

Dr. Zámbó Gyula*:

Automatizált ügyfélbefogadással és monitoringgal harcolnak a pénzmosók ellen

A mesterséges intelligencia tért hódít a pénzmosás megelőzését célzó küzdelemben is. A pénzügyi intézmények immár szerződéskötés előtt ügyfélprofil felállításával szűrhetik ki a gyanúsnak minősülő cégeket. A szokatlan tranzakciós mintázatokra vagy éppen az eladdig „alvónak” látszó cégek hirtelen aktivizálódására pedig az automatizált monitoring eszközével (is) felfigyelhetnek ezentúl a bankok vagy a befektetési vállalkozások. Bár mindez adatvédelmi vagy felelősségi kérdéseket is felvet, a cél egyértelmű: a tisztességes ügyfelek és az egész piac biztonsága.

Az elmúlt évek technológia fejlődését az egyre jobban terjedő digitalizáció határozta meg. Az okostelefonok megjelenését követően hétköznapi használati tárgyaink sokasága és számos szolgáltatás is a virtuális világ részévé vált. Nincs ez másképp a pénzügyi szolgáltatásokkal sem. A „régi világ” sorban állását felváltották a pár kattintással megnyitható bankszámlák, a tranzakciók sorát pillanatok alatt lebonyolító alkalmazások.

Mindez egyrésztől nagyban megkönnyítette és felgyorsította a legkülönbözőbb ügyek intézését, másrésztől azonban a visszaéléseknek is új lehetőségeket teremtett. Ez komoly kihívás elé állította a pénzügyi intézményeket és a bűnüldöző hatóságokat. Ma már percek alatt, országhatárokon fittyet hányva mozgatható például az elsikkasztott pénz, vagy éppen a kábítószer-, ember-, vagy illegális fegyverkereskedelemből származó vagyon. A több millió ügyfél napi több tízmillió tranzakciója közül pedig szinte lehetetlen (nem mellel rendkívül költséges) feladat kiszűrni ezeket. Eközben viszont egyre erősebb mind a felügyeleti, mind az általános társadalmi elvárás, hogy a pénzügyi rendszer szereplői hatékonyan lépjenek fel a visszaélésekkel szemben. Ebben segíthet az új technológiák - a nagy mennyiségű adat feldolgozására képes „big data”, a gépi tanulás vagy a mesterséges intelligencia (MI) - hadrendbe állítása.

Mint az élet szinte minden területére, úgy a pénzmosásra is igaz, hogy ha már megtörtént a baj, azt sokkal nehezebb orvosolni, mint ha megelőztük volna. Ennek megfelelően a cél az, hogy a bűnözők eleve ne is férhessenek hozzá a pénzügyi szolgáltatásokhoz, vagy ha mégis, sikerüljön megakadályozni a piszkos pénzek elrejtését. Ez ki is jelöli a pénzmosás-megelőzés legkritikusabb pontjait: az ügyfélbefogadást (onboarding), és az ügyfél, valamint a tranzakciók folyamatos figyelemmel kísérését (monitoring).

Elutasítani a gyanús ügyfelet

Ma már természetes, hogy online nyithatunk bankszámlát, de személyes megjelenés hiányában sokszor az ügyfél személyazonosságának megállapítása is nehézségekbe ütközhet. Minimális számítástechnikai képzettséggel szerkeszthetünk új fényképet egy szkennelt igazolványra, emellett az internetes feketepiacon (dark web) fillérekért vásárolható lopott „személyiség”. A bűnözőknek tehát egyre kifinomultabb és egyre könnyebben hozzáférhető eszközök állnak rendelkezésükre hamis ügyfélprofil létrehozására. Az arcfelismerő és összehasonlító szoftverek, a bemutatott személyazonosító igazolványok valóságát ellenőrző eszközök éjjel-nappal egyformán nagy hatékonysággal képesek leleplezni az ilyen próbálkozásokat.

Aki már nyitott bankszámlát, az megtapasztalhatta, hogy esetenként számos, látszólag a bankra nem tartozó információt is meg kell osztania a hitelintézetével. Az ügyfél-azonosítási (know your customer, KYC) eljárás azonban nem öncélú adatgyűjtés, és nem is csak a személyre szabott szolgáltatás érdekében történik. A pénzügyi intézmény az így nyert adatok birtokában képes csak felmérni az ügyfelében rejlő kockázatot, azaz például azt, hogy mennyire számíthat gyanús ügyletekre az újonnan nyitott bankszámlán.

A hagyományos KYC-eljárások azonban önbevallásos elven működtek. Nem nehéz belátni, hogy egy bűnözőtől kevésbé várható olyan információk megadása, melyek segítenék saját leleplezését. Az új technológiák ezen a téren is nagy segítséget jelenthetnek. A közösségi média felületek, online sajtóhírek és egyéb nyilvános adatbázisok automatikus átvizsgálásával ugyanis sokkal pontosabb és valósabb ügyfélprofil állítható fel, s így pontosabb lehet a jogszabályok által is előírt kockázatbesorolás, ami a továbbiakban az ügyfélátvilágítás mélységét is meghatározza.

Felébredő „alvó cégek”, szokatlan tranzakciós minták

A pénzügyi szolgáltató azonban még a legalaposabb előzetes kockázatértékelés ellenére sem dőlhet egyszerűen hátra. Még a legfejlettebb rendszerek is kijátszhatók, illetve utóbb is kockázatosá válhat egy addig megbízható ügyfél. Jellemző például, hogy úgynevezett „alvó cégek” számláit használják fel pénzmosásra. Az ilyen esetek feltárását szolgálja egyfelől az ügyfél körülményeinek, másfelől az általa kezdeményezett ügyleteknek a folyamatos nyomon követése.

Az ügyfél jellemző adatainak naprakészen tartása az onboarding kapcsán már említett ügyfélprofil rendszeres karbantartásával biztosítható. Erős jelzés lehet a pénzügyi szolgáltatónak, ha gyakran változik egy cég tulajdonosi köre, székhelye, vagy éppen papír-írószer kereskedelemről hirtelen fegyverkereskedésre tér át.

A monitoring másik kiemelt területe a kezdeményezett ügyletek vizsgálata. Bármennyire is egyedi minden ügyfél, az általános üzletvitel, illetve egy átlagos ember élete jól körülhatárolható mintázatba rendezi tranzakcióit. Áruklódó például, hogy ha egy cég számláján sosincs bér- vagy adófizetés, vagy ha a szokásos összegű rezsiszámlák befizetése mellett egyszer csak milliárdos átutalások jelennek meg, mondjuk a Karib-tenger térségébe. A naponta több millió ügylet közül az ilyen szokatlan jelenségek kiszűrésére eddig is léteztek szoftverek, azonban ezek jellemzően csak általános, előre beállított tényezők (pl. utalás összege, célországa) vizsgálatára voltak képesek.

A mesterséges intelligencia ezzel szemben sokkal hatékonyabb, képes az ügyfél korábbi ügyleteinek és ügyfélprofiljának együttes elemzése alapján egyedi mintázatok felállítására, s ehhez viszonyítottn vizsgálni a lehetséges szokatlan jellemzőket. Nem elég azonban a gyanús tranzakciók felfedezése, lehetőség szerint annak teljesítését is meg kell akadályozni (különösen a bankszámlacsatlások esetében), így kiemelt jelentőségű a kiszűrt ügyletek mielőbbi vizsgálata. A nagy mennyiségű adat valós idejű feldolgozása tehát kulcsfontosságú. Ebben is nagy előrelépést jelentenek az új technológiák.

Az új technológiák határai

Az előbbiekben bemutatott néhány kézenfekvő példa is jól bemutatja, milyen nagy jelentőségű változást hoznak az új technológiák a pénzügyi rendszer biztonságosabb, a visszaélésekkel szemben ellenállóbb működésében. Érdemes azonban pár szóban ennek korlátait, veszélyeit is bemutatni.

Mind a pénzügyi intézményeket, mind a jogalkotókat komoly dilemma elé állítják az adatvédelmi kérdések, ismerve a személyes adatok védelmének fontosságát. Naponta tapasztalhatjuk, hogy egy internetes keresésünket, hogyan követik a közösségi médiafelület által számunkra feldobott posztok, kéretlen reklámajánlatok. A mesterséges intelligencia által létrehozható szélesspektrumú ügyfélprofilok adatvédelmi szabályozása sem maradhat el.

Az új technológiák révén bővülő automatizmus (például egy átutalási megbízás visszautasítása) emellett a mesterséges intelligencia felelősségének kérdését feszegeti, ahogy az mondjuk a közlekedés világában már az önvezető autók által okozott balesetek kapcsán többször is felmerült.

Látjuk és tapasztaljuk tehát a mindennapjainkban, hogy a digitalizáció térnyerése alapjaiban változtatja meg életünk majd' minden területét. Közös érdekünk, hogy ez a fejlődés a pénzügyi rendszerben is – a pénzmosás- és terrorizmusfinanszírozási gyanús ügyletek automatizált kiszűrésével, kezelésével – mindnyájunk javát szolgálja és kialakítsuk az ennek legmegfelelőbb kereteket.

** A szerző a Magyar Nemzeti Bank Pénzmosás vizsgálati főosztályának munkatársa*

„Szerkesztett formában megjelent Infostart.hu portálon 2022. november 15-én.”