VISTA BANK

Deschiderea contului bancar prin mijloace de identificare video

Ciprian Chiorean – Director Coordonator VISTA BANK, Vicepresedinte ACJSFB
Timisoara, 31 martie 2023

DISPOZITII LEGALE INCIDENTE

- Directiva UE 2015/849 privind prevenirea utilizarii sistemului financiar in scopul spalarii banilor sau finantarii terorismului, modificata prin Directiva UE 2018/843;
- EBA GL 2022/15 privind aplicabilitatea art. 13(1) din Directiva UE 2015/849 publicat la 22.11.2022
- Regulamentul European 910/2014 (eIDAS) privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna
- Norma ADR din 24.11.2021 privind reglementarea, recunoasterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanta utilizand mijloace video

DIRECTIVA UE 2015/849 PRIVIND PREVENIREA UTILIZARII SISTEMULUI FINANCIAR IN SCOPUL SPALARII BANILOR SAU FINANTARII TERORISMULUI

- Art. 13 alin. (1) din Directiva UE 2015/849 privind prevenirea utilizarii sistemului financiar in scopul spalarii banilor sau finantarii terorismului:

(1) Măsurile de precauție privind clientela cuprind:

(a) identificarea clientului și verificarea identității clientului pe baza documentelor, a datelor sau a informațiilor obținute dintr-o sursă sigură și independentă, inclusiv, dacă sunt disponibile, **a mijloacelor de identificare electronică, a serviciilor de încredere relevante prevăzute în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului sau a oricărui alt proces de identificare sigur, la distanță sau electronic, reglementat, recunoscut, aprobat sau acceptat de autoritățile naționale relevante**;

(b) identificarea beneficiarului real și adoptarea unor măsuri rezonabile pentru a verifica identitatea acestuia, astfel încât entitatea obligată să aibă certitudinea că știe cine este beneficiarul real, inclusiv, în ceea ce privește persoanele juridice, fiduciile, societățile, fundațiile și construcțiile juridice similare, adoptarea unor măsuri rezonabile pentru a înțelege structura de proprietate și de control a clientului. În cazul în care beneficiarul real identificat ocupă o funcție de conducere de rang superior, astfel cum se menționează la articolul 3 alineatul (6) litera (a) punctul (ii), entitățile obligate iau toate măsurile rezonabile necesare pentru a verifica identitatea persoanei fizice care ocupă funcția de conducere de rang superior și țin evidența măsurilor luate și a eventualelor dificultăți întâmpinate în timpul procesului de verificare;

(c) evaluarea și, după caz, obținerea de informații privind scopul și natura dorită a relației de afaceri;

(d) realizarea unei monitorizări continue a relației de afaceri, inclusiv examinarea tranzacțiilor încheiate pe toată durata relației respective, pentru a asigura că tranzacțiile realizate sunt conforme cu informațiile entității obligate referitoare la client, la profilul activității și la profilul riscului, inclusiv, după caz, la sursa fondurilor, precum și că documentele, datele sau informațiile deținute sunt actualizate.

La aplicarea măsurilor menționate la literele (a) și (b) din primul paragraf, entitățile obligate verifică, de asemenea, dacă o persoană care pretinde că acționează în numele clientului este autorizată în acest sens și identifică și verifică identitatea persoanei respective.

EBA GL 2022/15 PRIVIND APLICABILITATEA ART. 13(1) DIN DIRECTIVA UE 2015/849

- EBA a publicat o versiune finala a Ghidului la 22 noiembrie 2022, dupa consultarea publica incheiata in martie 2022, cu intrare in vigoare la 6 luni de la publicarea in toate limbile oficiale ale UE
- EBA isi propune sa stabileasca pasii pe care trebuie sa ii adopte institutiile financiare pentru siguranta si eficienta inrolarii clientilor la distanta in conformitate cu legislatia privind combaterea spalarii banilor si a finantarii terorismului si cea privind protectia datelor.
- Liveness detection – de fiecare data cand sunt folosite solutii de inrolare de la distanta care nu presupun interactinea cu un angajat pentru efectuarea procesului de verificare, liveness detection va fi obligatorie.
- Controale suplimentare - indiferent de metoda de verificare aleasa, EBA stabileste ca acolo unde este identificat risc de spalare de bani sau finantare terorism asociat relatiei de afaceri, institutiile trebuie sa utilizeze controale suplimentare in vederea cresterii fiabilitatii procesului de verificare. Ghidul ofera o lista neexhaustiva de posibile controale, cum ar fi trimiterea unui cod de acces generat aleatoriu catre client pentru a confirma prezenta in timpul procesului de verificare la distanta.
- Externalizare – pe langa cerintele de guvernanta stabilite in Ghid (cum ar adoptarea de politici de risc, evaluarea si monitorizarea inainte de implementare a solutiei de inrolare la distanta) institutiile vor trebui sa isi adapteze procedurile de externalizare la cerintele stabilite in Ghid si sa le aplice colaboratorilor.
- Ghidul doreste sa ofere beneficii semnificative institutiilor prin crearea unui standard comunde urmat si minimizarea riscului AML prin urmarea pasilor recomandati

NORMA ADR DIN 24.11.2021 PRIVIND REGLEMENTAREA, RECUNOASTEREA, APROBAREA SAU ACCEPTAREA PROCEDURII DE IDENTIFICARE A PERSOANEI LA DISTANTA UTILIZAND MIJLOACE VIDEO

- Elementul principal al procesului de identificare video este reprezentat de procesul de verificare a identitatii. Fluxul de identificare presupune urmatorii pasi: initierea procesului, colectarea atributelor, datelor si dovezilor, legarea si verificarea acestora, validarea dovezilor/probelor.
- Mod de implementare automata sau cu operator uman
- Amenintari in cadrul utilizarii **solutiei automate**:
  - Photo attack
  - Video reply attack
  - 3D mask
  - Deepfake attack
- Mecanisme de contracarare:
  - Asigurarea ca fotografia si elementele inscrise pe documentul de identitate corespund persoanei care parcurge procedura de identificare;
  - Asigurarea ca informatiile continute in documentul de identificare sunt corecte si valabile, in raport cu persoana care parcurge procedura de identificare;
  - Validarea biometrica si corelarea cu autenticitatea documentelor;
  - Analizarea validitatii documentului de identitate;
  - Analizarea existentei elementelor de securitate optica/vizuala la nivelul documentelor de identitate

- **Solutia video cu operator uman** presupune inregistrarea intr-o sesiune unica a procesului de identificare a persoanei la distanta, in prezenta unui operator uman (agent de incredere)
- Persoana care urmeaza sa fie identificata trebuie sa isi dea consimtamantul explicit asupra inregistrarii video a intregului proces de identificare, a fotografiilor si a capturilor de ecran ale acestora si ale documentului de identitate.
- Consimtamant expres pentru parcurgerea procesului de identificare si pentru scopul identificarii.
- Persoana este informata cu privire la clauzele si conditiile privind utilizarea serviciului pentru care se realizeaza identificarea, inclusiv orice restrictie privind utilizarea acestuia.

CONDITII DE FORMA A CONTRACTULUI DE CONT BANCAR

- **Art. 1178 si art. 1179 alin. (2) Cod civil**
- **Art. 1240 si art. 1245 Cod civil**
- Contractul se incheie prin simplul acord de vointa al partilor, daca legea nu impune o anumita formalitate
- Consimtamantul (vointa de a contracta) poate fi exprimat:
  - Verbal
  - In scris
  - Printr-un anumit tip de comportament care, potrivit legii, conventiei partilor, practicilor statornicite intre acestea sau uzantelor nu lasa nicio indoiala asupra intentiei de a produce efectele juridice corespunzatoare
- Daca legea prevede o anumita forma a contractului, aceasta trebuie respectata sub sanctiunea prevazuta de dispozitiile legale aplicabile
- Contractele incheiate prin mijloace electronice sunt supuse conditiilor de forma prevazute de legea speciala
- In Codul civil nu exista o definitie a contractului de cont bancar curent si de asemenea nu sunt mentionate cerinte special de forma pentru validitatea sa
- Contractul de cont bancar curent = depozit remunerat ⟹ art. 2104 Cod civil forma scrisa (cerinta de proba)

INCHEIEREA CONTRACTULUI DE CONT BANCAR LA DISTANTA

- Oferta acceptata de destinatar ⟶ contract intre ofertant si destinatarul ofertei (art. 1182 alin. 1 Cod civil)
- Consimtamant valabil exprimat in cazul ofertei de a contracta adresata unor destinatari nedeterminati (art. 1189 alin. 2 Cod civil)
- Contract incheiat prin mijloace electronice (art. 7 din Legea nr. 365/2002)
- Proba contractelor incheiate prin mijloace electronice
- Daca partile nu au convenit altfel, contractul incheiat prin mijloace electronice se considera incheiat in momentul in care acceptarea ofertei de a contracta a ajuns la cunostinta ofertantului (art. 9 din Legea nr. 365/2002)

PROBA CONTRACTULUI DE CONT BANCAR INCHEIAT ELECTRONIC

- Art. 267 Cod procedura civila – inscrisuri in forma electronica
- Art. 282-284 Cod procedura civila - inscrisuri pe suport informatics
- Conditii de admisibilitate:
  - documentul sa fie inteligibil
  - documentul sa prezinte garantii suficient de serioase pentru a face deplina credinta in privinta continutului acestuia si a identitatii persoanei de la care acesta emana. Conform art. 283 Cod procedura civila, inscrierea datelor unui act juridic pe suport informatic este prezumată a prezenta garanții suficient de serioase pentru a face deplină credință în cazul în care ea este **făcută în mod sistematic şi fără lacune şi când datele înscrise sunt protejate contra alterărilor şi contrafacerilor astfel încât integritatea documentului este deplin asigurată**. O astfel de prezumție există şi în favoarea terților din simplul fapt că înscrierea este efectuată de către un profesionist.

MOD DE FUNCTIONARE

- Identificarea persoanei la distantă prin mijloace video reprezintă procesul de identificare şi verificare a identității în baza documentelor prezentate, a imaginilor capturate şi/sau a informațiilor comunicate de persoana fizică, utilizând mijloace video
- Tehnologiile de „recunoaștere a fetei" (sau „FRT") sunt un tip specific de tehnologii biometrice care se referă la o multitudine de tehnologii utilizate în scopuri diferite, de la simpla detectare a prezentei unei fete într-o imagine, până la cele mai complexe verificări, identificări și categorisiri sau clasificării persoanelor
- Verificarea (comparațte unu-la-unu) permite compararea a două sabloane biometrice, de obicei se presupune că apartin aceluiași individ. Identificarea (comparație unu-la- mai mulți) înseamnă că sablonul imaginii faciale a unei persoane este comparat cu alte sabloane stocate într-o bază de date pentru a descoperi dacă imaginea acesteia este stocată acolo. FRT-urile sunt, de asemenea, folosite pentru a efectua o clasificare a indivizilor, pe baza caracteristicilor lor personale. În acest sens, a fost dezvoltată o gamă largă de programe pentru a evalua atributele unei persoane din chipul său, în scopul „clasificării atributelor fetei" (de exemplu, gen, rasă sau etnie) sau pentru „estimarea atributelor fetei" (de exemplu, vârsta)

- Identificarea prin recunoastere facială cu mijloace electronice presupune ca persoana fizică să folosească un dispozitiv electronic cu care să captureze imagini ale fetei si imagini ale cărtii de identitate sau pasaport. Este necesară fotografierea față-verso a cărtii de identitate. Software-ul va scana documentul, va extrage datele, va face o verificare rapidă și va valida documentul.
- Pe parcursul procedurii de video-identificare, persoanei i se pot adresa diverse întrebări pentru a se asigura că în fața laptopului sau a telefonului nu este o altă persoană decât cea din documente, prin tehnologii noi, pentru a detecta dacă în respectivul selfie este o persoană sau o imagine falsă, videoclip sau obiect inanimat.
- Se utilizează tehnologie de inteligentă artificială pentru a verifica identitatea persoanei. Un algoritm complex compară fotografia din cartea de identitate cu cea din selfie pentru a se asigura că este vorba despre aceeasi persoană.
- După ce acesti pasi au fost parcursi cu succes, ultimul pas este confirmarea cu un factor de autentificare suplimentar, prin transmiterea către persoana fizică care parcurge procedura de identificare la distanță a unui cod de unică folosință („One Time Password" – OTP), sau prin transmiterea unui link cu o durată limitată, special creat în acest scop, generat în mod individual (prin e-mail sau SMS).
- Identificarea prin mijloace video presupune prelucrarea de date biometrice prin captarea imaginii faciale, a datelor din actul de identitate, a mediului ambient pentru imaginea capturată pentru selfie, vocea.

CHAT GPT SI IA IN BANCI

Automatizarea proceselor prin utilizarea inteligenței artificiale în sistemul bancar poate aduce o serie de beneficii semnificative.

- Unul dintre cele mai importante beneficii este **reducerea timpului** necesar pentru a finaliza sarcinile bancare, cum ar fi procesarea tranzacțiilor sau verificarea documentelor și a identității clienților. Aceasta poate **îmbunătăți eficiența** și poate **reduce costurile**, permițând băncilor să ofere **servicii mai rapide și mai accesibile** clienților lor.
- De asemenea, utilizarea inteligenței artificiale în procesele bancare poate **îmbunătăți calitatea serviciilor bancare prin reducerea erorilor și a fraudelor**. Sistemele IA pot identifica modele și anomalii în tranzacții și în alte date, ajutând la prevenirea fraudei și la protejarea datelor și a banilor clienților.
- În plus, utilizarea IA în sistemul bancar poate **îmbunătăți experiența clienților** prin oferirea de servicii personalizate și adaptate nevoilor și preferințelor acestora. De exemplu, băncile pot utiliza algoritmi de învățare automată pentru a oferi recomandări personalizate pentru investiții sau pentru a personaliza ofertele de credite pentru clienți.
- Un alt beneficiu al utilizării inteligenței artificiale în sistemul bancar este **îmbunătățirea conformității cu reglementările**. Sistemele IA pot ajuta la monitorizarea și raportarea datelor în conformitate cu reglementările locale și internaționale, precum și la respectarea standardelor de securitate a datelor.

În concluzie, utilizarea inteligenței artificiale pentru automatizarea proceselor în sistemul bancar poate aduce o serie de beneficii semnificative, cum ar fi îmbunătățirea eficienței, calității serviciilor bancare, conformității cu reglementările și experiența clienților.

CHAT GPT SI IA IN BANCI

În ciuda beneficiilor semnificative pe care le poate aduce automatizarea proceselor prin utilizarea inteligenței artificiale în sistemul bancar, există și **riscuri asociate cu această tehnologie**.
Iată câteva dintre aceste riscuri:

- **Securitatea datelor**: Utilizarea inteligenței artificiale în procesele bancare poate implica manipularea și stocarea unor cantități mari de date sensibile ale clienților. Astfel, este necesară o securitate sporită a acestor date pentru a preveni accesul neautorizat sau furtul de date.
- **Decizii incorecte sau nedrepte**: Algoritmii de inteligență artificială sunt programați pentru a lua decizii în funcție de datele și instrucțiunile pe care le primesc. Cu toate acestea, algoritmii pot fi influențați de bias-ul uman și pot produce decizii incorecte sau nedrepte. De exemplu, un algoritm de creditare automată poate discrimina femeile sau minoritățile etnice din cauza unor modele incorecte de date.
- **Lipsa de transparență**: Uneori, algoritmii de inteligență artificială sunt atat de complecsi încât nu este clar cum au luat o anumită decizie. Acest lucru poate duce la o lipsă de transparență și poate fi dificil pentru bănci să explice clienților cum anumite decizii au fost luate, ceea ce poate afecta încrederea și satisfacția clienților.
- **Erori de programare**: Programele de inteligență artificială sunt concepute pentru a procesa date și a lua decizii în funcție de acestea. Cu toate acestea, erorile de programare pot duce la luarea deciziilor greșite sau la erori în procesarea datelor, ceea ce poate avea consecințe grave.
- **Dependența excesivă de tehnologie:** In sistemul bancar poate duce la o dependență excesivă de tehnologie, ceea ce poate crea vulnerabilități în ceea ce privește capacitatea băncilor de a gestiona situații de criză. În cazul unui atac cibernetic sau a unui sistem care se defectează, băncile pot fi incapabile să își desfășoare activitățile în mod normal, ceea ce poate duce la pierderi financiare și reputaționale
- **Costuri ridicate**: Implementarea tehnologiilor de inteligență artificială poate fi costisitoare și poate necesita resurse semnificative în ceea ce privește pregătirea datelor, programarea algoritmilor și dezvoltarea infrastructurii necesare. Aceste costuri pot fi prohibitiv de mari pentru unele bănci mai mici sau pentru instituțiile financiare din țări mai puțin dezvoltate.
- **Reglementări și conformitate**: Utilizarea inteligenței artificiale în procesele bancare poate fi reglementată de diverse legi și reglementări, iar băncile trebuie să fie conforme cu acestea pentru a evita sancțiunile și amenzile. În plus, băncile trebuie să se asigure că algoritmii lor respectă normele etice și morale și că deciziile luate sunt în conformitate cu valorile lor.

În general, utilizarea inteligenței artificiale în sistemul bancar poate aduce beneficii semnificative, dar este important ca băncile să fie conștiente de riscurile asociate cu această tehnologie și să ia măsuri pentru a le gestiona și minimiza impactul lor.