hatóság a jelen jelentés tárgyát képező adatkezelések vizsgálatát követően az alábbi általános jó gyakorlatokat emeli ki a jelentésben. A jelentés hiánypótló jellegű, a figyelemfelhívás a célja, nem a témakör teljes körű feldolgozása. Mindenképpen léteznek a jelentésben írtakon kívül más jó gyakorlatok is, mivel a jelentés csak a magyar banki szektor egy részéből vett mintán alapul, és az adatkezelők részére a létező jó példákat kívánja megmutatni. A jelen jelentés nem érinti az adtakezelők jogszabályok alapján fennálló kötelezettségeit, és az adatvédelmi megfelelésre fókuszál. Más uniós vagy tagállami jogszabályok eltérő vagy további kötelezettségeket állapíthatnak meg az adatkezelőkre.

Az MI egyik gyakori alkalmazási módja a képek felismerése, abból információ kiolvasása. Fontos megfelelően dokumentálni vagy harmadik fél megoldásának használata esetén információt szerezni és rögzíteni arról, hogy a képeket adatokká átalakító MI modell tanítása során mely forrásból származó, mely adatokat használtak, és miként mérték az MI modell pontosságát. Mivel az azonosítás egyik eredménye, hogy adott személy – sokszor szenzitív banki – személyes adataihoz hozzáférést szerez a felismert érintett, adatvédelmi szempontból is fontos, hogy a felismerés megbízható legyen. A felismeréshez használt élőkép megőrzési idejének megfelelő megválasztása is szükséges a GDPR adattakarékosság és korlátozott tárolhatóság elvének megfeleléshez, az adatbiztonság veszélyeztetése nélkül.

A szöveg és hang felismerése és feldolgozása egy jelenleg népszerű felhasználási módja az MI modelleknek, amely például a virtuális asszisztensek működése során szükséges. Ezek általában a nyomógombos irányítás alternatívájaként jelennek meg, és amíg nem minősülnek a GDPR 22. cikke szerinti automatizált döntéshozatalnak (mivel csak egy menüben egy pont kiválasztását szolgálják gombok használata helyett, vagy előre meghatározott kész válasz mondatokból, tudástárból csak kiválasztják a kérdéshez legközelebbi, amúgy manuálisan is

megkereshető választ), addig általában nem hordoznak érdemi kockázatot. A képek felismerésénél leírtak itt is megfelelően alkalmazandóak.

Az MI modellek tudását nem elsősorban az algoritmus, hanem a tanításra használt adatok határozzák meg. Emiatt nem mindegy, hogy a tanításra használt adatok milyen minőségűek, továbbá szükséges-e adott természetes személyhez köthetőnek lenniük. Amennyiben csak személyes adatokkal lehetséges az adott célra az MI modell tanítása, akkor a jogalap vagy más célra hasznosítás GDPR 6. cikk (4) bekezdése szerinti feltételeinek vizsgálata szükséges, az adatforrás megfelelő dokumentálásával. Az álnevesítés (pszeudonim személyes adattá alakítás) vagy az anonimizálás (véglegesen nem személyhez köthető adattá alakítás) sok esetben használható a tanítást megelőzően az adatvédelmi kockázatok csökkentésére.

A „Shadow AI" használata viszonylag új jelenség. A „shadow AI" gyűjtőfogalomként minden olyan esetet lefed, amelyekben egy adott szervezetnél a felhasználók a szervezet IT infrastruktúrájának igénybevételével az egyes MI rendszereket, akár munkavégzéshez, akár valamilyen személyes felhasználás érdekében a szervezet szempontjából nézve szabályozatlan, nem átlátható, koordinálatlan módon használják. Az adatkezelők által tudatosan és megfelelő garanciák mellett használt eszközökkel ellentétben ilyen esetben az adatkezelő munkavállalói vagy alvállalkozói a saját munkájuk megkönnyítésére az adatkezelő tudta nélkül használnak mesterséges intelligenciát a munkájuk végzéséhez. Mivel ezzel sok személyes adat és más jogszabály alapján védett adat is kikerülhet az adatkezelő irányítása alól, ezért az adatkezelő megfelelő lépéseket kell tegyen ennek elkerülése érdekében mind oktatás, mind szervezeti és eljárási garanciák szintjén. Ez különösen igaz olyan adatkezelők esetén, mint a bankok, amelyek számos szenzitív adatot kezelnek sok érintettről.

A vizsgált bankok működésük során analitikus modelleket is használnak hitelképesség és termékaffinitás elemzésére és előrejelzésére, amelyek pontos besorolása kérdéseket vethet fel. Ezek sok esetben statisztikai alapon működnek, de lehet mesterséges intelligencián alapuló részük is. Az adatvédelmi kötelezettségek szempontjából a GDPR technológiasemleges szabályozása miatt nincs jelentősége, hogy egy adott adatkezelési eszköz ezen határterületen belül minek minősül, az alapvető elvi feltételek minden adatkezelési eszközre azonosak, és az adatkezelés összes körülménye alapján szükséges azokra alkalmazni a megfelelő garanciákat.

A korábbiakban kifejtett témakörökben többször felmerült az anonimizálás jelentősége. E tekintetben jelenleg a gyakorlat még kialakulóban van. Az Európai Adatvédelmi Testület dolgozik az álnevesítéssel és az anonimizálással kapcsolatos iránymutatásokon. Az ezzel kapcsolatos elvárások a folyamatosan változó technikai környezettől is függenek, mivel bármely eszköz használata esetén az adatkezelés teljes időtartama alatt kell biztosítani a személyes adatok védelmét. Ezen környezet gyors változása a pontos követelmények meghatározását is nehézzé teszi.

3. KÉPEK FELDOLGOZÁSÁRA HASZNÁLT MI

A magyarországi bankokat ügyfélazonosítási kötelezettség terheli a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (a továbbiakban: **Pmt.**) és az auditált elektronikus hírközlő eszköz útján végzett elektronikus ügyfél-átvilágítás végrehajtásának szabályait a 29/2024. (VI. 24.) MNB rendelet[10] (a továbbiakban: **MNB rendelet**) tartalmazza. Fontos kiemelni az adatkezelési célok pontos megjelölését és elkülöníteni a jogszabályi kötelezettségen alapuló adatkezelést a hozzájáruláson, illetve jogos érdeken alapuló adatkezelésektől. Így például a Pmt.-ben meghatározott ügyfél átvilágítási és bejelentési kötelezettség teljesítése érdekében végzett adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, de ha az azonosítás során felvett adatokat az algoritmus fejlesztéséhez kívánnák felhasználni, ahhoz az érintett kifejezett hozzájárulásának beszerzése lenne szükséges. A jogi kötelezettség keretében vagy az érintett hozzájárulásával végzett adatkezelések egyoldalú kiterjesztése sok esetben sértheti a tisztességes és átlátható adatkezelés elvét[11], mivel ilyenkor az érintettnek nincs érdemi befolyása az alap adatkezelésre.

A magyarországi bankszektor szereplői egyre szélesebb körben alkalmazzák az MI komponenst tartalmazó eszközöket ügyfélazonosító rendszereikben. Az ilyen rendszerek alkalmazása során az ügyfelek azonosításához felhasználhatják az ügyfelek saját kameraképét, valamint ügyfelek okmányainak képét és azokról beolvasott információkat. A bankok használhatnak egy harmadik fél által kifejlesztett megoldást ezekre a feladatokra, de vannak nyilvánosan elérhető képi adatbázisok is, melyek segítségével kialakíthatják a saját

[10] 29/2024. (VI. 24.) MNB rendelet a Magyar Nemzeti Bank által felügyelt szolgáltatók által alkalmazott auditált elektronikus hírközlő eszköz és működtetésének, belső szabályozása minimumkövetelményeinek, auditálása módjának, valamint az ilyen eszköz útján végzett elektronikus ügyfél-átvilágítás végrehajtásának részletszabályairól

[11] Lásd az Európai Adatvédelmi Testület 28/2024. sz. véleménye a személyes adatoknak mesterségesintelligencia-modellekkel összefüggésben történő kezelésével kapcsolatos bizonyos adatvédelmi szempontokról, 92. bekezdés

megoldásukat. Az ilyen eszközök használatának azonban meg kell felelnie az MNB rendelet közvetett elektronikus ügyfél-átvilágításra vonatkozó szabályinak.

3.1. Bank 1

A Bank 1 az online számlanyitási folyamatában a nem valós idejű (közvetett elektronikus) azonosítási megoldást alkalmazza (ami az okmányon szereplő arckép és a folyamatban készített önarckép összehasonlítására épülő azonosítás útján történik). Ehhez a Bank 1 egy adatfeldolgozói minőségben közreműködő külső beszállító szolgáltatását veszi igénybe, aki a szolgáltatásához MI rendszert használ. A sikeres azonosítási folyamatot mind az adatfeldolgozónál, mind a Bank 1-nél emberi, manuális ellenőrzés követi. Ha sikertelen lett az azonosítás (küszöbérték alatti az egyezőségi arány, ideértve amikor az arckép nem érzékelhető emberi arcként), akkor az azonosítási folyamat ezzel az eredménnyel lezárul, következésképp az ügyfél ebben az esetben az online folyamatban nem tudja megnyitni a számlát. A számlanyitás lehetősége ebben az esetben is elérhető más csatornákon (például a bankfiókban személyesen vagy online videóhívás keretében nyújtott szolgáltatásként). Az őrzési idő az adatfeldolgozó eljárásában minden körülmények között 24 óra, ezt követően az adatfeldolgozó a használt adatokat véglegesen törli. 24 óra elteltével a Bank 1 a Pmt. szerinti adatokat az abban meghatározott jogszabályi kötelezettségének eleget téve kezeli tovább. Az adatfeldolgozó MI rendszere több komponensből áll, ezek vonatkozásában az adatfeldolgozó különböző megfelelőségi tanúsítványokkal rendelkezik.

3.2. Bank 2

Bank 2 alkalmaz saját MI komponenst használó ügyfélazonosítási rendszert, melyhez egy előre tanított nyílt forráskódú modell-t használ. A rendszer nem tárol személyes adatokat és külön adatbázist sem hozott létre a bank. A megoldás egy dedikált banki szerveren fut, a központi rendszer erre küldi a képeket, illetve a szelfivideót belső hálózaton, és szintén a belső hálózaton kapja vissza az azonosítás eredményét. A Bank 2 által használt megoldás kétkomponensű, egyrészt egy előtanított megoldást használ az arcképek ellenőrzésére és az ügyfelek okmányképével való összevetésére, valamint egy OCR rendszert a személyazonosító okmányok szövegének beolvasására. A megoldás alkalmas online személyazonosítás és szerződéskötésre, ezen kívül további nyilatkozatok aláírására. A rendszer automatikusan végzi az arcok összehasonlítását és élőségvizsgálat ellenőrzést (élő ember van-e a kamera előtt vagy egy felvétel vagy generált személy), de a végső ellenőrzés során manuális banki ügyintézői felülvizsgálat is történik.

3.3. Bank 3

Bank 3 esetében a közvetett elektronikus ügyfél átvilágítást végző rendszerbe került beépítésre egy MI modul, mely egy külső társaság által fejlesztett termékként került beszerzésre. A gépi látás modul az ügyfelek okmányain szereplő fényképek és a folyamatban általuk készített képmások összevetését végzik el, az ügyfél személyazonosságának megerősítése érdekében, illetve ellenőrzik, hogy az ügyfél az eszközt valós időben használja-e. A kimenet a rendszer által kerül felhasználásra: az érintett vagy tovább léphet az átvilágítási folyamatban, vagy más átvilágítási illetve ellenőrzési folyamatba kerül átirányításra. Az MI modul csak a képmásokat, illetve az azokból származtatott adatokat kezeli. Ezeket átmeneti tárban - „cache" - tárolja a személyazonosság megerősítéséig. Amennyiben a Bank 3 által alkalmazott közvetett ügyfélazonosítási rendszer nem tudja sikeresen azonosítani az ügyfelet eléggé magas biztossággal, akkor az ügyfél automatikusan manuális - közvetlen elektronikus ügyfél-átvilágítási - folyamatba kerül átirányításra, azaz ilyenkor mindig emberi felülvizsgálat történik.

4. SZÖVEGES FELDOLGOZÁS

A bankszektorban a mesterséges intelligenciát használó, szöveges feldolgozást végző eszközök jellemzően a virtuális asszisztensek, melyek különböző feladatokat láthatnak el. Az ilyen virtuális asszisztensek automatizálják azokat a feladatokat, amelyeket korábban emberi alkalmazottak végeztek, azaz ügyfelek, illetve potenciális ügyfelek általános jellegű, hitelezéssel kapcsolatos tájékoztatását, egyszerű kérdések megválaszolását és általános hitelkalkulációk készítését. Ezáltal gyorsítja és hatékonyabbá teszi a folyamatokat, mentesítve az emberi munkaerőt a rutinszerű feladatoktól. Az ilyen rendszerek jellegzetessége, hogy a felhasználóktól függ, hogy milyen adatokat adnak meg, így megadhatnak bármilyen személyes adatot, akár annak szükségessége nélkül is. Emiatt a virtuális asszisztenst alkalmazó bankoknak szükséges olyan eljárásrendet alkalmazni, mellyel a szükségtelen személyes adatokat kiszűri, a szükséges (így például az ügyfelek azonosításához használt) személyes adatokat pedig biztonságosan tárolja a célhoz kötöttség és adattakarékosság elveinek tiszteletben tartása mellett.

4.1. Bank 1

A Bank 1 ezen a téren részben egy telefonos ügyfélszolgálatba épített szolgáltatást, részben egy írásbeli chat szolgáltatást alkalmaz. Az előbbit az ügyfél élőszóban vezérli, előadja hívása tárgyát, majd ennek alapján a rendszer a megfelelő ügyintézőhöz kapcsolja. A chat szolgáltatásnál az ügyfél szabadszövegesen leírt problémájának téma szerinti besorolása alapján általános válasz érkezik az ügyfélhez.

A Bank 1 a telefonos ügyfélszolgálat esetében MI rendszert csak a természetes nyelvi feldolgozásra épülően használ. Használata az ügyfél számára opcionális, interakció hiányában a hívás átkerül nyomógombos rendszerbe. A Bank 1 e célra használt MI rendszere saját fejlesztésű, tanítását a Bank 1 felügyelt módon végzi és az a működése során nem tanul új képességeket. Az elkülönítve tárolt tanító adatbázis képzéséhez a Bank 1 hangfelvételeket gyűjtött az ügyfeleitől, ezeket manuálisan leiratozta, majd a leiratokat a személyes adatoktól megtisztította.

A chat szolgáltatáson belül a Bank 1 használ MI komponenst a témafelismerő funkció tekintetében. Ha kétszer elutasítja az ügyfél a saját maga által megadott problémaleírás alapján neki felajánlott témát, akkor egy manuális témaválasztó felületre kerül átirányításra. Ha a problémafelvetésére nincs témakiszolgálás, végső soron az ügyfél ügyintézőhöz irányítása is lehetséges. A Bank 1 e célra használt MI rendszere saját fejlesztésű, tanítását a Bank 1 felügyelt módon végzi és az a működése során nem tanul új képességeket. A tanításhoz a Bank 1 itt is elkülönített tanító adatbázist hozott létre. Ehhez felhasználta az ügyfelek szolgáltatáson belüli interakcióinak leiratát, azokból a személyes adatokat manuálisan eltávolította.

Mindkét szolgáltatás vonatkozásában felmerülhetnek olyan szolgáltatási elemek, amelyekben a Bank 1 csak akkor tud az ügyfélnek ezeken a csatornákon keresztül segíteni, ha az ügyfél azonosítja magát. Ez az azonosítási módszer szabályalapú protokollon keresztül valósul meg a szükséges esetekben, de a nyilatkozata szerint a Bank 1 az ügyfélazonosításhoz ezekben az esetekben nem használ MI komponenst.

4.2. Bank 2

A Bank 2-nél alkalmazott virtuális asszisztens alapvetően az általános tájékoztatást szolgálja a bank által kínált szolgáltatásokról, de speciálisabb feladatok elvégését is végezheti (így például hitelkalkulációt). A megoldás elsősorban automatizálja azokat a feladatokat, amelyeket korábban a bank alkalmazottjai végeztek, azaz ügyfelek, illetve potenciális ügyfelek általános jellegű, hitelezéssel kapcsolatos tájékoztatását, egyszerű kérdések megválaszolását és általános hitelkalkulációk készítését. A felhasználóknak a Felhasználási Feltételeket és az Adatkezelési Tájékoztatót el kell olvasniuk és fogadniuk ahhoz, hogy megkezdhessék a rendszer használatát. A rendszer mögött álló szoftvert azonban egy amerikai székhelyű harmadik fél szolgáltató biztosítja, a felhasználók által megadott üzenetek és Bank 2 publikusan elérhető dokumentumainak releváns részletei kerülnek továbbításra a harmadik fél modellje általi feldolgozására. A bank szervere közvetítőként kommunikál a harmadik fél szolgáltató szerverével, így a felhasználó ügyfél IP-címe vagy egyéb azonosítója a harmadik fél számára nem megismerhető, kizárólag a banki szerver IP címe látható. Mindezek mellett

azonban a felhasználó megadhat személyes adatot a lekérdezés szövegében, és ebben az esetben az továbbításra kerül a harmadik fél felé a kérdés feldolgozása céljából. Erre a működésre felhívják a felhasználók figyelmét az Adatkezelési Tájékoztatóban.

4.3. Bank 3

Bank 3 digitális asszisztense a mobilbank alkalmazás elválaszthatatlan része, és az ügyfelekkel folytatott digitális kommunikációra szolgál. Ez a szolgáltatás két eltérő módon működik, az első esetben kérés nélkül lép kapcsolatba a felhasználókkal, jellemzően push üzeneteket küld információkkal, a másik esetben pedig a felhasználók beszélgetést folytathatnak amikor kérdést tesznek fel. A virtuális asszisztens az esetek egy részében úgy válaszol, hogy az ügyfelet a használni kívánt mobilbanki funkcionalitáshoz irányítja, de ezek a funkciók az asszisztens közvetítése nélkül is elérhetőek, az csak odairányítja a megfelelő menüponthoz a felhasználót. Ha a megoldás nem tud válaszolni, akkor átirányítja az ügyfelet az emberi csatornához, például telefonos ügyintézőhöz. A megoldás nem vesz igénybe külső (harmadik félnél futó) komponenst, a bank belső rendszereit használja a szükséges adatok lekérdezéséhez. A megoldás egy MI nyelvi modellt használ az ügyfél természetes nyelven adott utasításainak értelmezésére (hang szöveggé átiratozó, amelyhez hasonlót a Hatóság is használ jelenleg[12]).

5. TANÍTÁSRA HASZNÁLT ADATOK

Az MI tanítása nem minden esetben igényli adott természetes személyhez köthető adatok használatát. Az adattakarékosság elvéből adódóan ahol lehetséges, ott főszabály szerint anonim adatokkal kell az MI modell tanítását elvégezni. Amennyiben más célból gyűjtött adatok felhasználása történik akár anonimizáció útján, az megfelelő jogalappal (vagy a GDPR 6. cikk (4) bekezdése szerinti feltételek igazolásával) és az érintettek tájékoztatásával valósulhat meg, mivel a személyes adatok anonimizációja is adatfeldolgozási művelet.

5.1. Bank 1

A Bank 1 az ügyfélazonosító MI rendszerének tanításához nem használta ügyfeleinek személyes adatait, a rendszert harmadik féltől már tanítva szerezte be.

[12] https://naih.hu/adatkezelesi-tajekoztatok
„Adatkezelési tájékoztató a Hatóságnak a személyes adatok védelmére és a közérdekű, illetve közérdekből nyilvános adatok megismerésére vonatkozó követelmények érvényesítésére irányuló közhatalmi eljárások lefolytatásával összefüggő adatkezeléseihez”, 6.3. pont

5.2. Bank 2

Bank 2 egy kiegészítő adatbázist hozott létre a bank által előállított, ellenőrzött és nyilvánosságra hozott dokumentumokból, és harmadik fél által biztosított MI megoldás ezen személyhez nem köthető információkat tároló adatbázisban keresi ki az asszisztensnek feltett kérdés megválaszolásához szükséges adatokat, és nem használ személyes adatokat a válaszok létrehozásához. A virtuális asszisztens egy harmadik fél megoldását használja és nem tanítja a modellt, csak a kiegészítő „tudástár" adatbázist fejleszti (például az általános szerződési feltételek, tájékoztatók tartalma stb.). A harmadik fél által biztosított modell nem rendelkezik hozzáféréssel a banki adatbázisokhoz, illetve a Bank 2 belső rendszereihez. A Bank 2 által fejlesztett adatkészlet úgy került létrehozásra, hogy lefedje a Bank 2 által kínált termékekhez kötődő leggyakoribb kérdéseket. A rendszer a kész válaszokból választja ki a releváns egész bekezdést vagy mondatot, melyekből kérdésre optimalizált válaszokat generál.

5.3. Bank 3

A Bank 3 esetében a szöveges MI modell tanításához használt új adatok anonimizált naplóbejegyzések elemzése során nyert tapasztalatokból, illetve a fejlesztőktől származnak. A tanítás során felhasznált adatok egyszerű magyar szavak, mondatok, amelyek nem tartalmaznak személyes adatot vagy banktitok körébe tartozó adatot. A címkézés kézzel történik több körben először az alkalmasságukat, majd a megfelelő csoportba (szándék) tartozásukat állapítjuk meg, ezután a mondatban található kiemelt jelentőségű entitásokat jelölik.

Bank 3 az általa használt gépi látás megoldás esetében nem biztosít hozzáférést az általa kezelt személyes adatokhoz a modell tanítása érdekében, a megoldást termékként szerezték be harmadik féltől.

6. SHADOW AI HASZNÁLAT

A „shadow AI" nyilvánvalóan adatbiztonsági kockázatot hordoz, mivel ilyen esetekben a szervezet nem bír kontrollal a saját IT infrastruktúráján futó ilyen természetű adatkezelésekről (például használ-e olyan MI rendszert a felhasználó, amely a működése során hozzáfér a belső hálózaton kezelt adatokhoz; használja-e a felhasználó a munkavégzését megkönnyítendő az MI rendszert; felhasználja-e a felhasználó az MI rendszerrel való interakciók, különösen a promptok[13] során a szervezet által kezelt személyes adatokat, stb.)

[13] A prompt egy bemeneti utasítás, kérdés vagy egyéb felhasználói interakció, amely alapján az MI választ vagy tartalmat állít elő.

6.1. Bank 1

A Bank 1 jelenlegi működési rendjében tiltott az olyan MI eszközök használata, amelyek nem a Bank 1 infrastruktúráján futnak. A korlátozást a gyakorlatban technikai tiltások biztosítják. A munkatársak csak azokat az eszközöket érik el, amelyek egységes bejelentkezési rendszerrel (SSO) és adatszeparációval védettek. Egyes MI rendszerek használata dedikált felhasználóknak engedélyezett. Ezek az MI rendszerek biztonsági beállítások és korlátozások mellett érhetőek el az arra jogosult felhasználók számára, akik felhasználói kézikönyvet is kaptak a belső szabályzatokkal egyező etikus használatról.

6.2. Bank 2

Bank 2 tiltja a szervezetén belüli „shadow AI" használatot és annak érdekében bank érvényt tudjon szerezni a tiltó rendelkezéseknek, tartalomszűrő szolgáltatás került bevezetésre, így a tiltott kategóriába eső oldalak felkeresésére nincs lehetőség.

6.3. Bank 3

Bank 3 is tiltja „shadow AI" használatot, de emellett a bank anyavállalata egyedi, globális szerződést kötött egy szolgáltatóval, amely által Bank 3 alkalmazottai használhatják a szolgáltató MI asszisztensét a használati adatok modell tanításához való felhasználásának kizárás mellett. Az egyes felhasználók tevékenységére vonatkozóan széleskörűen testre szabható szabályok és riasztásokat állíthatóak be, melyek erősítik a kontroll környezetet.

7. HITELKÉPESSÉG ÉS TERMÉKAFFINITÁS SZÁMÍTÁSA

A vizsgált bankok működésük során többfajta technikai megoldást is használnak. Ezek némelyike nem egyértelműen azonosítható be MI-ként. A döntéstámogató analitikus modellek készíthetnek több szempont alapján is ügyfélprofilt (így például hitelkockázat vagy csalásmegelőzési kockázatértékelés). Az ilyen eszközök által kiadott előrejelzés többféle termékkel vagy szolgáltatással függhet össze, így például hitel, befektetés vagy kártyaszolgáltatás. Tekintettel egyes megoldások nehéz elhatárolhatóságára, az ilyen eszközöket alkalmazóknak fokozott figyelmet kell fordítaniuk arra, hogy a döntéstámogató modellek milyen módon működnek. Az MI besoroláshoz segítséget nyújthat a fenti 1. pontban hivatkozott EB Iránymutatás. Adatvédelmi szempontból azonban a GDPR technológiasemlegessége miatt az adatkezeléshez felhasznált eszköz technikai besorolásától függetlenek az elvi adatvédelmi követelmények, amelyek eredményt írnak elő, nem eszközöket szabályoznak.

7.1. Bank 1

A Bank 1 sütikezelési tevékenysége körében, hozzájárulási jogalappal alkalmaz olyan célzó- és hirdetési sütiket, amelyek a honlap látogatójának az érdeklődésére szabott célzott marketinget tesznek lehetővé. A Bank 1 közlése alapján, a promóciókat gépi tanulás alapú modellek és/vagy szabályalapú modellek segítségével jelenítik meg. A honlap látogatójának hozzájárulása esetén, a Bank 1 a sütik alkalmazása során gyűjtött adatokat az ügyfélnek a Bank 1-nél rendelkezésre álló személyes adataival együttesen használhatja fel, ami egyedibb válaszadást tesz lehetővé.

Az értékesítést támogató tevékenységében a Bank 1 kalkulációkat végez, hogy az ügyfél számára megfelelő terméket ajánlhasson vagy épp azért, hogy felmérje az adott termék igénybevehető-e az adott ügyfél számára. A termékaffinitási score az adott ügyfélnek leginkább megfelelő termék ajánlását támogatja, a credit score az ügyfél hitelképességének bírálását segíti. A Bank 1 ilyen kalkulációkat korábban is végzett emberi erőforrás útján, de aktuálisan igénybe vesz hozzá MI rendszereket is.

A termékaffinitási score a banki termékek értékesítési valószínűségének értékét mutatja meg az adott ügyfél vonatkozásában. Az MI rendszer banki termékenként pontozza, hogy mennyire venné igénybe az ügyfél adott hónapban az adott terméket. Az MI rendszer különböző adatcsoportoknak az összerendelési variációiból képzi ezt a változót. Az így képzett értékekhez csak az ügyintéző fér hozzá, további adatok nem keletkeznek. A pontszám az ügyintéző munkáját segíti, azonban az sem az ügyintézőt, sem az érintettet nem kötelezi semmire. A generált pontszám adatot a Bank 1 egyéb célból nem használja, az ügyfeleket ennek alapján nem osztályozza. Az MI rendszer teljes egészében belső fejlesztésű (a fejlesztés, üzemeltetés, tanítás a Bank 1-en belül történik).

A credit score a hitelbírálati folyamat egyik elemeként, statisztikai alapon előállított érték. Előállításának célja az ügyfél hitelképességének mérése. Az ennek alapján történő besorolás, annak valószínűségi szintjét jelzi, hogy mekkora eséllyel válik fizetésképtelenné a hitelt kérelmező ügyfél 1 éven belül. Az így képzett minősítési érték a bírálati rendszer egyik eleme, de nem a döntési pont. A Bank 1 e célra saját fejlesztésű modellt alkalmaz. Mind a fejlesztést, mind az üzemeltetést önállóan végzi. A modell nem öntanuló, havi rendszerességű monitoring mellett emberi felügyelettel tanul. A tanító adatbázisból a Bank 1 a személyes adatokat eltávolította és egy speciális azonosítón keresztül kötötte össze az összetartozó adatelemeket. A modell tesztelése előbb az így képzett tesztadatokkal történt, majd valós adatokkal, de még (az éles rendszer helyett) egy integrált tesztkörnyezetben. A tesztelés kapcsán nem történik olyan jogosultság-kiosztás, ami azzal az eredménnyel járhatna, hogy a munkatárs olyan

adathoz is hozzáférhet, amihez egyébként nincs hozzáférése. Az adat éles rendszerben eltárolt formáját érintő módosítás vagy törlés nem történhet.

A Bank 1 tevékenységében a csalások szűrése, az erős adatbiztonsági szint, az ügyfél azonosíthatósága és a szélesebb értelemben vett hitelesség kérdése központi kérdés. E tekintetben számos jogforrási előírásnak is meg kell felelni. Az e körben alkalmazott MI rendszer alkalmazásának célja a bankkártyákkal, bankszámlákkal és elektronikus azonosító adatok jogtalan felhasználásával elkövetett csalások megelőzése, felderítése, vizsgálata, olyan események monitorozása, amelyek visszaélésre utalhatnak.

7.2. Bank 2

Bank 2 a vizsgált időben nem alkalmaz termékek értékesítéséhez kapcsolódó profilalkotás vagy marketing és kereskedelmi tevékenységhez kapcsolódó profilalkotás tekintetében MI eszközöket.

7.3. Bank 3

Bank 3 használ modelleket marketing célból, melyek funkciója, hogy a marketing szakértőknek információt nyújtson, mely termékek, csatornák, kommunikációk lehetnek relevánsak az ügyfelek részére.

A Bank 3 használt hitelkockázati modellek célja a felelős, jogszabályok által elvárt hitelezési gyakorlat támogatása. Ezen modellek kimenete egy szám, amely a hitelezési kockázatot jelöli, és amely – a marketing modellekhez hasonlóan - szakértői döntés támogatására szolgál. A hitelkockázati modellek célja a felelős, jogszabályok által elvárt hitelezési gyakorlat támogatása.

8. AZ ANONIMIZÁLÁS FOGALMA ÉS JELENTŐSÉGE AZ MI-VEL KAPCSOLATOS ADATKEZELÉSEKNÉL

Több vizsgált banknál is felmerült a személyi asszisztenssel folytatott chatbeszélgetések közben megadott személyes adatok kezelése, illetve a beszélgetések naplózása előtt a személyes adatok eltávolításának kérdése. A technikai leírásokban van ahol szerepel ebben a körben a deperszonalizáció kifejezése, az anonimizációval együtt. Ebben a körben szükséges tisztázni, hogy adatvédelmi szempontból anonimizáció[14] és álnevesítés[15] létezik, a deperszonalizáció jogilag nem definiált fogalom.

---

[14] GDPR (26) preambulumbekezdés szerint az anonimizált adatok olyan információk „*amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint (…) amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható*”

[15] GDPR 4. cikk 5. pont szerint az álnevesítés fogalma „*a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes*

8.1. Bank 1

A Bank 1 a témakör felismerő modulhoz a tanítási adatokat az ügyfelek szolgáltatáson belüli interakcióinak leiratából állította elő, azok manuális anonimizálása mellett. A hitelbírálati modul modell nem öntanuló, havi rendszerességgel, emberi felügyelettel tanul. A tanító adatbázisból a Bank1 a személyes adatokat eltávolította, a modell tanításához nem használ személyes adatokat. A tesztelés kapcsán nem történik olyan jogosultság kiosztás, ami azzal az eredménnyel járhatna, hogy a banki munkatárs olyan adathoz is hozzáférhetne, amelyhez egyébként ne lenne hozzáférése a mindennapi munkája során.

8.2. Bank 2

A Bank 2 által alkalmazott virtuális asszisztenssel folytatott beszélgetések a felhasználó általi lezárásig, de legfeljebb a felhasználói inaktivitástól számított 30 percig tárolódnak. Ezt követően anonimizálásra kerülnek, és az anonimizált szöveg a bank saját szerverein kerül tárolásra a rendszer fejlesztéséhez szükséges ideig. Az anonimizálást egy NLP[16] alapú algoritmus végzi, amely előre meghatározott paraméterek alapján keres személyes adatokat a beszélgetésben, majd törli őket a tárolás előtt.

8.3. Bank 3

Bank 3 felhasználja a felhasználóknak a digitális asszisztenssel folytatott beszélgetéseit annak fejlesztésére, de azok anonimizálására kerül sor az ilyen célú felhasználás előtt. Először előállítanak egy chat naplót, mely az ügyféllel folytatott beszélgetés első szabad szöveges mondatát tartalmazza, továbbá annak értékelését, hogy a passzív digitális csatorna a megfelelő választ adta-e, illetve ha nem, melyik választ kellett volna meghívnia a mondatnak. Itt még szerepel egy „chat ID” hozzárendelve a beszélgetéshez (álnevesített adatkezelés), de ezt követően kiválogatásra kerülnek a tanításra felhasználandó magyar mondatok, minden más adat törlése mellett. Az így megmaradt napló újabb ellenőrzése előzi meg a tanításra való felhasználást.

---

adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni”

[16] NLP: A „Natural Language Processing” algoritmus a mesterséges intelligenciát használó algoritmusok egy fajtája, amely a természetes nyelvek, például a magyar nyelv feldolgozásával és elemzésével foglalkozik.