Între siguranța cibernetică și nesiguranța juristului

Lucian Bondoc, Managing Partner,
Bondoc & Asociații

Colocviile juridice ale BNR - Ediția a XXX-a

28 martie 2025, Facultatea de Drept din cadrul Universității de Vest din Timișoara

Agenda

1. **Problema corelării dreptului cu revoluțiile industriale. Punctul actual**
2. **Cadrul juridic principal și unele aspecte terminologice**
   (a) **Un cadru european în dezvoltare accelerată**
   (b) **Definiția AI conform AI Act. Ce este AI? Diferența între AI și softul tradițional**
3. **Unele aspecte de context**
   1. **Evoluția AI în sectorul financiar**
   2. **Unele limitări impuse de Convenția Cadru a Consiliului Europei privind AI**
   3. **AI Act**
   4. **DORA (și NIS2, CRA)**
4. **Ce înseamnă cele de mai sus pentru siguranța cibernetică și juriști în context IA**
5. **Unele concluzii**

Problema corelării dreptului cu revoluțiile industriale – Punctul actual

- O lume naturală și două artificiale
- 5 revoluții industriale
- > 4400 meserii în COR și > 600 coduri CAEN
- > 85.000 acte normative din care
- >17.300 legi, OG, OUG și HG
- Coexistența și interacțiunile nivelurilor.

Un cadru juridic european în dezvoltare accelerată

În principal (ca relevanță potențială pentru siguranța cibernetică în sectorul bancar):

- Regulamentul IA
- Convenția Cadru a Consiliului Europei
- DORA
- Nis2
- CRA (Cyber Resilience Act),

o parte, deja cu regulamente delegate etc.

Sancțiuni potențiale foarte mari.

Unele aspecte terminologice – Cele 7 elemente principale ale definiției IA

- **Conform IA Act:**
  - „**sistem de IA**” înseamnă un sistem bazat pe o mașină care este conceput să funcționeze cu diferite niveluri de autonomie și care poate prezenta adaptabilitate după implementare, și care, urmărind obiective explicite sau implicite, deduce, din datele de intrare pe care le primește, modul de generare a unor rezultate precum previziuni, conținut, recomandări sau decizii care pot influența mediile fizice sau virtuale;
- **Deci:**
  - **Este bazat pe mașini** – funcționează pe hardware și software;
  - **Are un anumit grad de autonomie** - poate lua decizii fără intervenție umană completă;
  - **Poate fi adaptabil** - în unele cazuri, se poate modifica singur după ce este lansat;
  - **Are obiective explicite sau implicite** - este creat pentru a rezolva anumite probleme;
  - **Face deducții din date** - poate analiza date și genera rezultate bazate pe acestea;
  - **Produce rezultate concrete** - predicții, recomandări, decizii etc.;
  - **Poate influența un mediu fizic sau virtual** - afectează lumea reală sau digitală.
- **În esență**, AI (“Inteligența Artificială”) reprezintă un tip de tehnologie prin care un computer poate gândi și învăța într-un mod asemănător oamenilor.

Diferențe între AI și softul tradițional?

Soft tradițional

- Urmează un set fix de reguli și instrucțiuni definite de programatori. Orice schimbare necesită intervenția umană pentru actualizare.
- Este static, funcționează pe baza regulilor presetate și oferă aceleași rezultate pentru aceleași intrări.
- Necesită instrucțiuni clare din partea utilizatorului pentru a efectua o sarcină.
- Funcționează după un set fix de reguli și instrucțiuni, prin adresarea aceleiași întrebări, se va primi același răspuns de fiecare dată.

AI

- Poate învăța din date și își poate ajusta comportamentul fără a fi nevoie de o reprogramare explicită. Algoritmii AI identifică modele în date și iau decizii bazate pe acestea.
- Se poate adapta și îmbunătăți în timp pe baza experienței și a noilor date primite.
- Poate interpreta limbaj natural, imagini, sunete și poate oferi răspunsuri complexe fără a necesita comenzi exacte.
- Poate funcționa în mod probabilistic, oferind răspunsuri diferite în funcție de învățarea anterioară și de context.

Unele aspecte de context (1)
Evoluția AI în sectorul bancar

- EBA confirma spre finalul anului 2024 că AI era deja folosită pe scară largă în sectorul bancar din UE/SEE, fiind integrată în unele operațiuni de cel puțin 5 ani. Principalele utilizări includ analiza datelor, detectarea fraudelor și îmbunătățirea serviciilor pentru clienți.
- Deși 40% dintre băncile UE folosesc deja Generative AI (GPAI), majoritatea acestora sunt, însă, încă în faza de testare sau experimentare, având în vedere provocările legate de securitate, transparență și explicația rezultatelor.
- Potrivit EBA, majoritatea băncilor din UE folosesc metode AI precum analiza regresivă, arbori de decizie, procesare a limbajului natural și rețele neuronale. Aceste tehnologii sunt utilizate cel mai frecvent în profilarea clienților și tranzacțiilor, dar și pentru prevenirea fraudelor și spălării banilor.
- Unul dintre principalele riscuri identificate de EBA este lipsa de transparență a modelelor AI, în special a celor de tip „black box”, care pot genera decizii opace, dificil de explicat în fața autorităților de reglementare. De asemenea, datele utilizate pentru antrenarea modelelor AI pot introduce abordări subiective, afectând corectitudinea deciziilor luate. Riscuri semnificative potențiale sunt legate și de utilizarea AI în deciziile automate, mai ales în ceea ce privește evaluarea bonității și modelarea riscurilor de credit, unde utilizarea AI nu este încă complet reglementată.
- Conform Raportului comun al Bank of England și Financial Conduct Authority (**“FCA”**)

Unele aspecte de context (2) – Exemple de limitări impuse de Convenția Cadru a Consiliului Europei privind IA (memento)

- Convenția Cadru (semnată de Comisia Europeană în numele UE în sept. 2024) impune respectarea drepturilor fundamentale ale omului în utilizarea IA, conform legislației internaționale și naționale, **iar acest principiu se aplică tuturor sectoarelor, inclusiv celui bancar.** Sistemele de IA nu trebuie să afecteze integritatea proceselor democratice, independența justiției sau accesul echitabil la informații;
- Statele trebuie să adopte măsuri care asigură respectarea principiilor egalității și non-discriminării, transparența și supravegherea adecvată a sistemelor IA, inclusiv în ceea ce privește identificarea conținutului generat de IA. **Aceste măsuri pot include obligații pentru bănci și alte instituții financiare;**
- Convenția Cadru impune ca statele să asigure mecanisme de răspundere a celor responsabili de efectele negative ale IA asupra drepturilor omului, democrației și statului de drept.
- Statele trebuie și să impună măsuri stricte de protecție a datelor și să ofere garanții pentru securitatea informațiilor utilizatorilor;
- Tehnologiile IA trebuie să fie fiabile și sigure, iar inovațiile trebuie testate în medii controlate, sub supravegherea autorităților;
- Persoanele afectate de decizii automate trebuie să aibă acces la mecanisme eficiente de contestare, inclusiv prin instanțe sau soluționare alternativă a litigiilor;
- Persoanele privite de decizii IA trebuie să fie informate că interacționează cu un sistem automat și să beneficieze de garanții procedurale eficiente pentru protejarea drepturilor lor.

Unele aspecte de context (3) - AI Act (memento)

- Reg. (UE) 2024/1689 al PE și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Reg. (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 ("AI Act").
- AI Act reglementează utilizarea tehnologiilor de inteligență artificială în spațiul UE. Scopul principal este acela de a asigura o utilizare sigură și etică a sistemelor AI, protejând drepturile fundamentale ale cetățenilor și promovând inovația.
- Autoritatea de supraveghere a pieței din fiecare stat membru și Autoritatea Europeană pentru Protecția Datelor sunt responsabile de aplicarea AI Act. Statele membre trebuie să desemneze autoritățile de supraveghere de la nivel național până la data de 2 august 2025.
- Prevederile Art. 5 din AI Act au intrat în vigoare la data de 2 Februarie 2025, iar interdicțiile prevăzute de acest articol sunt aplicabile tuturor sistemelor AI, indiferent de momentul la care au fost puse în funcțiune.
- Celelalte capitole ale AI Act vor intra în vigoare începând cu data de 2 August 2025, inclusiv prevederile referitoare la sancțiuni. Astfel că eventualele încălcări ale AI Act nu vor fi sancționate conform prevederilor Regulamentului înainte de 2 August 2025.

Cum clasifică AI Act sistemele de operare utilizate în banking

AI Act utilizează un sistem de clasificare bazat pe riscuri pentru a reglementa sistemele de inteligență artificială, clasificându-le în patru niveluri:

Risc inacceptabil

Conform prevederilor art. 5 din AI Act, este interzisă utilizarea anumitor tehnologii AI, în special acele utilizări care pot genera riscuri sistemice pentru drepturile omului sau pot manipula consumatorii. De exemplu, în esență, este interzisă utilizarea IA pentru:

- manipulare subliminală sau influențarea deciziilor financiare ale clienților fără ca aceștia să își dea seama;
- exploatarea vulnerabilităților (sisteme care profită de vârsta, dizabilitățile sau situația socio-economică a clienților pentru a influența deciziile financiare);
- evaluarea și clasificarea oamenilor pe baza comportamentului lor social, stilului de viață sau a altor date care nu sunt relevante ca atare pentru serviciile bancare;
- a prezice/anticipa dacă o persoană ar putea comite o infracțiune doar pe baza trăsăturilor personale sau a istoricului său.

Risc ridicat

Sistemele AI cu risc ridicat („high-risk”) nu sunt detaliate exhaustiv de AI Act, însă Regulamentul prevede că acestea sunt cele care prezintă un **risc semnificativ de a aduce prejudicii sănătății, siguranței și drepturilor fundamentale.**

Sunt permise în banking, dar trebuie să respecte cerințe stricte pentru a proteja clienții și integritatea pieței financiare. AI Act impune utilizarea mecanismelor de control uman, iar băncile trebuie să garanteze că IA nu ia decizii fără validare umană.

Pentru ca un sistem AI să fie clasificat drept sistem cu risc ridicat, Art. 6 din AI Act prevede că acesta trebuie să îndeplinească anumite criterii specifice sau să facă parte dintr-o listă prestabilită de domenii reglementate, în conformitate cu următoarele trei categorii:

- Sistemul AI este utilizat ca o componentă de siguranță a unui produs;
- Sistemul AI este un produs în sine, reglementat de legislația de armonizare a UE, conform Anexei I a AI Act;
- Sistemul AI este menționat explicit în Anexa III a AI Act, ceea ce îl încadrează automat ca fiind cu risc ridicat.

În cazul sistemelor menționate în Anexa III a AI Act, operatorii pot demonstra că acestea nu prezintă un risc semnificativ pentru sănătate, siguranță sau drepturile fundamentale și că nu influențează în mod substanțial rezultatele procesului decizional. Dacă această demonstrație este validată de autorități, sistemul poate fi exceptat de la regimul strict aplicabil HRS.

Sisteme AI în domeniul financiar care prezintă risc ridicat

Sistemele AI utilizate în domeniul financiar considerate de risc ridicat trebuie să respecte cerințe stricte de transparență, supraveghere umană, management al riscurilor și guvernanță a datelor.

- **Luarea deciziilor în materie de creditare** – pot fi utilizate sisteme AI în evaluarea bonității prin analiza veniturilor, cheltuielilor și istoricului financiar al unui client prin estimarea probabilității de rambursare. Însă AI nu poate lua decizia finală în mod automatizat, ci rezultatul AI va rămâne la aprecierea unei persoane.
- **Detectarea fraudelor** – pot fi utilizate sisteme AI pentru identificarea tranzacțiilor suspecte și identificarea modalităților de fraudă. Sistemele AI analizează modelele de tranzacționare prin comparație cu mecanismele anterioare de fraudă. De asemenea, sistemul AI trebuie să fie supravegheat de o persoană, pentru a putea evita decizii incorecte, întrucât conform raportului FSB, AI poate genera un număr mare de alarme false, afectând utilizatorii.
- **Monitorizarea tranzacțiilor suspecte** – sistemele AI pot fi utilizate și pentru supravegherea fluxurilor financiare și raportarea automată a tranzacțiilor care depășesc anumite limite sau care sunt suspecte. Analiza trebuie să se bazeze exclusiv pe date obiective și

AI Act vs GDPR

GDPR	AI Act
Printre altele, GDPR cere consimțământul explicit pentru colectarea și utilizarea categoriilor speciale de date personale (ex: date biometrice, istoricul medical). Utilizatorul are dreptul de a refuza acordarea consimțământului.	AI Act permite utilizarea datelor în scopuri de antrenare a modelelor AI, chiar și fără consimțământ direct, în anumite condiții. Recunoașterea facială și analiza emoțiilor sunt permise în contexte „de securitate” sau „interes public”, chiar dacă GDPR restricționează astfel de practici.
GDPR permite utilizarea datelor biometrice (ex. amprente, recunoaștere facială) doar în baza unor situații de excepție, precum consimțământul explicit.	AI Act permite supravegherea biometrică în spații publice pentru „interese de securitate” și „combaterea criminalității”.
GDPR permite utilizatorilor să solicite ștergerea datelor personale, iar datele trebuie șterse dacă nu mai sunt necesare sau alte condiții expres menționate sunt îndeplinite.	AI Act nu specifică cum ar trebui gestionate datele folosite deja în antrenarea unui AI.
GDPR face clar cine este responsabil pentru o încălcare a protecției datelor –	AI Act introduce reguli pentru dezvoltatorii AI, dar nu clarifică mereu

Unele aspecte de context (4) – DORA

- Reg. (UE) 2022/2554 al PE și al Consiliului din 14 dec. 2022 privind reziliența operațională digitală a sectorului financiar („DORA”) - publicat pe16 ian. 2023 și intrat în vigoare pe 17 ian. 2025
- Obiectivul principal al DORA : participanții la piața financiară să poată continua să funcționeze în condiții de siguranță și fiabilitate, chiar și în cazul unor perturbări semnificative ale sistemelor de tehnologia informației și comunicațiilor (TIC). În plus, reducerea riscului de disfuncționalități sistemice și protejarea consumatorilor, precum și a economiei în ansamblu.
- Entitățile financiare trebuie să **integreze gestionarea riscurilor TIC în guvernanța corporativă**. Membrii organului de conducere trebuie să își asume în mod direct responsabilitatea pentru **identificarea**, **evaluarea** și **atenuarea** riscurilor TIC.
- Clasificarea incidentelor TIC și a amenințărilor cibernetice. Entitățile financiare sunt obligate **să raporteze** incidentele majore legate de TIC către autorități în termene specifice (raportare inițială, intermediară și finală).
- Entitățile financiare trebuie **să informeze** fără întârziere nejustificată, imediat ce iau cunoștință de situație, clienții și utilizatorii afectați, în cazul în care un incident TIC este susceptibil să aibă consecințe financiare sau să perturbe serviciile oferite acestora
- DORA se extinde și asupra unor entități care, în mod obișnuit, sunt exceptate de la reglementările financiare – precum furnizorii terți de servicii TIC care oferă instituțiilor financiare sisteme și servicii legate de TIC, precum furnizorii de

DORA - Definiții relevante principale

- „**Atac cibernetic**” înseamnă un incident legat de TIC, de natură rău intenționată, cauzat de o tentativă a oricărui actor de amenințare de a distruge, expune, modifica, dezactiva, fura sau obține acces neautorizat la un activ ori de a-l utiliza în mod neautorizat;
- „**Funcție critică sau importantă**” înseamnă o funcție a cărei perturbare ar compromite în mod semnificativ performanța financiară a unei entități financiare sau soliditatea ori continuitatea serviciilor și activităților acesteia sau a cărei întrerupere, îndeplinire defectuoasă ori neîndeplinire ar compromite în mod semnificativ respectarea continuă de către entitatea financiară a condițiilor și obligațiilor aferente autorizației sale ori a altor obligații care îi revin conform legislației aplicabile din domeniul serviciilor financiare;
- „**Reziliență operațională digitală**” înseamnă capacitatea unei entități financiare de a-și construi, asigura și revizui integritatea și fiabilitatea operațională prin garantarea, direct sau indirect, prin utilizarea serviciilor furnizate de furnizori terți de servicii TIC, a întregii game de capacități legate de TIC necesare pentru a aborda securitatea rețelelor și a sistemelor informatice utilizate de entitatea financiară și care sprijină furnizarea continuă a serviciilor financiare și calitatea acestora, inclusiv pe durata perturbărilor;
- „**Risc legat de TIC**” înseamnă orice situație identificabilă în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice care, în cazul în care se materializează, poate compromite securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operațiunilor și proceselor ori a prestării de servicii, prin producerea unor efecte negative în mediul digital sau fizic;
- „**Incident legat de TIC**” înseamnă un eveniment unic sau o serie de evenimente interconectate, neplanificate de entitatea financiară, care compromit securitatea rețelelor și a sistemelor informatice și au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor sau asupra serviciilor furnizate de entitatea financiară;

DORA – Construirea unei reziliențe proactive

- DORA impune un cadru cuprinzător de gestionare a riscurilor legate de TIC pentru ca entitățile financiare să identifice, evalueze și atenueze proactiv amenințările digitale.
- O cerință centrală este aceea ca entitățile financiare să **identifice**, să **clasifice** și să **documenteze** corespunzător toate funcțiile de afaceri susținute prin TIC, rolurile și responsabilitățile aferente, activele informaționale și activele TIC care sprijină respectivele funcții, precum și rolurile și dependențele acestora în ceea ce privește riscul legat de TIC. Entitățile financiare trebuie să revizuiască, ori de câte ori este necesar și cel puțin o dată pe an, relevanța acestei clasificări și a documentației asociate.
- Pentru a proteja sistemele critice și datele sensibile, entitățile financiare trebuie **să implementeze mecanisme riguroase de protecție și prevenție**. Acestea includ **măsuri tehnice avansate**, cum ar fi criptarea, sisteme de detectare a intruziunilor și firewall-uri, completate de **testări periodice** de securitate și **evaluări ale vulnerabilităților**, pentru a aborda pro activ eventualele puncte slabe.
- Controlul accesului trebuie menținut strict, asigurând că personalul care gestionează sistemele TIC dispune de **formare adecvată** pentru a reduce riscurile interne.
- **Protocoalele eficiente de comunicare** sunt esențiale atât pentru gestionarea crizelor interne, cât și pentru raportările către autoritățile de supraveghere, garantând transparență în cazul unei deficiențe majore a TIC. În plus, entitățile

DORA – Construirea unei reziliențe proactive (cont)

- Entitățile financiare trebuie să mențină un program structurat de testare a rezilienței operaționale digitale, care să includă **diverse metodologii**, precum: **evaluări și scanări ale vulnerabilităților**, **teste de penetrare**, **evaluări ale securității rețelei** și **revizuiri ale codului sursă**. Aceste testări trebuie să fie independente, efectuate cel puțin anual pentru sistemele TIC critice. Totodată, sunt necesare **proceduri clare de prioritizare**, **clasificare și remediere a deficiențelor** identificate.
- Un element-cheie al cadrului de testare prevăzut de DORA îl constituie testarea de penetrare tip Threat-Led Penetration Testing – „TLPT” (cel puțin o dată la trei ani de către anumite entități financiare cu impact semnificativ). Domeniul de aplicare al TLPT se stabilește în funcție de infrastructura TIC a entității, serviciile externalizate și profilul de risc, iar testarea trebuie validată de autoritățile competente.
- Dacă furnizorii terți de servicii TIC sunt incluși în domeniul de aplicare al TLPT, entitatea financiară trebuie să ia măsurile și garanțiile necesare pentru a asigura participarea acestora la testare și rămâne responsabilă pentru respectarea DORA.
- După efectuarea testărilor, entitățile trebuie să transmită constatările, planurile de remediere și documentația aferentă conformității către autoritățile de supraveghere, care, la rândul lor, vor furniza atestate pentru recunoașterea reciprocă a testărilor la nivel transfrontalier.
- Pentru a garanta cele mai înalte standarde în testarea securității cibernetice, DORA impune criterii stricte de eligibilitate pentru echipele de testare TLPT. Testatorii externi trebuie să fie recunoscuți, certificați, asigurați și să dispună de expertiză în intelligence cibernetic, teste de penetrare și simulări Red Team.
- Contractele cu testatorii externi trebuie să prevadă măsuri de protecție a rezultatelor TLPT, pentru a preveni scurgerile de date sau apariția unor riscuri nejustificate.

DORA – Gestionarea riscurilor legate de furnizorii terți de servicii TIC

DORA impune entităților financiare obligația de a implementa **clauze contractuale corespunzătoare pentru utilizarea serviciilor TIC care sprijină activitățile lor operaționale**, asigurând respectarea standardelor de securitate IT. Cel puțin, următoarele elemente:

- O descriere clară și completă a tuturor funcțiilor și serviciilor TIC care urmează a fi furnizate de furnizorul terț de servicii TIC, cu indicarea dacă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau a unor părți esențiale ale acesteia este permisă și în ce condiții se poate face aceasta;
- Locațiile (respectiv regiunile sau țările) în care urmează să fie furnizate funcțiile și serviciile TIC contractate sau subcontractate, precum și locația în care se procesează datele, inclusiv locul de stocare a acestora, și obligația furnizorului terț de servicii TIC de a notifica în prealabil entitatea financiară în cazul în care intenționează să schimbe aceste locații;
- Clauze privind disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, inclusiv a datelor cu caracter personal;
- Prevederi privind accesul, recuperarea și returnarea datelor cu caracter personal și a celor fără caracter personal, într-un format ușor accesibil, în cazul insolvabilității, al intrării în procedură de rezoluție sau al încetării activității furnizorului terț de servicii TIC, ori în cazul rezilierii acordurilor contractuale;
- Descrierea nivelurilor de servicii, inclusiv actualizările și revizuirile acestora;
- Obligația furnizorului terț de servicii TIC de a acorda asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante, în cazul apariției unui incident legat de TIC asociat serviciului furnizat;
- Obligația furnizorului terț de servicii TIC de a coopera în mod deplin cu autoritățile competente și cu autoritățile de decizie ale entității financiare;
- Clauze privind drepturile de reziliere și termenele minime de preaviz aferente încetării acordurilor contractuale;
- Condițiile de participare a furnizorilor terți de servicii TIC la programele de conștientizare în materie de securitate TIC și de formare privind reziliența operațională digitală organizate de entitățile financiare.

DORA – Relația cu Directiva NIS2

Merită menționat mai ales că:

- DORA se aplică entităților din sectorul financiar din UE, în timp ce Directiva NIS2 se extinde asupra altor sectoare, precum sănătatea, energia, transporturile, infrastructura digitală și altele;
- Cerințele prevăzute de DORA și Directiva NIS2 se pot suprapune, în special în cazul instituțiilor financiare, care sunt considerate și entități esențiale în sensul Directivei NIS2;
- DORA, în calitate de lex specialis, are prioritate față de Directiva NIS2 în ceea ce privește sectorul financiar, oferind cerințe mai detaliate în materie de gestionare a riscurilor legate de TIC și raportarea incidentelor;
- În timp ce DORA oferă norme specifice pentru instituțiile financiare, Directiva NIS2 impune obligații generale, care rămân aplicabile în paralel;
- Societățile care intră exclusiv sub incidența Directivei NIS2 nu sunt obligate să respecte cerințele prevăzute de DORA.

Ce înseamnă toate cele de mai sus? - Siguranța cibernetică în context AI pentru juriști (1)

Problema corelării dreptului cu revoluțiile industriale nu doar că subzistă, dar este mărită semnificativ în context IA

5 tendințe importante ale revoluției industriale ce include IA (și ale politicii de reglementare):

- Abstractizarea și creșterea în complexitate a tehnologiei de masă
- Creșterea numărului potențial de surse de probleme pentru siguranța cibernetică
- Tendința spre extinderea răspunderilor juridice “cvasiobiective”
- Presiunea spre creșterea numărului de cazuri de “piercing of the veil” orientat către interior (management)
- Delegarea în mare parte de către stat a “apărării” către operatori/utilizatori

Ce înseamnă toate cele de mai sus? - Siguranța cibernetică în context AI pentru juriști (2)

- Număr mare de verigi și segmente de avut în vedere
- Număr potențial mare de stakeholders (tendință spre consolidare)
- Probema dinamicii în timp (și ritmului schimbărilor)
- Importanța majoră a procedurilor, dar insuficiența lor (cu risc de tranformare în hârțogărie).
- Contractarea de furnizori terți, versus dezvoltare “in-house”
- Echilibrul între protejarea proprietății intelectuale și datelor comerciale sensibile, nevoia de siguranță și cea de transparență și raportare

Ce înseamnă toate cele de mai sus? - Siguranța cibernetică în context AI pentru juriști (3)

- Limitele supervizării umane (mai ales în timp)
- Variabilitate mult mai mare a puterii de negociere, ceea ce defavorizează România
- Legat parțial de aspectul de mai sus - problema limitărilor de răspundere, dar și a caracterului prea tehnic. Diferența dintre contracte perfecte și remedii efective.
- Problema rapoartelor de expertiză – problemă de hardware, de software, de input de date, de eroare umană, de expert, de atac cu viruși, de conectare la sisteme deficitare, de obiective, de metodă de training etc
- Riscul de “analfabetism funcțional” la nivelul juriștilor

Concluzii

- Sistemele AI oferă numeroase beneficii sectorului bancar, dar prezintă și riscuri potențiale semnificative, inclusiv în zona siguranței cibernetice;
- "Delegarea" în bună parte a apărării de către stat și presiunea spre o răspundere "cvasiobiectivă" în zona siguranței cibernetice sunt exagerate;
- De asemenea, o parte din tendințele reglementărilor din zona siguranței cibernetice nu sunt rezonabile sau sustenabile pe termen lung pentru majoritatea jucătorilor actuali și dezavantajează țările mai mici, precum România;
- Limitele intervenției juriștilor trebuie înțelese bine, inclusiv … de către juriști;
- Abordări cât mai moderate din partea autorităților și sprijinirea elaborării de standarde rezonabile pentru industrie vor fi foarte importante în următorii ani.