

Educația tinerilor în scopul prevenției fraudelor financiare online



Disclaimer: Acest material este dedicat tinerilor cu scopul de a-i familiariza cu principalele tipuri de fraude financiare ce se pot întâmpla în mediul online, cu scopul de a-i ajuta să anticipeze posibile fraude informatice și să combată perpetuarea acestora către un număr mare de persoane. Unele detalii din prezentul material ar putea să se schimbe în timp, așa că recomandăm să fie verificate întotdeauna informațiile.

Director de proiect:
Prof.univ.dr. Dorel Paraschiv



CUPRINS

1. Introducere

04

2. Educația Digitală în Uniunea Europeană

09

3. Necesitatea educației digitale în rândul tinerilor

16

3.1 Educația financiară digitală

3.2 Integrarea alfabetizării digitale în educația tinerilor și studenților

3.3 Dezvoltarea competențelor digitale ale elevilor/studenților

3.4. Rolul familiei, instituțiilor de învățământ și a mediului financiar-bancar în formarea competențelor financiare digitale în rândul tinerilor.

4. Fraudele financiare online – o perspectivă generală

28

4.1 Definirea și clasificarea fraudelor financiare online

4.1.1 Tipologii recunoscute în România și la nivel european

4.2 Evoluția fenomenului de fraudă în era digitală

4.3 Instrumente și tehnici folosite de infractorii cibernetici

4.3.1 Phishing

4.3.2 Investment Scam

4.3.3 Spoofing

4.3.4 Deepfake

4.3.5 Online Shopping Platforms Fraud

5. Vulnerabilitatea în fața fraudelor online a tinerilor

48

5.1 Factori care favorizează expunerea la fraude online

5.2 Aspecte comportamentale ale tinerilor care cresc gradul de vulnerabilitate

6. Combaterea fraudelor financiare online

52

6.1 Cadrul legislativ la nivel național și european

6.2 Rolul instituțiilor financiare în prevenirea și combaterea fraudelor

6.3 Colaborarea interinstituțională

7. Tranzacții online în siguranță – sfaturi esențiale pentru tineri

75

7.1 Verificarea site-urilor și platformelor de plată

7.2 Importanța protejării datelor personale și bancare

7.3 Semnale de alarmă (phishing, oferte false, investiții, aplicații periculoase)

7.4 Utilizarea metodelor sigure de plată și autentificare

7.4.1 Metode de plată recomandate și controlul riscului

7.4.2 Practici de autentificare sigure și exemple concrete

7.4.3 Configurări de control tranzacțional

7.4.4 Scenarii uzuale și soluții

7.4.5 Greșeli frecvente de evitat, cu exemple

7.4.6 Proceduri de răspuns în caz de suspiciune

Concluzii

88

Bibliografie

90

1. Introducere

Educația digitală reprezintă capacitatea de a identifica, înțelege, utiliza, crea și interacționa în mod eficient cu tehnologia, mediile online și resursele digitale. Deși indivizii, în special tinerii, utilizează zilnic tehnologia, nivelul lor de încredere și abilitatea de a se adapta la instrumentele digitale aflate într-o continuă evoluție pot varia considerabil. Consolidarea competențelor digitale este esențială, întrucât îi ajută pe indivizi să acceseze informații financiare, să își gestioneze finanțele personale, să utilizeze servicii bancare digitale și să își construiască un viitor economic sustenabil.

În cadrul conceptului mai larg de incluziune digitală, educația digitală reprezintă un pilon esențial, alături de accesul la internet de mare viteză, la un cost accesibil, și de utilizarea unor dispozitive digitale cu preț redus. Dezvoltarea unor competențe digitale solide le permite persoanelor să navigheze în siguranță și eficient pe platforme financiare, să ia decizii financiare informate și să beneficieze pe deplin de instrumentele și resursele financiare online.



Competențele de educație digitală financiară variază de la un nivel de bază la unul avansat. La nivel elementar, instruirea poate include navigarea pe site-ul unei instituții financiare, utilizarea aplicațiilor de mobile banking sau efectuarea de plăți online securizate. La un nivel avansat, educația digitală financiară poate cuprinde înțelegerea securității cibernetice în tranzacțiile financiare, utilizarea aplicațiilor de bugetare și investiții sau chiar analiza datelor financiare cu ajutorul unor programe specializate. Dezvoltând aceste competențe, indivizii sunt mai bine pregătiți să participe în siguranță și eficient la economia digitală.

De ce este importantă educația digitală și formarea competențelor digitale?

Tehnologia digitală poate fi un catalizator important pentru schimbări pozitive, cu condiția ca oamenii să dețină nivelul necesar de educație și competențe digitale pentru a participa în mod egal, semnificativ și sigur în spațiul digital.

Accesul la tehnologia digitală le permite indivizilor să rămână conectați cu familia și prietenii, să acceseze informații și servicii esențiale și să participe activ la oportunități educaționale, profesionale și economice. Într-o lume globalizată și interconectată, competențele digitale le oferă oamenilor posibilitatea de a-și îmbunătăți calitatea vieții, de a-și susține drepturile și de a se integra în comunități dinamice și moderne. O educație digitală solidă le permite indivizilor și comunităților să depășească obstacole, să rămână informați și să își construiască un viitor mai stabil.

Dezvoltarea competențelor digitale este esențială și pentru accesarea și utilizarea serviciilor online, care includ servicii publice (plăți de taxe, acces la documente oficiale, programe de sprijin social), dar și servicii financiare digitale precum online banking, plăți electronice, aplicații de bugetare, investiții sau asigurări. Lipsa abilităților digitale poate limita accesul la aceste resurse, ducând la excludere economică și socială, în timp ce dobândirea acestor competențe îi ajută pe oameni să își gestioneze mai eficient finanțele, să economisească timp și bani și să acceseze oportunități economice diverse.

Resursele și instrumentele trebuie puse la dispoziție pentru a facilita dezvoltarea competențelor digitale și a educației digitale necesare, astfel încât să fie abordată problema siguranței online

Cu toate acestea, oportunitățile de perfecționare digitală sunt adesea limitate, iar unele inițiative de dezvoltare a competențelor digitale nu sunt suficient de incluzive sau accesibile pentru toate categoriile sociale. Mulți oameni se confruntă cu lacune educaționale, acces redus la formare digitală sau condiții de infrastructură slab dezvoltate, ceea ce le limitează capacitatea de a aplica și dezvolta aceste competențe. Acest lucru contribuie la adâncirea decalajului digital și reduce șansele de participare activă în economia digitală.

Diferențele de competențe digitale pun în pericol și eficiența intervențiilor digitale. Succesul programelor digitale depinde în mod direct de capacitatea utilizatorilor de a interacționa eficient cu tehnologia. Fără abilități digitale adecvate, există riscul ca persoanele aflate în nevoie să fie excluse de la servicii esențiale precum asistența umanitară, sprijinul juridic, accesul la educație și sănătate, servicii financiare online sau instrumente de protecție și susținere. Pe măsură ce tot mai multe dintre aceste servicii devin exclusiv digitale, devine tot mai urgentă intervenția în domeniul educației digitale.

Este nevoie de un efort susținut pentru a sprijini toate categoriile de populație în utilizarea eficientă și sigură a tehnologiei, reducând riscurile digitale. În lipsa acțiunii, grupurile cele mai vulnerabile – precum femeile, persoanele în vârstă, cele cu dizabilități sau cu venituri reduse – vor fi cele mai expuse riscului de excluziune și de prejudicii în mediul digital. Consolidarea competențelor digitale, inclusiv a celor necesare pentru utilizarea serviciilor financiare online, este o condiție esențială pentru incluziunea socială și economică.

Consecințele inacțiunii și riscurile lipsei de educație digitală

Este esențial ca persoanele să dețină competențele și cunoștințele necesare pentru a minimiza riscurile asociate utilizării tehnologiei. Dezvoltarea abilităților digitale nu este importantă doar pentru siguranța în mediul online, ci și pentru a le permite oamenilor să acceseze servicii esențiale – de la informații oficiale, educație și sănătate, până la servicii financiare online precum plăți electronice, transferuri bancare, aplicații de bugetare sau platforme de economisire și investiții. Lipsa competențelor digitale limitează capacitatea indivizilor de a beneficia de aceste resurse, crescând riscul de excludere socială și economică.

Lipsa educației digitale poate conduce la riscuri serioase, inclusiv, dar fără a se limita la:

- expunerea la fraude online, furt de identitate și abuzuri digitale;
- excluderea de la servicii esențiale (educație, sănătate, sprijin social și umanitar) și de la servicii financiare online, esențiale pentru participarea economică;
- vulnerabilitate crescută la dezinformare și manipulare online;
- bariere în găsirea unui loc de muncă, dezvoltarea profesională sau accesul la oportunități economice;
- izolare socială și limitarea capacității de a comunica și interacționa în siguranță în mediul digital;
- creșterea decalajului digital între grupurile vulnerabile și restul populației, ceea ce reduce șansele de integrare socială și economică.

Prin urmare, educația digitală și dezvoltarea competențelor digitale, inclusiv a celor necesare utilizării serviciilor financiare online, reprezintă o componentă esențială a protecției, incluziunii sociale și economice, precum și a autonomiei persoanelor.

Educația financiară în era digitală

Într-o lume din ce în ce mai digitalizată, tot mai multe persoane accesează servicii financiare online. Totuși, este bine cunoscut faptul că în România ne confruntăm atât cu un nivel scăzut al competențelor digitale (penultimul loc în Uniunea Europeană, conform Eurostat[1]), cât și cu un nivel scăzut al nivelului de educație financiară (ultimul loc în Uniunea Europeană, conform Eurostat[2]), iar această situație reprezintă o vulnerabilitate importantă a populației din România când vine vorba de securitatea și siguranța finanțelor personale.

România a lansat în anul 2024 Strategia Națională de Educație Financiară 2024–2030 (SNEF)[1] care își propune să stabilească obiective concrete și direcții de acțiune până în anul 2030, având ca scop creșterea nivelului de educație financiară în rândul elevilor, studenților, adulților și mediului de afaceri din România. Conform Strategiei, educația financiară este considerată o prioritate comună la nivel național, atât pentru sectorul public, cât și pentru cel privat. Ea nu reprezintă o consecință a dezvoltării economice, ci un factor care o stimulează și o susține. Un nivel mai ridicat al educației financiare determină schimbări de comportament care duc la o mai bună stabilitate financiară, la creșterea bunăstării populației și, implicit, la progresul economic al țării. Strategia urmărește consolidarea culturii de alfabetizare financiară printr-un set de măsuri variate, coerente și adaptate diferitelor categorii de populație, pentru a ridica nivelul de cunoștințe și competențe în domeniu.

Educația financiară are efecte directe asupra calității vieții: sprijină obținerea unei mai bune siguranțe financiare, permite acumularea de resurse suplimentare pentru pensie și crește reziliența în fața riscurilor, cum ar fi crizele economice sau perioadele dificile generate de evenimente neprevăzute. Din acest motiv, este important să se integreze conceptele financiare în programele școlare, să formeze elevii și cadrele didactice, să informeze populația adultă și să perfecționeze angajații operatorilor economici, contribuind astfel la dezvoltarea nivelului de educație al actualilor și viitorilor utilizatori de produse și servicii financiare.

În vederea realizării acestui studiu s-au avut în vedere patru obiective care au fost atinse astfel:

- O1. Evaluarea nivelului actual de educație financiară și digitală în rândul tinerilor. Care sunt sursele principale de informare ale tinerilor în domeniul securității cibernetice și al educației financiare (Obiectiv atins în Capitolul 2).
- O2. Analiza comportamentelor digitale ale tinerilor și gradul de conștientizare privind riscurile financiare online (Obiectiv atins în Capitolul 3).
- O3. Identificarea tipologiilor frecvente de fraude financiare online care afectează tinerii (ex: phishing, fraude cu carduri, scam-uri pe rețelele sociale, aplicații false etc.) - (Obiectiv atins în Capitolele 4 și 5).
- O4. Analiza principalelor metode de prevenție a fraudelor financiare online și a acțiunilor pe care o entitate din domeniul financiar – bancar le-ar putea implementa pentru a preveni fraudele financiare (Obiectiv atins în Capitolele 6 și 7).

Totodată, rezultatele acestui studiu vor fi sintetizate în Ghiduri practice pentru tineri tocmai cu scopul de a crește nivelul competențelor financiare digitale.

2. Educația Digitală în Uniunea Europeană

Competențele și abilitățile digitale sunt esențiale pentru incluziunea socială, bunăstare, cetățenie activă și angajabilitate, precum și pentru productivitatea, competitivitatea și reziliența Uniunii Europene. Având în vedere importanța acestor competențe pentru societate și economie, Uniunea Europeană a stabilit o serie de obiective privind dezvoltarea competențelor digitale. Totuși, datele și tendințele recente arată clar că este nevoie de eforturi suplimentare pentru a accelera progresul către atingerea acestor obiective. În contextul revizuirii Planului de Acțiune pentru Educație Digitală al Comisiei Europene, urmează să fie adoptată o foaie de parcurs pentru viitorul educației și formării digitale.

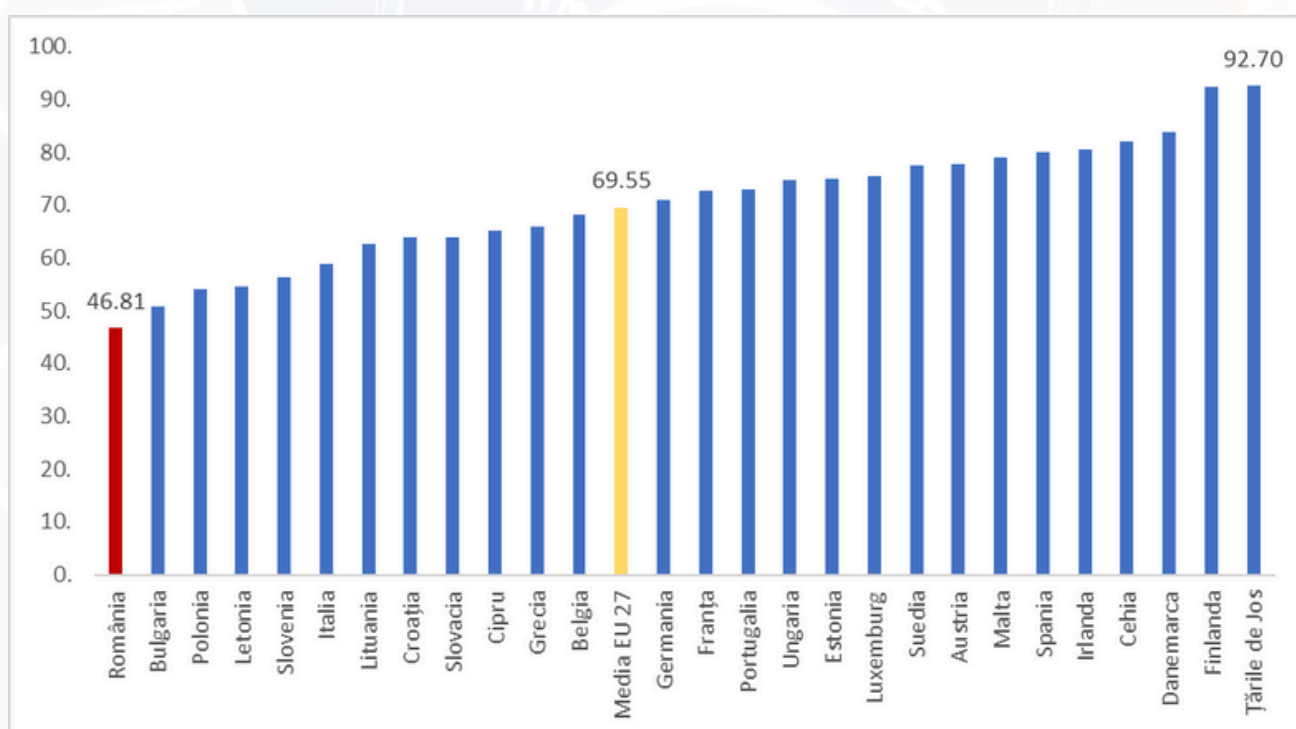
Transformarea digitală, impulsionată de inovație și dezvoltarea tehnologică, modelează profund societatea și economia, generând o cerere tot mai mare de competențe digitale (Van Veldhoven și Vanthienen, 2022). Toți cetățenii au nevoie de abilități și competențe digitale pentru a se dezvolta personal, a-și găsi un loc de muncă și a participa activ în comunitatea lor. De asemenea, aceste competențe sunt vitale pentru ca oamenii să poată înțelege și naviga cantitatea uriașă de informații întâlnite online și să identifice tentativele de fraudă.

Viitorul competitivității Uniunii Europene este strâns legat de dezvoltarea competențelor digitale fiind un factor cheie pentru tranziția digitală de succes a UE, cât și esențială pentru adoptarea și valorificarea noilor tehnologii. Totodată, raportul evidențiază creșterea cererii pentru competențe digitale avansate în domenii precum inteligența artificială (AI), programare, gestionarea datelor și securitatea cibernetică. În acest context, raportul insistă asupra rolului crucial al sistemelor de educație și formare în dotarea populației cu competențe de înaltă calitate, într-un mod incluziv.

Astfel, competențele digitale devin din ce în ce mai esențiale atât pentru viața personală (Livingstone et al, 2023), cât și pentru cea profesională. În prezent, peste 90% dintre locurile de muncă din Europa necesită cunoștințe digitale de bază, alături de abilități tradiționale precum alfabetizarea și calculul matematic. Cu toate acestea, aproximativ 32% dintre europeni încă nu dețin competențe digitale de bază. Având în vedere rolul omniprezent al tehnologiei digitale în sectoare care variază de la afaceri la transport și agricultură, devine tot mai importantă măsurarea și îmbunătățirea competențelor digitale la nivelul întregii Uniuni Europene.

Conform EUROSTAT [4], în Uniunea Europeană aproximativ 69% dintre persoanele cu vârste între 16 și 74 de ani aveau cel puțin competențe digitale generale de bază. Există totuși diferențe semnificative între statele membre, 92% în Țările de Jos și 46% în România (Figura 2.1).

**Figura 2.1. Nivelul de competențe digitale generale de bază în EU27
(% din total populație)**



Sursa: Eurostat 2024

Totuși, nivelul educației formale influențează gradul de competențe digitale al indivizilor (Tabel 1.1). Diferența în ceea ce privește competențele digitale de bază între persoanele cu un nivel ridicat de educație (80%) și cele fără educație formală sau cu educație scăzută (34%) în Uniunea Europeană era de 46 puncte procentuale (pp). Cele mai mari diferențe au fost înregistrate în Portugalia (66 pp), Grecia (63 pp) și Malta (59 pp). În schimb, cele mai mici diferențe au fost observate în Estonia (12 pp), Finlanda (14 pp) și Lituania (22 pp).

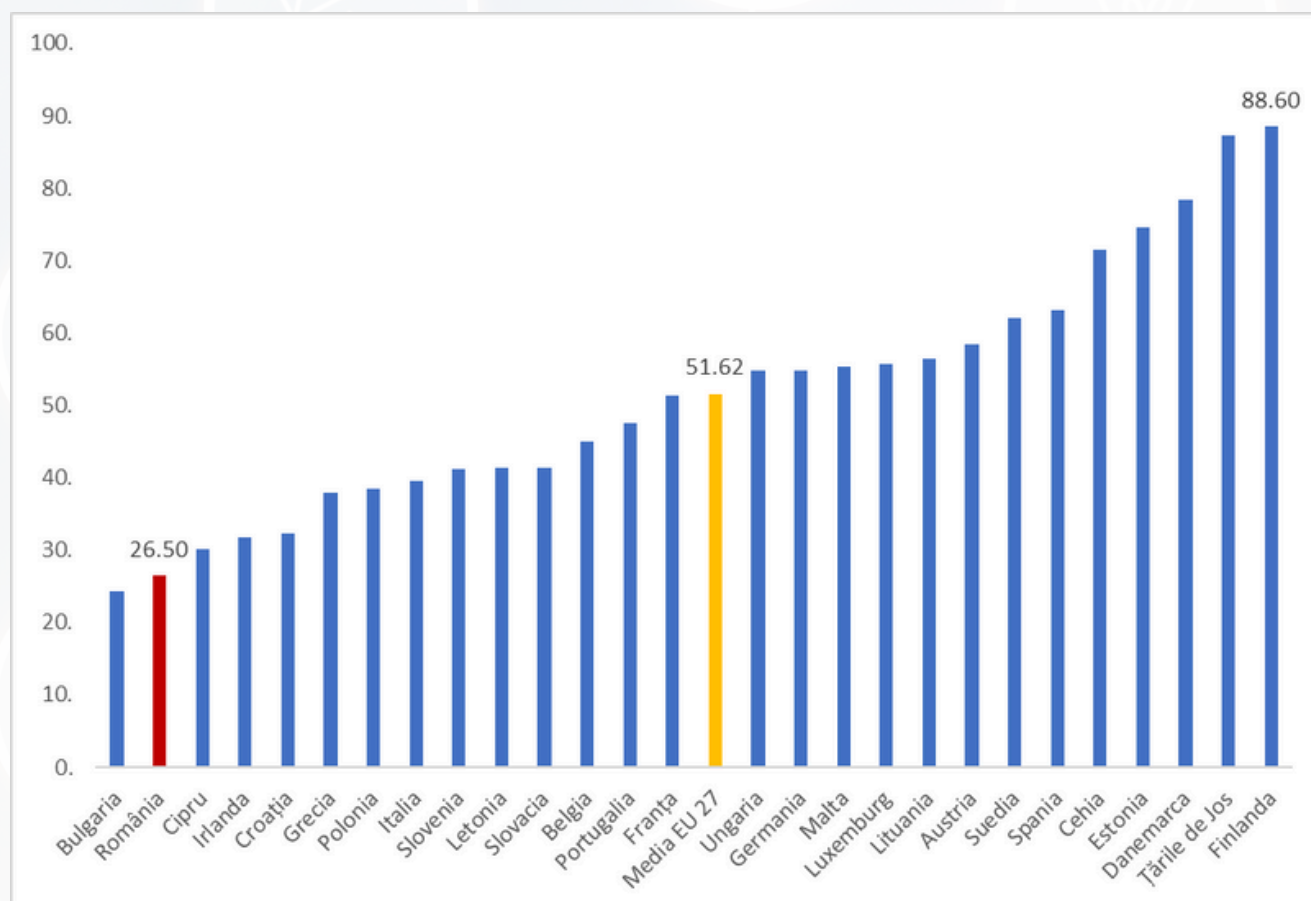
Tabel 1.1. Nivelul de competențe digitale generale de bază în EU27 pe nivel educațional (% din total populație)

	General	Persoane fără sau cu nivel de bază de educație (%)	Persoane cu nivel mediu de educație	Persoane cu nivel ridicat de educație
România	46,81	26,50	46,66	75,91
Bulgaria	50,75	24,34	47,41	77,76
Polonia	54,06	38,47	44,17	79,63
Letonia	54,61	41,37	44,94	72,19
Slovenia	56,34	41,25	52,21	74,43
Italia	59,00	39,61	65,58	80,84
Lituania	62,68	56,48	48,32	80,05
Croația	63,90	32,31	70,38	86,29
Slovacia	63,91	41,38	59,67	84,32
Cipru	65,26	30,05	62,81	82,38
Grecia	66,03	37,88	68,21	87,39
Belgia	68,20	44,94	64,71	85,29
Media EU 27	69,55	51,62	67,48	87,07
Germania	71,03	54,78	70,24	84,30
Franța	72,69	51,34	71,11	88,87
Portugalia	73,07	47,60	90,52	94,20
Ungaria	74,81	54,77	73,06	89,39
Estonia	74,97	74,67	70,68	79,29
Luxemburg	75,49	55,69	74,15	87,74
Suedia	77,42	62,08	76,00	87,72
Austria	77,67	58,37	76,75	88,66
Malta	78,96	55,42	88,21	96,14
Spania	80,12	63,13	87,77	92,23
Irlanda	80,69	31,84	73,28	93,00
Cehia	81,98	71,43	79,02	96,33
Danemarca	83,95	78,36	82,07	91,28
Finlanda	92,35	88,60	90,70	96,77
Țările de Jos	92,70	87,37	91,88	96,87

Sursa: Eurostat 2024

Astfel, în Uniunea Europeană aproximativ 51% dintre persoanele cu un nivel scăzut de educație sau deloc, cu vârste între 16 și 74 de ani, aveau cel puțin competențe digitale generale de bază. Există totuși diferențe semnificative între statele membre, 83% în Țările de Jos și 26.5% în România (Figura 2.2).

Figura 2.2. Nivelul de competențe digitale generale de bază în EU27 în rândul persoanelor fără sau cu un nivel scăzut de educație (% din total populație)

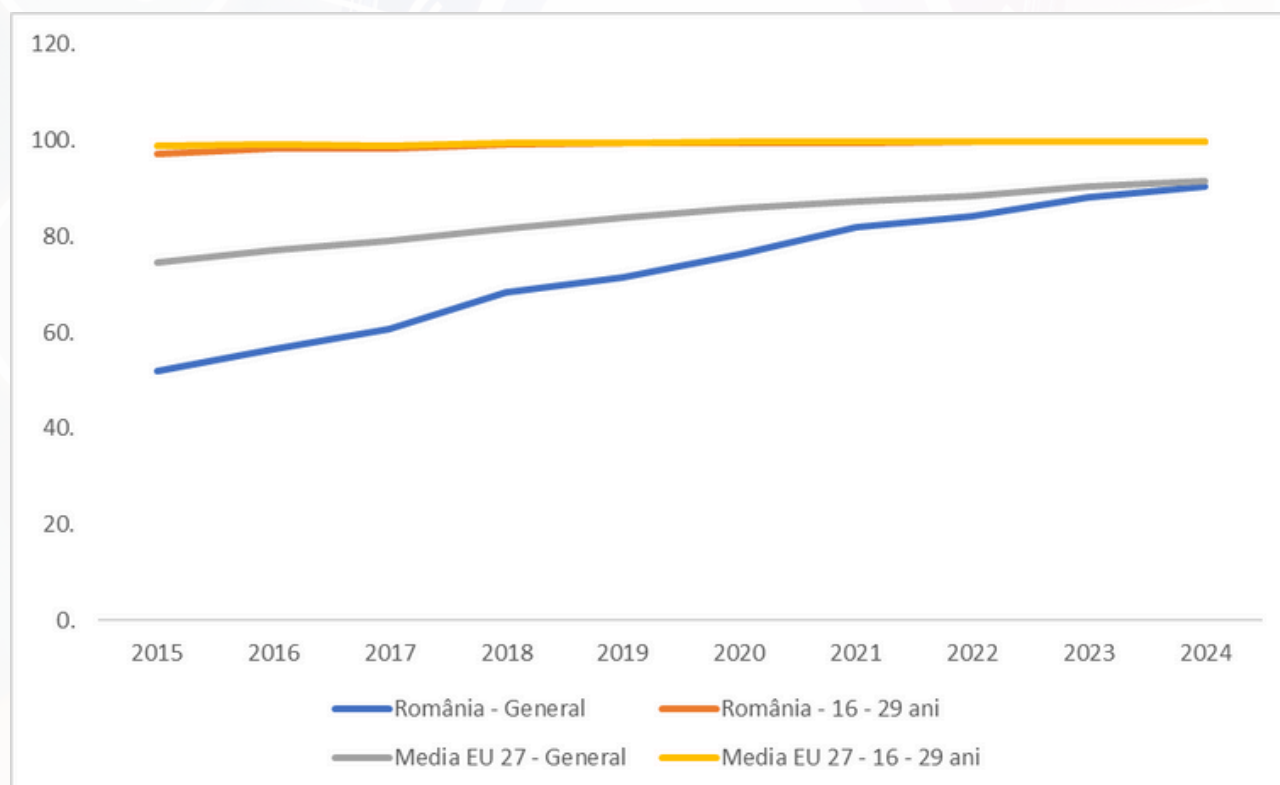


Sursa: Eurostat 2024

Știm foarte bine că atunci când vorbim de competențe digitale, vârsta este un factor determinant. Un segment important al populației, persoanele vârstnice, rămân adesea în urmă din punct de vedere tehnologic. Diferențele dintre generații în ceea ce privește utilizarea tehnologiei au condus la un decalaj digital tot mai accentuat. Mulți vârstnici întâmpină dificultăți în utilizarea dispozitivelor moderne, cum ar fi smartphone-urile, tabletele sau calculatoarele. Accesarea serviciilor online, cum ar fi plățile bancare, programările medicale sau comunicarea prin e-mail și rețele sociale, poate părea complicată și uneori intimidantă. Lipsa unei educații digitale formale în timpul vieții active, dar și teama de a greși sau de a fi victima unei fraude cibernetice, contribuie la această reticență.

În anul 2024, 88% din populația totală a UE și 97% dintre persoanele cu vârste între 16 și 29 de ani din UE au declarat că folosesc internetul zilnic. În anul 2015, 65% din populația totală a UE și 89% dintre tinerii de 16-29 de ani utilizau internetul zilnic, iar această proporție a crescut constant în această perioadă pentru toate grupele de vârstă (vezi Figura 2.3). Totuși, nu în același ritm: diferența dintre generații s-a redus constant în ultimul deceniu (vezi Figura 2.4). În 2024, în toate țările UE, această proporție era cuprinsă între 93% și 100%.

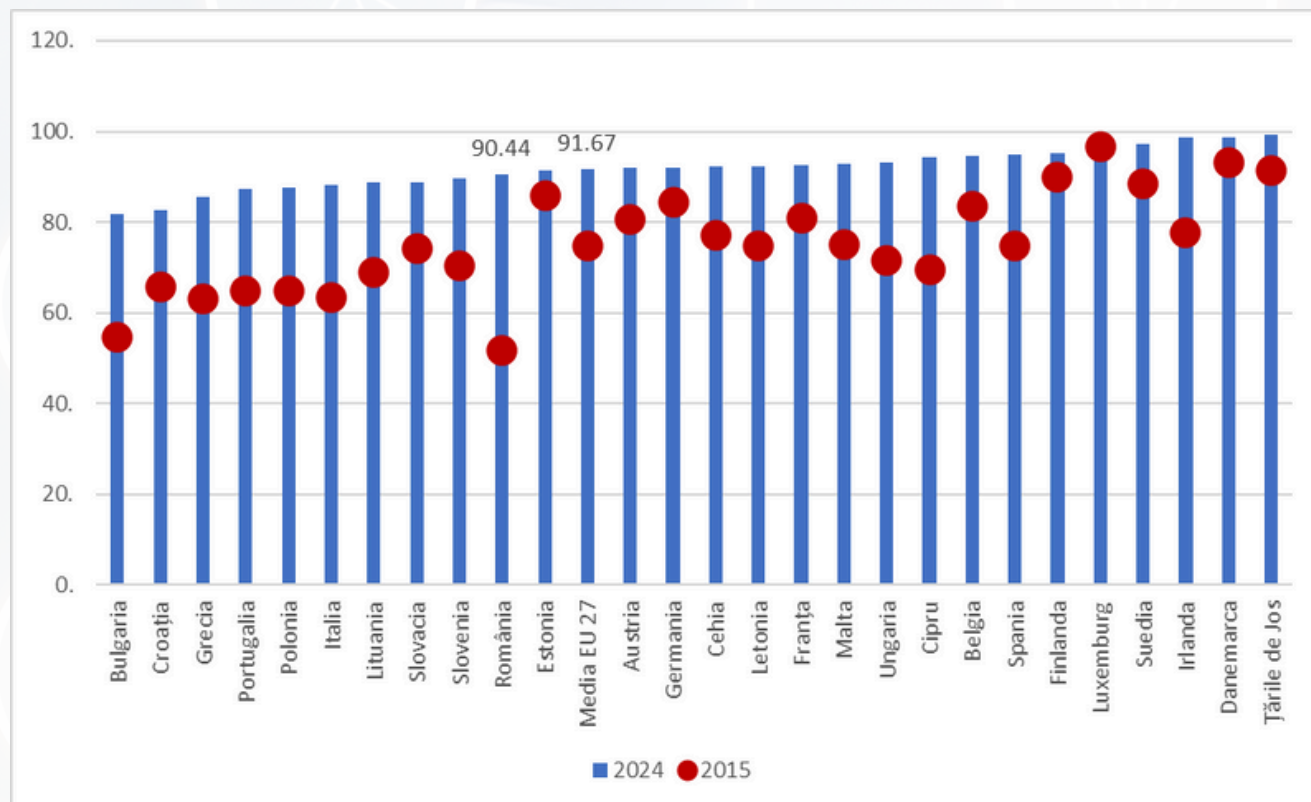
**Figura 2.3. Utilizarea zilnică a internetului în UE și România comparativ 2015 - 2024
(% din total populație)**



Sursa: Eurostat 2024

Cu toate că populația tânără a avut acces la internet în România comparativ cu media UE, totuși nivelul de alfabetizare digitală este unul relativ scăzut în comparație cu multe dintre statele membre UE (Tabel 2.2).

**Figura 2.3. Utilizarea zilnică a internetului în UE și România comparativ 2015 - 2024
(% din total populație)**



Sursa: Eurostat 2024

Competențe digitale mai scăzute au fost înregistrate în rândul grupelor de vârstă mai înaintate, atât în rândul bărbaților, cât și al femeilor. De exemplu, în grupa de vârstă 65-74 de ani, procentul bărbaților cu cel puțin competențe digitale de bază este mai mic de jumătate comparativ cu cei cu vârste între 25-34 de ani (69% față de 34%). Contrastul între femeile din diferite grupe de vârstă a fost și mai pronunțat: 71% dintre femeile cu vârste între 25-34 de ani dețineau cel puțin competențe digitale de bază, comparativ cu doar 25% dintre cele cu vârste între 65-74 de ani.

Tabel 2.2. Nivelul de competențe digitale generale de bază pe grupe de vârstă în EU27 (medie) și România pe nivel educațional (% din total populație)

	EU 27 Medie	Romania
General	55,56	27,73
Bărbați, 16–24 de ani	67,93	48,53
Femei, 16–24 de ani	72,16	45,56
Bărbați, 16–74 de ani	56,69	29,06
Femei, 16–74 de ani	54,46	26,47
Bărbați, 25–34 de ani	69,29	43,27
Femei, 25–34 de ani	71,07	36,92
Bărbați, 35–44 de ani	64,25	33,48
Femei, 35–44 de ani	66,28	34,75
Bărbați, 45–54 de ani	58,2	27,47
Femei, 45–54 de ani	57,31	28,05
Bărbați, 55–64 de ani	46,5	14,57
Femei, 55–64 de ani	42,24	15,32
Bărbați, 65–74 de ani	33,81	7,3
Femei, 65–74 de ani	23,33	5,34

Sursa: Eurostat 2024

În grupele de vârstă 16–24, 25–34 și 35–44 de ani, mai multe femei dețineau cel puțin competențe digitale de bază comparativ cu bărbații din aceleași categorii de vârstă. În rândul persoanelor de 45 de ani sau mai în vârstă, situația a fost inversă, iar proporțiile au fost mai mari în rândul bărbaților – diferența de gen crescând odată cu înaintarea în vârstă.

3. Necesitatea educației digitale în rândul tinerilor

3.1. Educația financiară digitală

Educația financiară digitală reprezintă un set de cunoștințe și competențe esențiale care permit indivizilor să înțeleagă, să utilizeze și să gestioneze eficient instrumentele financiare și serviciile disponibile în mediul digital. În contextul digitalizării accelerate a serviciilor financiare, abilitatea de a naviga în siguranță și cu încredere în lumea finanțelor online a devenit o necesitate pentru toți utilizatorii.



Această formă de educație nu se referă doar la cunoașterea conceptelor financiare tradiționale, precum economisirea, investițiile sau bugetarea, ci și la dobândirea competențelor digitale necesare pentru a utiliza aplicații financiare, platforme bancare online, portofele digitale și alte tehnologii emergente precum criptomonedele.

Un aspect crucial al educației financiare digitale este conștientizarea riscurilor asociate utilizării tehnologiei în domeniul financiar. Lipsa competențelor digitale adecvate poate expune utilizatorii la diverse fraude online, precum phishing-ul, furtul de identitate, tranzacții neautorizate sau scheme de înșelătorie care pot conduce la pierderi financiare semnificative. Fără o educație adecvată, oamenii pot fi vulnerabili la astfel de riscuri, care pot avea efecte devastatoare asupra situației lor financiare și personale.

Prin urmare, educația financiară digitală contribuie la creșterea gradului de siguranță și încredere în utilizarea serviciilor financiare online, facilitând accesul corect și protejat la resursele financiare digitale. Ea este esențială pentru incluziunea financiară și pentru capacitatea oamenilor de a participa activ și protejat în economia digitală modernă. Dezvoltarea acestor competențe sprijină nu doar gestionarea responsabilă a finanțelor personale, ci și prevenirea riscurilor și a fraudelor, asigurând astfel o experiență digitală sigură și benefică pentru utilizatori.

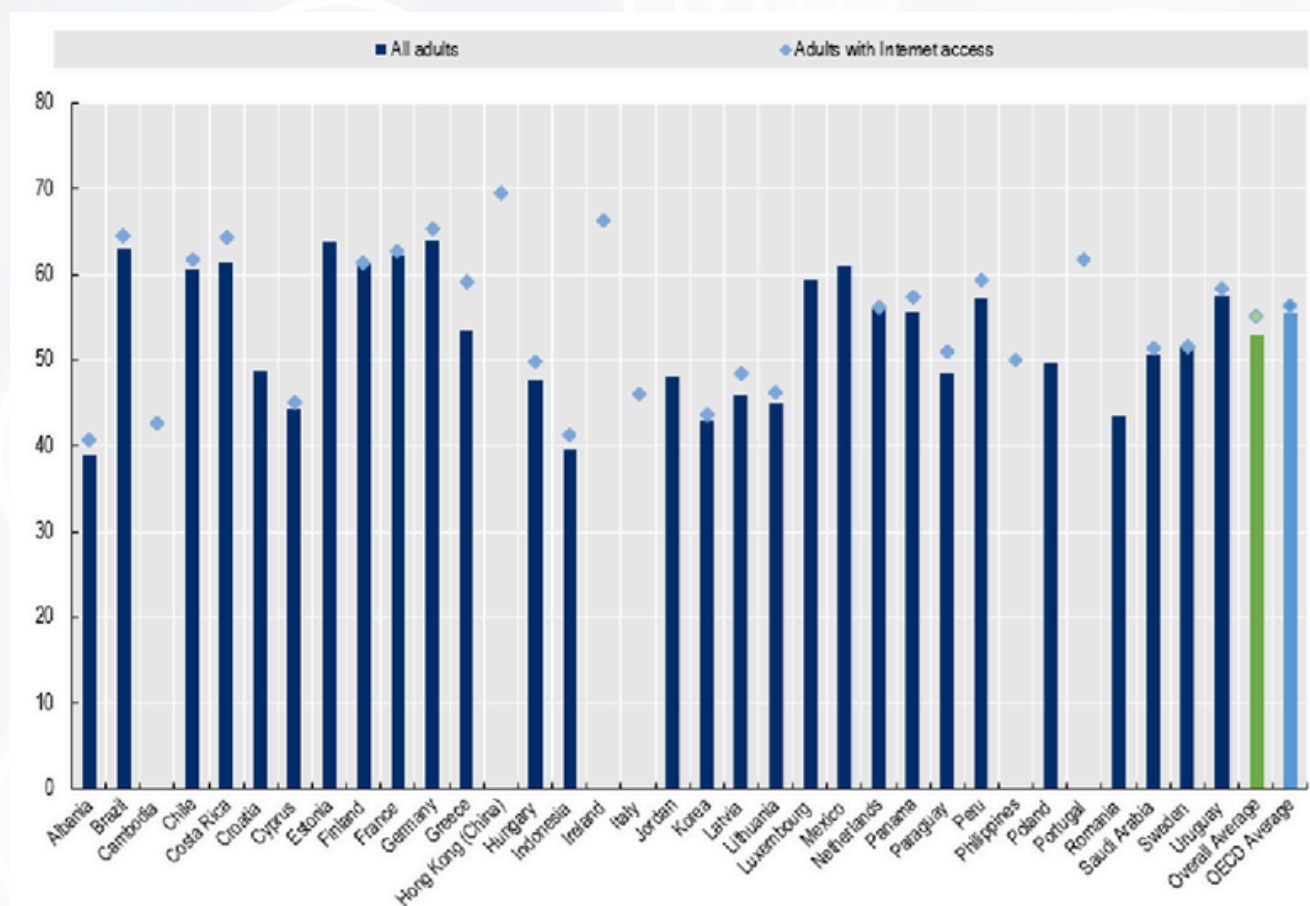
Într-un raport recent publicat de OECD, (OECD/INFE 2023 International Survey Of Adult Financial Literacy[5]), a fost realizat un sondaj cu întrebări menite să exploreze măsura în care indivizii folosesc serviciile financiare digitale și să evalueze nivelul lor de educație financiară digitală. Conform raportului, determinarea nivelului de educație financiară digitală în rândul populației din UE s-a bazat, în general, pe trei componente: **cunoștințe, comportament și atitudini**.

- Componenta de cunoștințe a scorului de educație financiară digitală este calculată pe baza numărului de răspunsuri corecte la trei întrebări care evaluează înțelegerea contractelor digitale, utilizarea datelor personale și a cripto-activelor.
- Componenta de comportament a scorului de educație financiară digitală este calculată ca numărul de comportamente digitale „avizate” identificate prin patru afirmații.
- Componenta de atitudini este calculată ca numărul de atitudini „avizate” legate de finanțele digitale, identificate prin trei afirmații.

Prin urmare, conform metodologiei OECD, scorul de educație financiară digitală reprezintă suma componentelor de cunoștințe digitale (3), comportamente (4) și atitudini (3). Scorurile brute variază între 0 și 10, iar scorul final este rescalat pentru a avea o valoare între 0 și 100. Un scor mai mare reflectă un nivel mai ridicat de educație financiară digitală. În medie, în toate țările și economiile participante, scorul de educație financiară digitală al populației adulte este de 53 din 100 (55 din 100 în țările membre OECD participante) – Figura 3.1.

Se poate observa că în România se înregistrează un scor mult mai redus decât în majoritatea statelor OECD, acest lucru arătând clar necesitatea ca în țara noastră să fie implementate politici publice de creștere a alfabetizării digitale și de conștientizare a riscurilor la care este supusă populația în utilizarea produselor financiare în mediul online.

Figura 3.1. Nivelul de educație financiară digitală în OECD



Sursa: Eurostat 2024

Pentru a respecta principiul „a nu face rău”, este esențial ca populația generală să dețină competențele și cunoștințele necesare pentru a reduce riscurile asociate utilizării tehnologiei. În absența unor demersuri eficiente de dezvoltare a alfabetizării digitale, pot apărea riscuri semnificative, inclusiv, dar fără a se limita la:



Dezinformare, care constă în răspândirea deliberată de informații false cu scopul de a induce în eroare și de a provoca daune unor persoane sau comunități.



Informațiile false (misinformation), acestea fiind informații incorecte răspândite fără intenția de a face rău, adesea din lipsă de cunoaștere sau din dorința de a ajuta, dar care pot avea consecințe negative. În practică, diferența dintre dezinformare și informații false poate fi greu de identificat. Înțelegerea intenției autorului și a modului în care circulă informația este esențială pentru alegerea unui răspuns adecvat. De exemplu, un zvon fals răspândit accidental în mediul online are nevoie de o abordare diferită față de o campanie coordonată de manipulare.



Riscurile informaționale — un termen umbrelă utilizat în cadrul sistemului ONU — includ toate aceste forme de comunicare dăunătoare și acoperă și riscurile emergente apărute în contextul progreselor rapide în domeniul inteligenței artificiale.



Abuzul datelor personale – distribuirea necontrolată a informațiilor personale online poate duce la furt de identitate sau fraude financiare.



Obiceiuri digitale nesănătoase – consumul excesiv de conținut digital poate duce la dependență, afectând sănătatea mintală și capacitatea de luare a deciziilor raționale, inclusiv în gestionarea banilor.



Excluderea digitală – lipsa accesului la tehnologie sau la competențe digitale de bază poate duce la pierderea oportunităților economice sau educaționale.



Cyberbullying și hărțuire online – persoanele pot fi atacate sau discriminate în spațiul digital, ceea ce afectează încrederea în platformele online, inclusiv cele financiare.



Tactici de manipulare sau recrutare – unele persoane pot fi vizate pentru trafic, exploatare sexuală sau alte forme de violență, inclusiv prin promisiuni financiare false.



Recrutare în scopuri ilegale – radicalizarea sau implicarea în activități ilegale prin platforme online, inclusiv în rețele de fraudă.



Înșelătorii și fraude financiare – scheme de tip scam sau promisiuni false privind locuri de muncă, investiții sau ajutoare financiare pot duce la pierderi materiale semnificative.



Supraveghere și monitorizare – activitatea online a utilizatorilor poate fi urmărită de terți (ex. entități comerciale sau guvernamentale), cu riscuri de securitate și confidențialitate.

3.2. Integrarea alfabetizării digitale în educația tinerilor și studenților

Pe măsură ce strategiile digitale sunt adoptate tot mai mult la nivelul societății, atingerea obiectivelor acestor inițiative riscă să fie compromisă în absența unor progrese concrete în domeniul alfabetizării digitale în rândul populației. Alfabetizarea digitală reprezintă o condiție esențială pentru orice intervenție care implică utilizarea tehnologiei (Gutierrez-Angel et al, 2022).

Prin urmare, pașii recomandați pentru dezvoltarea și implementarea inițiativelor digitale — în special etapele de definire a cadrului general și de stabilire a domeniului de aplicare — ar trebui să includă în mod central preocuparea pentru creșterea competențelor digitale ale tinerilor și studenților. Fără această componentă, intervențiile digitale riscă să fie ineficiente, inechitabile sau chiar să genereze efecte negative.

Pentru a reuși acest lucru este necesară o abordare în 3 piloni:

1. Incluziune digitală - Deși incluziunea digitală poate aduce beneficii semnificative la nivel individual și comunitar, un obstacol major în adoptarea și utilizarea eficientă a tehnologiei este lipsa competențelor digitale de bază și a alfabetizării digitale. Fără aceste abilități, există riscul ca indivizii să rămână simpli consumatori pasivi ai tehnologiei, în loc să devină utilizatori activi și creatori de conținut digital într-o societate conectată.

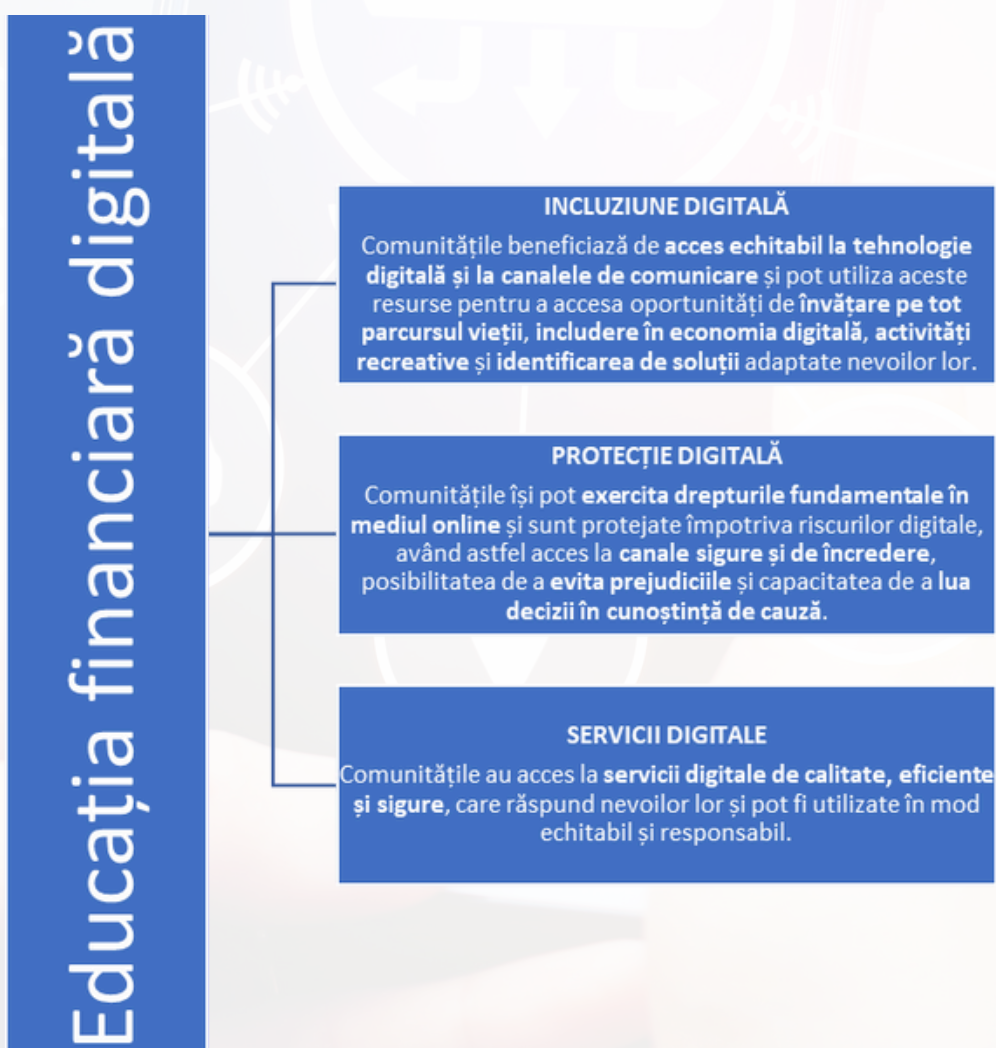
2. Protecție digitală - Alfabetizarea digitală, înțelegerea modului în care funcționează datele și capacitatea de a naviga în siguranță în mediile digitale sunt elemente esențiale pentru protejarea utilizatorilor în spațiul online. Este important ca oamenii să învețe:

- cum să folosească tehnologia în mod eficient și responsabil;
- cum să ia decizii informate cu privire la modul în care se conectează și interacționează cu conținutul digital;
- cum să recunoască și să gestioneze riscurile precum dezinformarea, discursul instigator la ură, hărțuirea online sau tentativele de fraudă;
- când și cum să raporteze comportamentele abuzive din mediul online.

3. Servicii digitale - Odată cu digitalizarea accelerată a serviciilor în multiple domenii precum plățile electronice, gestionarea identității, feedback și reclamații, ocuparea forței de muncă sau incluziunea economică este crucial ca toate categoriile de populație să aibă acces echitabil și sigur la aceste servicii, indiferent de vârstă, gen, nivel de educație sau alte caracteristici personale.

Pentru a asigura o transformare digitală echitabilă și sustenabilă, nu este suficient să fie oferite doar acces la dispozitive, conexiune la internet și platforme digitale. Este esențial să investim și în dezvoltarea competențelor digitale, astfel încât utilizatorii să fie pregătiți să se orienteze, să participe activ și să se protejeze în spațiul digital, inclusiv în ceea ce privește instrumentele de educație și gestionare financiară.

Figura 3.2. Componentele educației financiare digitale

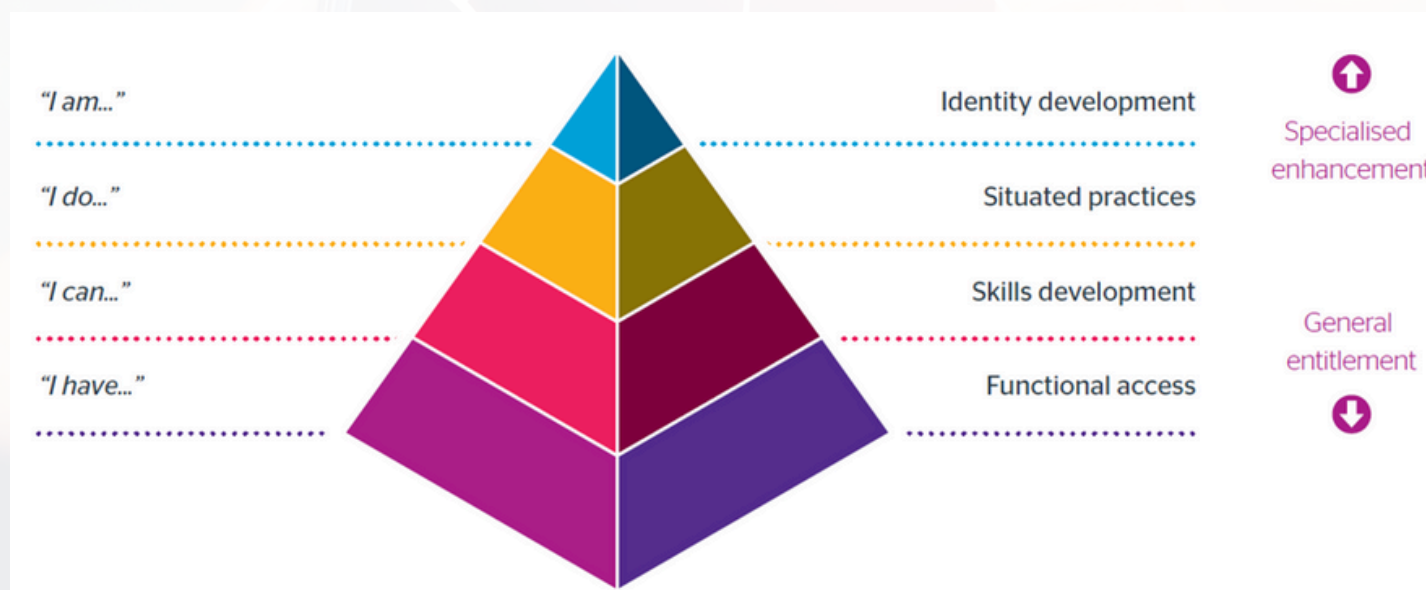


3.3. Dezvoltarea competențelor digitale ale elevilor / studenților

Alfabetizarea digitală este un concept amplu și holistic, care înseamnă mult mai mult decât simple competențe tehnice sau IT funcționale necesare pentru a face față într-o societate digitalizată. Deși mulți studenți sunt utilizatori experimentați ai tehnologiei, ei nu intră, de regulă, în învățământul superior cu toate competențele digitale necesare pentru a reuși în mediul academic și, ulterior, în viața profesională.

Această realitate subliniază rolul cheie pe care sistemul de învățământ superior trebuie să îl joace în sprijinirea dezvoltării unor competențe digitale diferențiate, specializate și avansate, care depășesc nivelul de bază pe care mulți studenți îl consideră un drept implicit. Asemenea celorlalte forme de alfabetizare, competențele digitale se dezvoltă progresiv, prin sprijin și practică constantă. Modelul propus de Beetham și Sharpe (2010) prezentat în Figura 3.3 evidențiază cum acest proces de dezvoltare trece de la acces și abilități funcționale către capacități de nivel înalt, precum gândirea critică digitală, responsabilitatea în mediul online sau crearea de conținut.

Figura 3.3. Procesul de dezvoltare trece de la acces și abilități funcționale către capacități de nivel înalt în domeniul educației digitale



Sursa: Beetham și Sharpe (2010)

Un aspect esențial al acestui model este că alfabetizarea digitală variază în funcție de context – indivizii sunt motivați să-și dezvolte noi abilități și comportamente digitale în funcție de situațiile și cerințele specifice în care se află.

Integrarea educației financiare digitale în curriculumul universitar este importantă și, prin urmare, universitățile sunt locurile ideale pentru a introduce, exersa și consolida practici digitale corecte și responsabile, inclusiv în domeniul educației financiare. Activitățile autentice integrate în conținutul disciplinelor oferă exemple concrete și relevante despre modul în care competențele digitale pot fi aplicate în contexte profesionale sau personale, în special pentru gestionarea responsabilă a resurselor financiare.

Este esențial ca sprijinul acordat studenților în acest proces să fie adaptat contextului lor academic și nevoilor specifice, întrucât o abordare universală nu este suficientă. De asemenea, dialogul între cadre didactice, studenți și parteneri din domeniul financiar-bancar este important pentru a defini în mod clar ce înseamnă alfabetizarea digitală și financiară în fiecare domeniu de studiu. Acest tip de colaborare poate contribui la formarea unei viziuni comune asupra modului în care competențele digitale, inclusiv cele legate de utilizarea responsabilă a tehnologiei în gestionarea informațiilor financiare, pot fi dezvoltate, susținute și evaluate pe parcursul formării universitare.

3.4. Rolul familiei, instituțiilor de învățământ și a mediului financiar-bancar în formarea competențelor financiare digitale în rândul tinerilor

Formarea competențelor financiare digitale în rândul tinerilor este un proces de lungă durată și există mai mulți actori ce trebuie să fie implicați pentru ca acest segment de populație să câștige abilitățile necesare: familia, instituțiile de învățământ și entitățile din domeniul financiar – bancar.

1. Familia

Familia, părinții sau persoanele care au grijă de copii/tineri au un rol esențial în a cultiva educația financiară și a modela abilitățile digitale în rândul acestora. Furnham et al (2024)[6] arată că, până la vârsta de șapte ani, copiii își formează deja primele obiceiuri legate de bani, ceea ce evidențiază rolul major al părinților în conturarea acestor deprinderi timpurii. Dezvoltarea capacității părinților de a discuta deschis și de a-și ghida copiii în privința aspectelor financiare creează o bază solidă pentru formarea unor adulți responsabili și încrezători în gestionarea resurselor proprii.

Importanța începerii educației financiare de la o vârstă fragedă are în vedere creșterea nivelului de alfabetizare financiară și digitală. Concentrarea pe anii timpurii urmărește să formeze o generație capabilă să își administreze corect finanțele, să înțeleagă modul în care serviciile financiare pot fi accesate online și să fie capabilă să detecteze posibile fraude financiare. Pregătirea părinților pentru a transmite obiceiuri financiare sănătoase și abilități digitale este un pas decisiv către dezvoltarea unui comportament financiar responsabil pe termen lung.

Totuși pentru a putea crea competențe financiare digitale solide în rândul copiilor/tinerilor, trebuie ca adulții să aibă încredere în propriile abilități de administrare a finanțelor personale, mai ales cei din medii socio-economice vulnerabile. De aceea, sprijinirea părinților este crucială, întrucât discuțiile despre bani în familie sporesc încrederea copiilor în propriile competențe financiare, dar și competențe digitale. Totodată, este important de recunoscut că unii părinți se simt nesiguri sau nepregătiți să abordeze aceste subiecte, iar depășirea acestei bariere este necesară nu doar pentru educația individuală, ci și pentru reducerea inegalităților economice. Din acest motiv considerăm că rezultatele acestui studiu și ghidurile ce se vor realiza sunt un bun punct de plecare pentru ca adulții să fie mai bine pregătiți în transmiterea unor informații relevante copiilor lor.

Mai mult, tinerii gestionează deja sume de bani sau obțin venituri proprii, rolul părinților de ghizi în educația financiară devenind și mai vizibil. Prin urmare, gestionarea veniturilor și cheltuielilor, realizarea bugetului personal, investițiile realizate prin intermediul aplicațiilor online puse la dispoziție de brokeri, utilizarea serviciilor bancare online sunt abilități pe care tinerii ar trebui să le deprindă mai ales prin relația cu membrii familiei. În acest sens, cele mai importante acțiuni trebuie să aibă în vedere:

- Încurajarea părinților și îngrijitorilor să inițieze și să întrețină discuții despre bani cu copiii lor, folosind resursele existente și canalele de comunicare disponibile, pentru a întări lecțiile despre educația financiară în mediul online și în mediul familial;
- Susținerea proceselor de învățare de acasă, prin ghiduri practice (ce vor fi parte a rezultatului acestui studiu) oferind părinților instrumentele și materialele necesare pentru a prezenta conceptele financiare într-un mod eficient.

2. Instituțiile de învățământ

Instituțiile de învățământ au un rol esențial în dezvoltarea competențelor financiare ale tinerilor (Johnson și Sherraden, 2007), prin transmiterea conținuturilor educaționale și cultivarea dorinței de învățare pe tot parcursul vieții. Perfecționarea pregătirii cadrelor didactice și accesul sporit la resurse educaționale în domeniul educației financiare, cât și a celei digitale le oferă profesorilor instrumentele necesare pentru predarea unor abilități fundamentale, precum înțelegerea modului în care funcționează mediul online și a gestionării banilor personali.

Prin adaptarea noțiunilor financiare complexe în lecții accesibile, profesorii răspund diversității nevoilor elevilor și transformă educația financiară într-un sprijin practic pentru viața adultă. Creșterea competențelor cadrelor didactice în domeniul alfabetizării financiare permite realizarea unor conținuturi care fac legătura între teoria predată la clasă și deciziile financiare reale, sporind încrederea și capacitatea de decizie a elevilor. Dotarea profesorilor cu instrumente moderne și oferirea de oportunități de formare continuă contribuie la dezvoltarea unei culturi a responsabilității financiare, ce include familiile și comunitatea largă, sprijinind astfel prosperitatea economică a generațiilor viitoare.

Strategia Națională de Educație Financiară 2024-2030 a României vine cu un set de acțiuni concrete în care instituțiile de învățământ, dar și alți actori din piață ar trebui să se implice, acțiuni ce au în vedere OS1, Dezvoltarea și introducerea elementelor de educație financiară în curriculumul național la toate nivelurile de învățământ, OS2. Realizarea de acțiuni de educație financiară complementare, adresate învățământului preuniversitar și universitar, OS3. Introducerea educației financiare în universități, OS4. Promovarea unor comportamente financiar responsabile în rândul copiilor, tinerilor prin intermediul mass-media și al canalelor de comunicare social media, OS5. Implementarea unor programe de educație financiară destinate cadrelor didactice din învățământul preuniversitar și universitar, OS6. Implementarea unui program național de conștientizare, consiliere și sprijin pentru părinți în vederea educării copiilor din perspectivă financiară. Astfel, învățământul are un rol crucial în dezvoltarea abilităților financiare digitale în rândul tinerilor.

Conform analizei realizate în baza Raportului OECD/INFE 2023 International Survey Of Adult Financial Literacy [7], cele mai importante măsuri ale instituțiilor de învățământ trebuie să aibă în vedere:

- Dezvoltarea programelor de formare a cadrelor didactice, care să includă atât activități de perfecționare profesională continuă (CPD), cât și cursuri specializate dedicate predării educației financiare și produselor financiare disponibile online.
- Creșterea gradului de conștientizare privind resursele și inițiativele existente în diverse sectoare, astfel încât profesorii să fie bine informați și să utilizeze eficient materialele necesare pentru consolidarea competențelor financiare digitale.

Mediul financiar-bancar

Instituțiile financiar-bancare au o acoperire excelentă în rândul populației locale, dispun de datele necesare pentru a fundamenta decizii și utilizează tehnologii avansate, capabile să proceseze volume mari de analize pentru a genera impact. Pentru a valorifica aceste atuuri, instituțiile financiar-bancare trebuie să:

- Organizeze datele – să le facă accesibile în timp real, permanent, și suficient de bine structurate pentru a oferi o imagine clară asupra comportamentului fiecărui client.
- Ofere servicii relevante – să pună la dispoziție, într-o manieră simplă și intuitivă, funcționalități de gestionare financiară precum bugete, rapoarte, prognoze de cashflow sau obiective de economisire.
- Furnizeze informații personalizate – să își sprijine clienții prin analize adaptate comportamentului lor financiar, să le explice consecințele anumitor decizii și să recomande, la momentul oportun, produsele financiare care le pot aduce beneficii reale.

Serviciile financiare digitale pot reprezenta un factor esențial pentru creșterea incluziunii financiare, în special în România, unde majoritatea populației are acces mai ușor la un telefon mobil decât la o bancă. Incluziunea financiară, în sensul său deplin, înseamnă accesul și utilizarea unor produse și servicii financiare de calitate, la prețuri accesibile, care contribuie la bunăstarea financiară a individului.

Având în vedere cele menționate anterior, cele mai importante măsuri ale instituțiilor financiar-bancare trebuie să aibă în vedere:

- Dezvoltarea de aplicații digitale ușor de utilizat, cu componentă educațională care să sprijine utilizatorul în a lua cele mai bune decizii pentru finanțele personale.
- Un nivel ridicat de siguranță pentru serviciile financiare oferite online, care să protejeze utilizatorul de posibile fraude ce pot apărea.

Un obstacol major în atingerea incluziunii financiare îl reprezintă nivelul redus de alfabetizare digitală și financiară pe care îl are România. Pe măsură ce produsele și serviciile financiare sunt livrate tot mai mult în format digital, competențele în ambele domenii devin esențiale. Implementarea unor inițiative eficiente de creștere a nivelului de alfabetizare ar putea îmbunătăți considerabil protecția consumatorilor și sănătatea financiară, în special în rândul grupurilor defavorizate. Totuși, proiectarea și aplicarea unor programe de alfabetizare digitală și financiară de succes reprezintă un proces complex. Colaborarea dintre sectorul public și cel privat, împreună cu societatea civilă, este esențială pentru elaborarea conținutului educațional, definirea strategiilor de atingere a utilizatorilor finali și evaluarea programelor-pilot între toți actorii menționați în acest subcapitol.

4. Fraudele financiare online – o perspectivă generală

4.1. Definirea și clasificarea fraudelor financiare online

Fraudele financiare online reprezintă un ansamblu de acțiuni intenționate și premeditate de inducere în eroare, concepute și executate prin utilizarea tehnologiilor informatice, a infrastructurilor digitale și a rețelelor de comunicații electronice, având ca finalitate obținerea unui folos patrimonial necuvenit sau provocarea unei pierderi materiale unei persoane fizice ori juridice. Acest tip de infracțiune se distinge prin caracterul său hibrid, îmbinând metode de natură tehnică — cum ar fi exploatarea vulnerabilităților software și hardware, interceptarea neautorizată a datelor sau manipularea fluxurilor informaționale — cu tehnici de inginerie socială, menite să exploateze încrederea, neatenția sau lipsa de pregătire a utilizatorilor.

De regulă, fraudă financiară online presupune interacțiunea dintre mai multe elemente esențiale:

1. Vectorul tehnologic – rețelele publice sau private de comunicații (internet, rețele mobile), sistemele informatice (serve, platforme de e-commerce, aplicații bancare) și dispozitivele terminale (PC, smartphone, tablete).
2. Obiectul economic – fonduri bănești, active digitale, date financiare sensibile (numere de card, coduri PIN, parole, date de autentificare multi-factor) și instrumente de plată fără numerar.
3. Modul de acțiune – tehnici precum phishing, malware financiar, compromiterea conturilor online, manipularea tranzacțiilor electronice sau falsificarea datelor informatice, preluarea controlului device-urilor.

Specificul fraudelor financiare online constă în dematerializarea mediului infracțional: autorul nu mai acționează într-un spațiu fizic delimitat, ci într-un ecosistem virtual, adesea distribuit la nivel global, ceea ce complică identificarea și urmărirea penală. În plus, natura transfrontalieră a acestor infracțiuni face ca legislațiile naționale să fie uneori insuficient armonizate, iar cooperarea internațională devine un element central în prevenire și combatere.

În plan juridic, aceste fapte se circumscriu atât sferei criminalității informatice, cât și celei a infracțiunilor economico-financiare, fiind reglementate prin acte normative interne (Codul Penal al României, Legea nr. 161/2003) și prin instrumente legislative europene și internaționale (Directiva (UE) 2013/40, Directiva (UE) 2019/713, Convenția de la Budapesta privind criminalitatea informatică). Impactul lor este dublu: pe de o parte, afectează direct patrimoniul victimelor prin pierderi financiare imediate; pe de altă parte, erodează încrederea publicului în mediul digital și în infrastructurile financiare electronice, generând efecte negative pe termen lung asupra stabilității economice și securității cibernetice.

Clasificarea fraudelor financiare online poate fi abordată sistematic prin luarea în considerare a unei game diverse de criterii, fiecare surprinzând aspecte distincte ale fenomenului - inclusiv fațete tehnice, economice, juridice și operaționale. Această analiză ajută la înțelegerea complexităților inerente infracțiunilor financiare online.

La nivel național, diverse organisme de reglementare și de aplicare a legii, cum ar fi Banca Națională a României (BNR), Direcția Națională de Securitate Cibernetică (DNSC) și Inspectoratul General al Poliției Române, au elaborat scheme de clasificare care pun accentul în principal pe trei dimensiuni critice: modus operandi, natura țintei și canalele tehnologice utilizate. Modus operandi se referă la tehnicile și tacticile utilizate de făptași, în timp ce tipul de țintă poate include categorii precum consumatori individuali, întreprinderi sau instituții financiare.

În plus, canalele tehnologice cuprind diverse medii, inclusiv e-mail, aplicații mobile, platforme web și rețele de socializare. Aceste tipologii operaționale joacă un rol crucial în facilitarea investigațiilor penale și a activităților de monitorizare, deoarece stabilesc repere clare care permit autorităților să identifice prompt tendințele emergente și vulnerabilitățile sistemice din cadrul ecosistemului financiar.

La o scară europeană mai largă, instituții precum Europol, Autoritatea Bancară Europeană (ABE) și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) pledează pentru sisteme de clasificare armonizate. Aceste sisteme sunt concepute pentru a aborda caracteristicile transnaționale ale infracțiunilor financiare online și pentru a ține cont de interacțiunea dintre criminalitatea cibernetică și criminalitatea financiară tradițională. Clasificările europene cuprind nu doar elemente tehnice și economice, ci și factori critici, cum ar fi nivelul de sofisticare al atacului. Aceasta include evaluarea complexității tacticilor utilizate, a obiectivelor finale ale actorilor infracționali - cum ar fi achiziționarea directă de fonduri, monetizarea datelor furate sau facilitarea spălării banilor - și evaluarea impactului potențial asupra stabilității piețelor financiare în statele membre.

O analiză comparativă relevă faptul că tipologiile naționale tind să fie mai pragmatice și strâns aliniate cu realitățile locale, concentrându-se pe amenințările predominante specifice unui anumit mediu socio-economic. În schimb, tipologiile europene adoptă o perspectivă mai largă, care încorporează scenarii și fenomene complexe cu dimensiuni geopolitice semnificative.

Integrarea acestor două perspective distincte, dar complementare, într-un cadru analitic unificat nu numai că sporește acuratețea clasificării fraudelor financiare online, dar consolidează și cooperarea transfrontalieră în combaterea acestor infracțiuni. Prin armonizarea eforturilor și partajarea informațiilor, națiunile se pot pregăti mai bine pentru a aborda natura din ce în ce mai sofisticată a fraudei financiare online și provocările reprezentate de operațiunile sale transnaționale.



După metoda de comitere (criteriu tehnic)

- **Phishing** – transmiterea de e-mailuri sau mesaje înșelătoare, aparent provenite de la bănci sau platforme de plăți, cu scopul colectării datelor bancare.
- **Vishing și smishing** – obținerea de informații confidențiale prin apeluri telefonice sau mesaje SMS frauduloase.
- **Pharming** – redirectionarea utilizatorilor către site-uri false prin compromiterea serverelor DNS.
- **Malware financiar** – troieni bancari, keyloggere, ransomware cu componentă de furt de date financiare.
- **Compromiterea e-mailului de afaceri (Business Email Compromise – BEC)** – interceptarea și falsificarea corespondenței comerciale pentru deturnarea plăților.

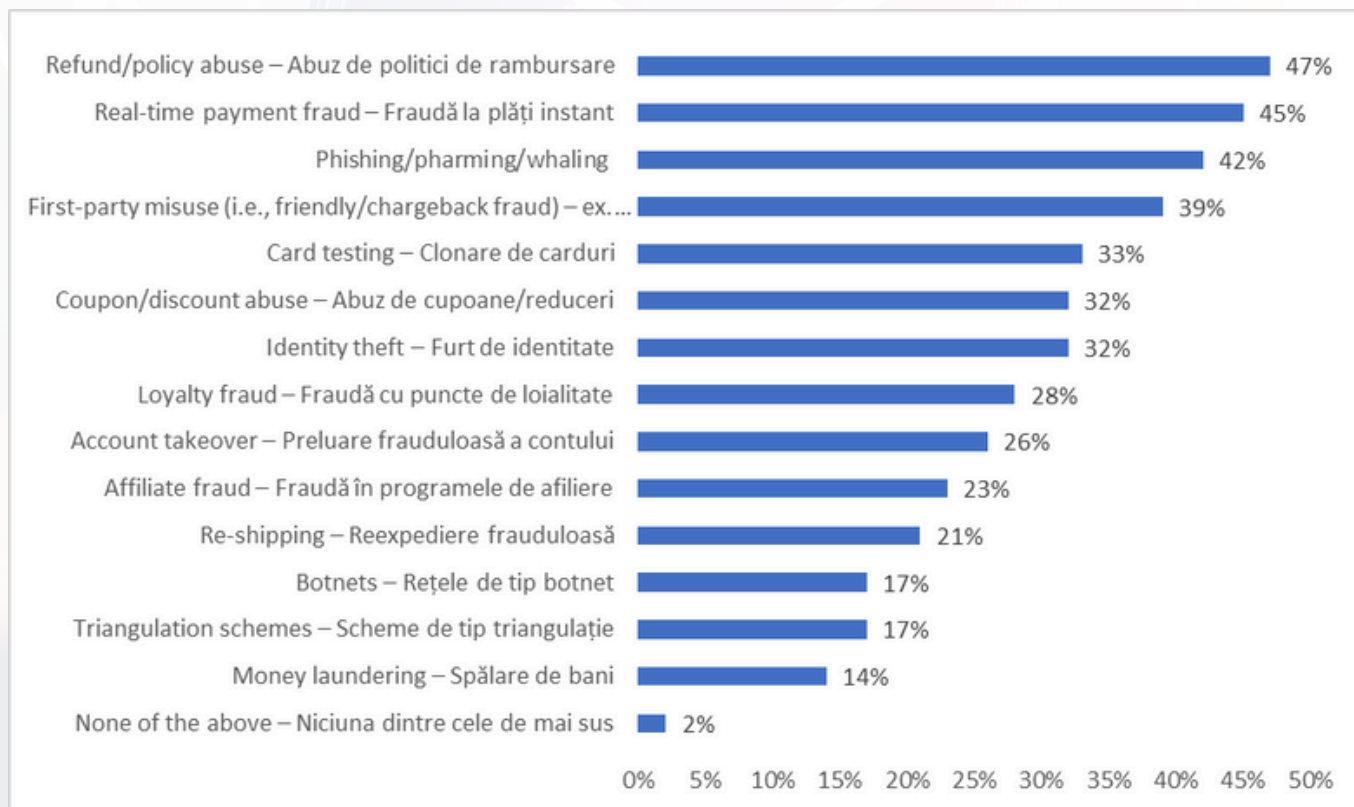
După scopul urmărit

- **Obținere directă de fonduri** – transferuri neautorizate din conturile victimei
- **Obținere indirectă de fonduri** – revânzarea datelor financiare pe piețe ilegale
- **Facilitarea spălării banilor** – tranzacții succesive prin platforme fintech sau criptomonede

După categoria victimei

- **Fraude B2B** – atacuri asupra infrastructurii de plăți și facturare ale companiilor.
- **Fraude B2C** – înșelarea consumatorilor prin platforme false de comerț online
- **Fraude C2C** – anunțuri înșelătoare pe platforme de tip marketplace

Figura 4.1. Cele mai comune tipuri de fraudă în anul 2024



Sursa: Statista 2024

4.1.1 Tipologii recunoscute în România și la nivel european

Fraudele financiare online reprezintă un ansamblu de acțiuni intenționate și premeditate de inducere în eroare, concepute și executate prin utilizarea tehnologiilor informatice, a infrastructurilor digitale și a rețelelor de comunicații electronice, având ca finalitate obținerea unui folos patrimonial necuvenit sau provocarea unei pierderi materiale unei persoane fizice ori juridice. Acest tip de infracțiune se distinge prin caracterul său hibrid, îmbinând metode de natură tehnică — cum ar fi exploatarea vulnerabilităților software și hardware, interceptarea neautorizată a datelor sau manipularea fluxurilor informaționale — cu tehnici de inginerie socială, menite să exploateze încrederea, neatenția sau lipsa de pregătire a utilizatorilor.

La nivel național (România)

Conform rapoartelor Directoratului Național de Securitate Cibernetică (DNSC), Băncii Naționale a României (BNR) și Poliției Române, tipologiile frecvente includ:

- **Phishing bancar personalizat** – imitarea paginilor web ale băncilor românești.
- **Fraude cu investiții online** – oferte false în criptomonede sau acțiuni, promovate prin reclame agresive.
- **Fraude cu plăți avansate** – solicitarea de sume pentru „deblocarea” unor câștiguri inexistente.
- **Fraude în comerțul electronic** – vânzători inexistenți sau bunuri fictive.
- **Compromiterea conturilor de utilizator** pe platforme de plăți și retragerea neautorizată de fonduri.

La nivel european

Potrivit Europol – Internet Organised Crime Threat Assessment (IOCTA) și European Banking Authority (EBA), tipologiile dominante sunt:

- **Social engineering avansat** – atacuri complexe combinând phishing, vishing și deepfake audio/video.
- **Fraude cu carduri și date de plată** – clonarea cardurilor și tranzacții frauduloase transfrontaliere.
- **Abuzul de sisteme de plăți instant** – exploatarea transferurilor rapide SEPA Instant.
- **Fraude cu criptomonede** – scheme Ponzi, „rug pull” și platforme false de exchange.
- **Fraude în sistemele B2B internaționale** – deturnarea facturilor și falsificarea instrucțiunilor de plată.

4.2. Evoluția fenomenului de fraudă în era digitală

Progresul accelerat al tehnologiei informației, alături de expansiunea utilizării internetului la nivel global, a condus la o transformare profundă a sectorului financiar, facilitând apariția unor practici inovatoare care au redefinit modalitățile prin care sunt efectuate tranzacțiile și gestionate resursele financiare. Digitalizarea serviciilor bancare, automatizarea proceselor financiare și dezvoltarea platformelor online au sporit accesibilitatea și eficiența operațiunilor economice, oferind utilizatorilor soluții rapide și convenabile. Totuși, această revoluție tehnologică a introdus și provocări semnificative, deschizând noi oportunități pentru infractorii cibernetici și favorizând apariția unor forme sofisticate și greu de detectat de criminalitate informatică, precum fraudele digitale, atacurile cibernetice, compromiterea datelor și spălarea banilor prin canale online.

Frauda financiară online reprezintă un aspect semnificativ al criminalității informatice contemporane, cuprinzând diverse activități ilicite menite să obțină câștiguri financiare prin mijloace înșelătoare în domeniul digital. Aceste activități includ, dar nu se limitează la accesul neautorizat la conturile bancare, schemele de phishing, manipularea plăților online, clonarea cardurilor și utilizarea identităților false pentru tranzacții.

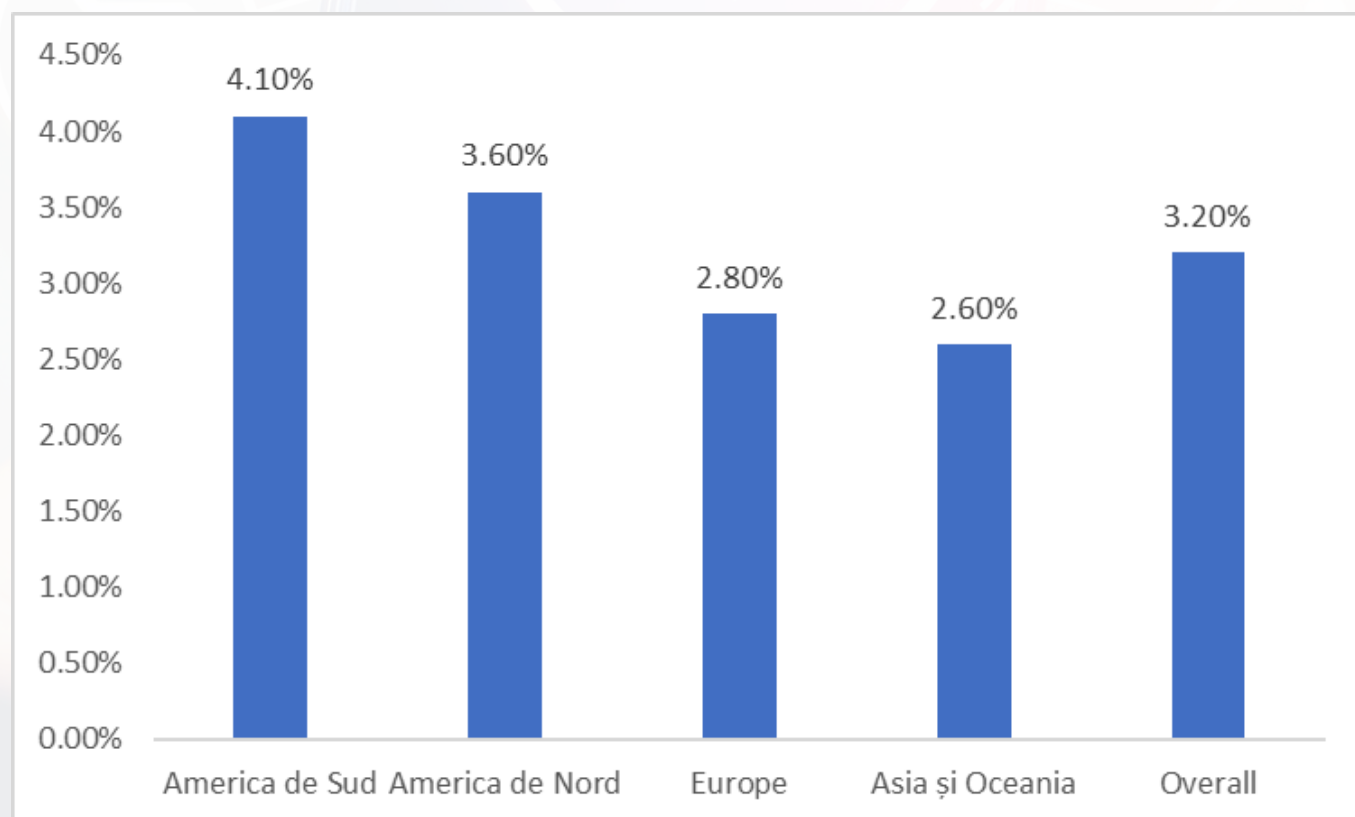
Fenomenul fraudei a cunoscut o transformare radicală odată cu tranziția societății către era digitală. Dacă, în trecut, fraudă se manifesta preponderent în mediul fizic, prin falsuri materiale, înșelăciuni directe sau manipularea documentelor tipărite:

- **Clonarea cardurilor bancare** – utilizată pentru accesarea conturilor bancare.
- **Fraude prin modem și linii telefonice** – interceptarea comunicațiilor sau obținerea de acces gratuit la rețele private („phreaking”).
- **Manipularea fișierelor contabile** pe sisteme informatice izolate - revoluția tehnologică din ultimele decenii a generat **un nou ecosistem infracțional** caracterizat prin dematerializarea mijloacelor, globalizarea spațiului de acțiune și creșterea exponențială a vitezei de execuție:
- **Spear-phishing și whaling** – atacuri direcționate asupra persoanelor-cheie din organizații.
- **Deepfake** – utilizarea de imagini și voci sintetizate pentru a convinge victimele să efectueze transferuri.

- **Fraude cu criptomonede, investiții prin achiziționare de acțiuni** – scheme Ponzi, phishing pe portofele digitale.
- **Fraude prin aplicații mobile false** – care imită aplicațiile bancare oficiale.
- **Exploatarea plăților instant** (SEPA Instant) pentru transferuri rapide și greu reversibile.

Odată cu digitalizarea rapidă a economiei și adoptarea pe scară largă a serviciilor financiare electronice, acest tip de fraudă a cunoscut o creștere notabilă atât în frecvență, cât și în sofisticare. Factorii care contribuie includ mobilitatea sporită a utilizatorilor, lipsa alfabetizării digitale, anonimatul oferit de internet și reglementările uniforme insuficiente la nivel internațional. În plus, progresele tehnologice continuă să faciliteze aceste activități frauduloase cu pierderi majore pentru comercianți și persoane fizice (Figura 4.2).

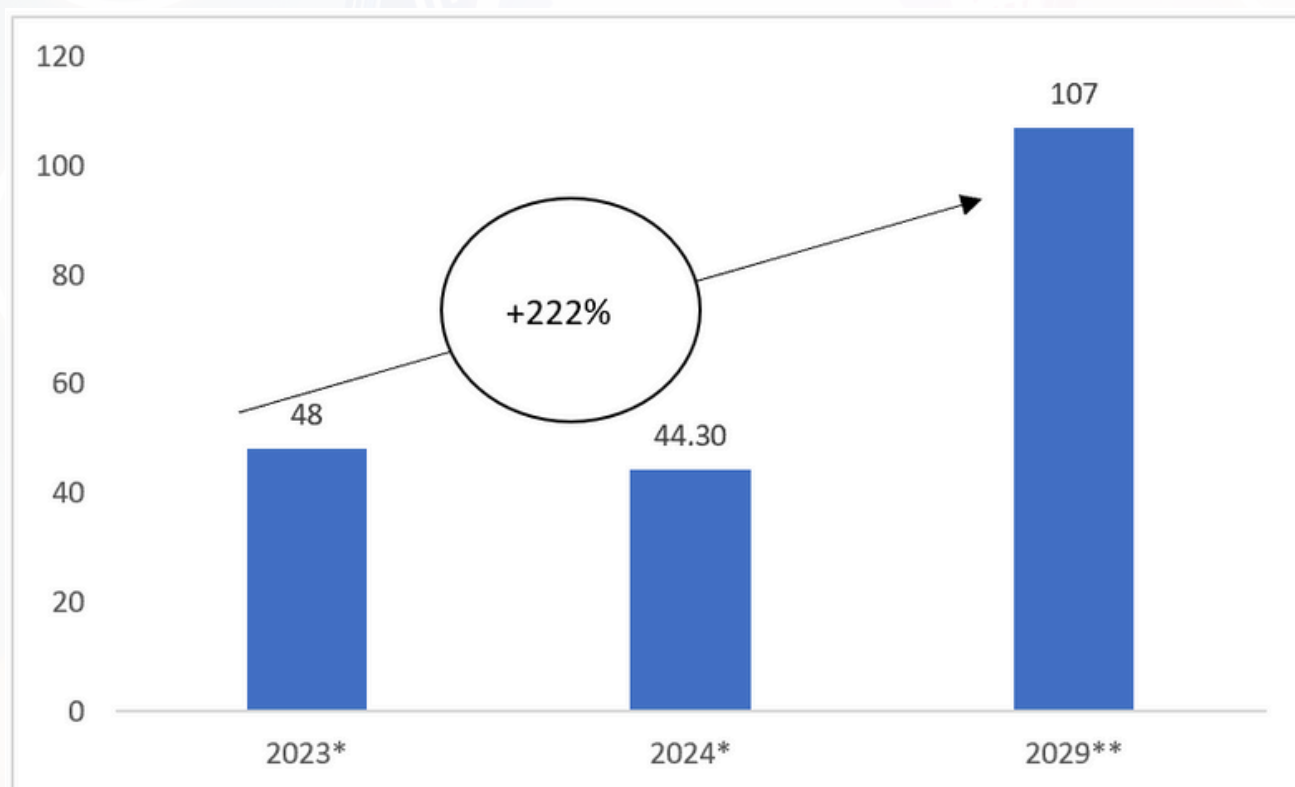
Figura 4.2. Procentul pierdut din veniturile generate de comerțul electronic din cauza fraudelor online



Sursa: Visa Acceptance Solutions; Merchant Risk Council; Verifi; B2B International

În plus, progresele tehnologice oferă infractorilor instrumente din ce în ce mai sofisticate, cum ar fi inteligența artificială, cryptocurrencies și dark web, ceea ce complică procesele de detectare și prevenție. În acest context, fraudă online a evoluat nu numai într-o problemă economică (ce va genera pierderi majore și în viitor - a se vedea Figura 4.3), ci și într-o provocare socială și instituțională, subliniind necesitatea unor măsuri coerente în materie de prevenire, reglementare și cooperare transfrontalieră.

Figura 4.3. Valoarea pierderilor din comerțul electronic cauzate de fraudă la plăți online la nivel mondial (miliarde USD)



Sursa: Juniper Research 2025

4.3. Instrumente și tehnici folosite de infractorii cibernetici

În peisajul digital de astăzi, fraudă cibernetică a evoluat într-un fenomen complex care transcende incidente izolate, acum susținute de infrastructuri criminale globale extinse. Aceste rețele sunt sofisticate și specializate, folosind o serie de instrumente tehnice și strategii psihologice pentru a-și desfășura activitățile ilicite. Infractorii cibernetici combină cu pricepere exploatarea vulnerabilităților tehnologice - cum ar fi slăbiciunile software-ului, parolele inadecvate și rețelele nesigure - cu tehnici avansate de inginerie socială. Această abordare duală le permite să manipuleze comportamentul uman, convingând indivizii să dezvăluie informații sensibile sau să ia măsuri care le compromit securitatea. În plus, acești infractori sunt extrem de adaptivi, modificându-și în mod constant metodele ca răspuns la progresele tehnologice și la schimbările în comportamentul utilizatorilor, făcând din ce în ce mai mult detectarea și prevenirea.

Înțelegerea acestor forme diferite de fraudă cibernetică este esențială pentru dezvoltarea unor contra-măsuri eficiente și pentru îmbunătățirea poziției de securitate a persoanelor și organizațiilor.

4.3.1. Phishing

Phishing-ul reprezintă o formă de fraudă informatică bazată pe transmiterea de comunicări electronice (e-mail, SMS, mesaje în aplicații) care imită surse legitime, cu scopul obținerii de date sensibile (parole, coduri PIN, date card bancar, informații personale). În esență, acest tip de atac combină ingineria socială cu exploatarea tehnologică pentru a compromite securitatea datelor financiare ale victimei.

Indiferent de scenariul folosit, atacurile de tip phishing urmează de regulă aceeași structură:

- Crearea identității false – imitarea identității unei bănci sau instituții financiare;
- Transmiterea mesajului fraudulos – prin canale electronice;
- Inducerea stării de urgență sau frică – pentru a stimula acțiunea rapidă și necriticată;
- Redirecționarea victimei către un mediu controlat de atacator – site clonat sau formular fals;
- Colectarea datelor – stocarea credențialelor în baze de date ilicite;
- Exploatarea datelor – tranzacții frauduloase, vânzarea pe dark web, contractarea de credite.

Scenarii concrete

A. Transmiterea de link-uri în numele băncii pentru actualizarea datelor bancare

Tehnici și instrumente utilizate

- E-mail spoofing: falsificarea antetului mesajului pentru a părea trimis de instituția bancară legitimă;
- Kits phishing: pachete software ce conțin pagini web clonă și scripturi pentru colectarea datelor;
- Hosting anonim: servere plasate în jurisdicții cu legislație permissivă;
- SSL/TLS fals: certificate obținute de atacatori pentru a simula conexiuni securizate („https”).
- Mecanism psihologic: utilizarea unui pretext administrativ („actualizarea obligatorie a datelor”) care invocă conformitatea cu procedurile băncii.



B. Mesaj de informare privind efectuarea unei plăți cu cardul victimei și necesitatea confirmării

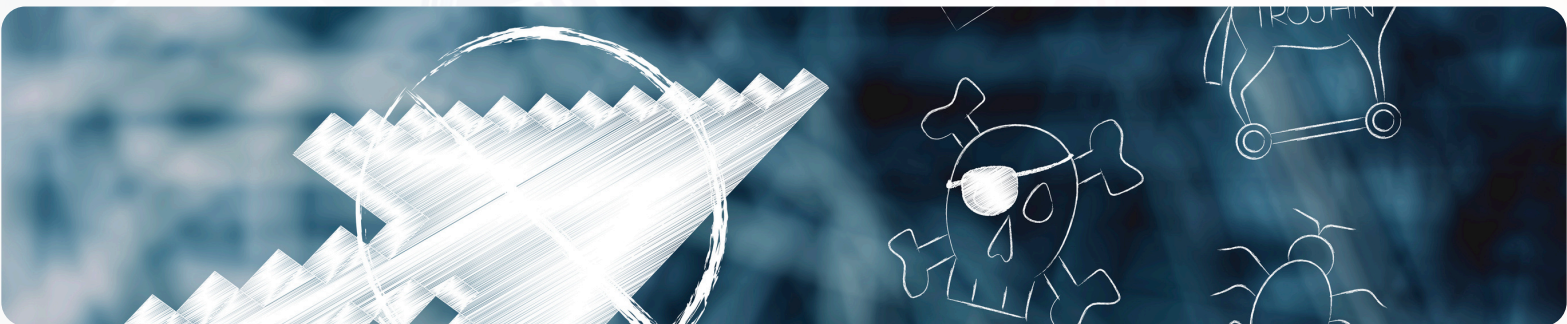
Tehnici și instrumente utilizate

- Trigger emoțional de panică: formulări precum „Tranzacție suspectă detectată”;
- Mesaje SMS (smishing): trimiterea de link-uri scurte către pagini de phishing optimizate pentru mobil;
- Interfețe mobile simulate: pagini ce imită exact aplicațiile bancare oficiale;
- Servere de redirectionare: pentru ascunderea sursei reale a atacului.
- Mecanism psihologic: crearea unui sentiment de urgență care determină victima să acționeze imediat, fără verificări suplimentare.

C. Mesaj privind contractarea unui credit în numele victimei și solicitarea confirmării datelor

Tehnici și instrumente utilizate

- Scenariu de fraudă cu identitate furată: invocarea riscului imediat de îndatorare neautorizată;
- Canale multiple de contact: e-mail, telefon (vishing) pentru validarea falsei urgențe;
- Formulare interactive frauduloase: câmpuri de completat ce solicită CNP, date de card, coduri de securitate;
- Integrarea cu baze de date furate: pentru a personaliza mesajul cu numele real al victimei, sporind credibilitatea.
- Mecanism psihologic: exploatarea fricii de prejudiciu financiar pe termen lung și presiunea de a „stopa” un proces ilegal în desfășurare.



Infrastructura folosită

În toate scenariile, instrumentele tehnice au elemente comune:

- Domenii web similare (typosquatting, ex. „banck-romania.ro”);
- Certificate SSL ieftine sau gratuite pentru crearea iluziei de securitate;
- Servere proxy și VPN-uri pentru anonimizarea locației atacatorului;
- Baze de date cu informații compromise achiziționate din dark web.

4.3.2 Investment Scam

Frauda de tip *Investment Scam* reprezintă o schemă frauduloasă prin care victimele sunt determinate să investească sume de bani în așa-zise oportunități financiare, prezentate ca fiind extrem de profitabile și cu risc scăzut sau inexistent. În realitate, aceste investiții sunt fictive, iar scopul final este transferul fondurilor către conturi controlate de infractori. Caracterul modern al acestor fraude constă în combinarea **publicității agresive pe platforme online cu manipularea directă a dispozitivelor victimei** prin instrumente tehnice de control de la distanță.

Frauda de tip Investment Scam demonstrează o integrare sofisticată între tehnologiile de marketing online, instrumentele de control la distanță și exploatarea directă a infrastructurii bancare personale a victimei. Abordarea tehnico-psihologică hibridă crește considerabil rata de succes a atacurilor.

Etapile tipice se caracterizează prin:

A. Identificarea și atragerea victimei

- **Reclame sponsorizate pe rețele sociale** (Facebook, Instagram, LinkedIn, TikTok), optimizate prin tehnici de microtargeting pentru a ajunge la persoane cu interes potențial în investiții.
- **Paginile de aterizare (landing pages)** care imită platforme legitime de trading sau portaluri financiare cunoscute.
- **Testimoniale false** (texte, fotografii sau videoclipuri cu „investitori mulțumiți”) pentru crearea unei aparențe de credibilitate.

B. Contactul direct cu victima

- **Apeluri telefonice inițiate de operatori frauduloși** (așa-numiții boiler room agents), care urmează un script prestabilit pentru a câștiga încrederea victimei.
- **Spoofing de număr** – tehnică prin care numărul afișat pe telefon pare a fi cel al unei instituții legitime.
- **Persuasiune prin tehnici de influențare psihologică** (autoritate, reciprocitate, urgență) – fraudatorii se prezintă drept „consultanți financiari” sau „specialiști în piețe de capital”.

C. Solicitarea instalării aplicațiilor de control la distanță

- **Reclame sponsorizate pe rețele sociale** (Facebook, Instagram, LinkedIn, TikTok), optimizate prin tehnici de microtargeting pentru a ajunge la persoane cu interes potențial în investiții.
- **Paginile de aterizare (landing pages)** care imită platforme legitime de trading sau portaluri financiare cunoscute.
- **Testimoniale false** (texte, fotografii sau videoclipuri cu „investitori mulțumiți”) pentru crearea unei aparențe de credibilitate.

D. Preluarea controlului asupra aplicației de Mobile Banking

Interacțiune directă cu aplicația băncii, în timp ce victima este prezentă, sub pretextul „alimentării contului de investiții”.

- **Capturarea codurilor OTP** primite prin SMS sau aplicații de autentificare, datorită accesului în timp real la telefon.
- **Transferuri imediate** către conturi de tip „mule account” (conturi bancare deschise pe numele unor terți, folosite pentru spălarea banilor).

Mecanisme psihologice exploatare

- **Lăcomia** – promisiunea unor câștiguri rapide și semnificative;
- **Frica de a pierde oportunitatea** (fear of missing out – FOMO);
- **Autoritatea** – prezentarea fraudatorului ca expert sau reprezentant al unei instituții prestigioase;
- **Reciprocitatea** – oferirea de „informații privilegiate” în schimbul unei acțiuni imediate.

Infrastructura utilizată

- **Servere de găzduire offshore** – pentru site-urile de promovare și platformele false;
- **Servicii VoIP internaționale** – pentru apeluri cu identificador fals;
- **Rețele de conturi bancare intermediare** – pentru dispersarea rapidă a fondurilor;
- **Platforme de conversie crypto** – pentru transformarea sumelor în criptomonede greu de urmărit.

4.3.3 Spoofing

În domeniul criminalității informatice, *spoofing*-ul desemnează tehnica prin care un atacator falsifică informațiile de identificare ale unei surse de comunicare (număr de telefon, adresă de e-mail, IP) pentru a se prezenta ca o entitate legitimă și de încredere. În contextul financiar, *caller ID spoofing* este folosit pentru a afișa pe telefonul victimei un număr real aparținând unei bănci, unei instituții financiare sau unei autorități publice, cu scopul de a obține acces la date sensibile ori de a determina victima să efectueze tranzacții financiare.

A. Obținerea și utilizarea tehnologiilor de falsificare a identității apelantului

- **Servicii VoIP cu funcție de schimbare a caller ID-ului** – multe operate din jurisdicții externe, cu reglementare redusă;
- **Platforme specializate în spoofing** (de ex. spoof card services) care permit introducerea manuală a numărului afișat;
- **SIM swap** – furtul numărului de telefon real al unei victime prin portare frauduloasă către alt operator (în cazuri mai complexe).

B. Impersonarea instituțiilor de încredere

Impersonarea Call Center-ului unei bănci

- falsificarea numărului oficial al băncii; atacatorul informează victima că datele bancare au fost compromise și solicită „validarea” acestora.
- scripturi verbale predefinite, în care sunt inserate detalii reale despre client (posibil obținute din baze de date scurse).

Impersonarea Băncii Naționale a României

- prezentarea apelului ca fiind efectuat din partea BNR, cu pretextul „protejării” victimei prin contractarea unui credit pe numele său.
- utilizarea unui nume real al unui salariat BNR și invocarea unor reglementări fictive pentru a spori credibilitatea.

Impersonarea Poliției

- apel cu număr oficial al unei secții de poliție, în care victima este informată că datele sale personale au fost furate. Se sugerează urgent contractarea unui credit, retragerea banilor și depunerea acestora într-un ATM Bitcoin „pentru securizare”.
- crearea unei presiuni psihologice intense prin invocarea unei anchete în desfășurare și a unui „termen limită” pentru acțiune.

Mecanisme psihologice exploatare

- Autoritatea – atacatorii se prezintă drept funcționari ai unor instituții puternice (bancă, BNR, poliție);
- Frica – amenințarea cu pierderi financiare iminente sau consecințe legale;
- Urgența – inducerea ideii că acțiunea trebuie efectuată imediat, fără verificări;
- Confuzia procedurală – utilizarea unui limbaj tehnic sau birocratic pentru a inhiba întrebările victimei.

Infrastructura tehnică utilizată

- Rețele VoIP anonimizate – cu servere în țări diferite de cele ale victimelor, pentru îngreunarea urmăririi;
- Sisteme de redirectionare a apelurilor pentru mascarea traseului real;
- Baze de date cu informații personale achiziționate din dark web, pentru personalizarea apelului;
- Rețele de ATM-uri Bitcoin folosite ca metodă finală de conversie și transfer a fondurilor, dat fiind caracterul pseudonim al tranzacțiilor crypto.

4.3.4 Deepfake

Frauda de tip *deepfake* reprezintă utilizarea tehnologiilor bazate pe **inteligență artificială generativă** (IA) și **rețele neuronale profunde** pentru a crea, modifica sau suprapune imagini, înregistrări audio ori video astfel încât acestea să pară autentice, deși sunt fabricate. În mediul financiar, deepfake-urile sunt exploatate pentru a induce în eroare investitori și consumatori prin falsificarea aparenței unor persoane publice, instituții sau branduri, cu scopul de a legitima oferte fictive de investiții și de a obține transferuri de bani.

1. Utilizarea imaginii unor persoane cunoscute (ex. politicieni, economiști, antreprenori de succes) pentru promovarea investițiilor

- generarea de videoclipuri sau imagini în care persoana respectivă „vorbește” și „recomandă” achiziția de acțiuni cu randament ridicat prin:
 - ✓ Platforme de *face-swapping* și *lip-syncing* bazate pe GAN (Generative Adversarial Networks) – ex. *DeepFaceLab*, *FaceSwap*.
 - ✓ Software de generare vocală (*voice cloning*) precum *ElevenLabs* sau *Respeecher*, pentru imitarea vocii persoanei.
- exploatarea reputației și credibilității unei figuri publice pentru a valida o schemă frauduloasă.

2. Utilizarea numelui unor instituții publice (ex. ministere, agenții de stat) pentru promovarea „vânzării de acțiuni”

- crearea de materiale video deepfake în care reprezentanți fictivi ai instituției (ori figuri reale falsificate) anunță o ofertă de acțiuni „cu acces limitat” prin:
 - ✓ Suprapunerea feței și vocii pe corpul unui actor care citește un script comercial fals.
 - ✓ Integrarea siglelor oficiale și a graficii instituționale autentice preluate de pe site-urile reale.

3. Crearea materialului deepfake

- **Colectarea datelor sursă:** imagini și înregistrări audio-video cu ținta (preluate din interviuri, rețele sociale, arhive media).
- **Antrenarea modelului AI:** folosirea unui set de date cu sute sau mii de cadre ale feței țintei pentru a antrena rețeaua neuronală.
- **Generarea materialului final:** combinarea feței și vocii falsificate cu un mesaj comercial sau investițional adaptat audienței-țintă.

4. Distribuirea materialului

- **Canale folosite:** platforme sociale (Facebook, Instagram, TikTok), site-uri de știri false, YouTube Ads sau reclame plătite în rețele de display.
- **Targetare:** folosirea algoritmilor de microtargetare pentru a afișa materialul către utilizatori cu profil financiar interesat (investitori, antreprenori).

5. Apelarea victimei

- **Call-to-action fals:** link către un site de tip phishing sau o platformă frauduloasă de investiții.
- **Escaladarea:** apel telefonic de la un „consilier de investiții” care finalizează tranzacția și solicită date bancare sau instalarea unei aplicații de control la distanță.

6. Instrumente și infrastructură tehnică utilizată

- **Software open-source de deepfake:** DeepFaceLab, FaceSwap, Avatarify.
- **Servicii comerciale de AI video editing (SaaS)** cu interfețe prietenoase, folosite fără cunoștințe tehnice avansate.
- **Voice cloning** – reconstituirea vocii din mostre de câteva secunde.
- **Site-uri frauduloase de investiții** – realizate cu șabloane predefinite, integrate cu procesatoare de plăți crypto sau conturi de transfer rapide.
- **Campanii de publicitate plătită** – pentru a amplifica vizibilitatea materialului deepfake și a-i conferi aparență de legitimitate.

7. Mecanisme psihologice exploatare

- **Efectul de autoritate:** folosirea figurilor publice pentru a conferi încredere schemei.
- **Aversiunea față de ratarea oportunității (FOMO):** promisiunea unor câștiguri rapide și „oferte limitate”.
- **Confirmarea socială:** prezentarea deepfake-ului ca parte dintr-o „campanie națională” sau „parteneriat cu statul”.
- **Iluzia profesionalismului:** folosirea unor elemente vizuale și sonore oficiale (sigle, decoruri instituționale, ton formal).

4.3.5 Online Shopping Platforms Fraud

Frauda de tip Online Shopping Platforms Fraud reprezintă totalitatea acțiunilor ilicite desfășurate prin intermediul platformelor de comerț electronic, site-urilor de anunțuri sau rețelelor de socializare, având ca scop inducerea în eroare a cumpărătorilor sau vânzătorilor în vederea obținerii de beneficii patrimoniale necuvenite. Acest tip de fraudă implică, de regulă, exploatarea încrederii în mecanismele de tranzacționare online, prin crearea unor scenarii aparent legitime de vânzare sau cumpărare.

Etapele tipice se caracterizează prin:

1. Anunțuri false de vânzare de bunuri – plata în avans, fără livrare

- Fraudatorul publică un anunț atractiv, cu un preț sub media pieței, pentru a stimula achiziția rapidă. După ce primește plata integrală sau un avans substanțial, dispare fără a expedia produsul. Cum:
 - ✓ Conturi false pe platforme consacrate (OLX, eMAG Marketplace, eBay).
 - ✓ Fotografii și descrieri copiate de la anunțuri legitime.
 - ✓ Adrese de e-mail temporare și numere de telefon virtuale (VoIP) pentru comunicare.

2. Postarea unui anunț real de către un vânzător, dar „cumpărătorul” solicită datele cardului sub pretextul livrării banilor

- infractorul pretinde că dorește să cumpere produsul, însă afirmă că plata se face printr-un „serviciu de livrare” al platformei, care ar necesita introducerea datelor cardului (număr, data expirării, CVV) pe un link transmis prin mesaj. În realitate, datele sunt folosite pentru fraudarea contului bancar. Cum:
 - ✓ Site-uri de phishing care imită perfect pagina oficială a platformei de comerț.
 - ✓ Link-uri scurtate sau mascate pentru a ascunde adresa reală a site-ului fraudulos.
 - ✓ Scripturi automatizate de captare a datelor introduse de victimă.

3. Confuzia intenționată între numărul de cont și datele cardului

- Victima este convinsă că, pentru a primi bani, trebuie să ofere date complete ale cardului, deși, în realitate, transferul bancar necesită doar IBAN-ul. Această tehnică exploatează necunoașterea procedurilor bancare de către utilizatorii obișnuiți. Cum:
 - ✓ Comunicarea directă prin platformă sau mesagerie instant (WhatsApp, Messenger).
 - ✓ Capturi de ecran false cu „interfața” băncii sau platformei, pentru a „dovedi” procedura.



4. Tehnici operaționale ale fraudatorilor

Inginerie socială

- Exploatarea urgenței („produsul are multe cereri”, „oferta este valabilă doar azi”) pentru a forța luarea unei decizii rapide.
- Crearea unui fals sentiment de legitimitate prin folosirea unui profil cu recenzii furate sau istoric fictiv de vânzări.
- Manipularea prin prezentarea de dovezi false (chitanțe falsificate, confirmări de plată inexistente).

Tehnici informatice

- Phishing avansat: pagini web clonă care trimit datele direct către serverul infractorului.
- Obfuscare URL: mascarea adresei reale prin domenii similare (typosquatting) sau folosirea serviciilor de scurtare a link-urilor.
- Anonimizare: folosirea de VPN-uri, servere proxy și numere virtuale pentru a evita identificarea.

Infrastructura și instrumentele utilizate

- Platforme de anunțuri clonate sau create special pentru fraudă.
- Servicii VoIP (Skype, Google Voice, TextNow) pentru a apela victimele din numere cu prefixe credibile.
- Servicii de e-mail temporar pentru crearea rapidă de conturi.
- Instrumente grafice (Photoshop, Canva) pentru falsificarea chitanțelor și capturilor de ecran.
- Rețele de conturi false pentru recenzii pozitive fictive, menite să crească încrederea.

Mecanisme psihologice exploatare

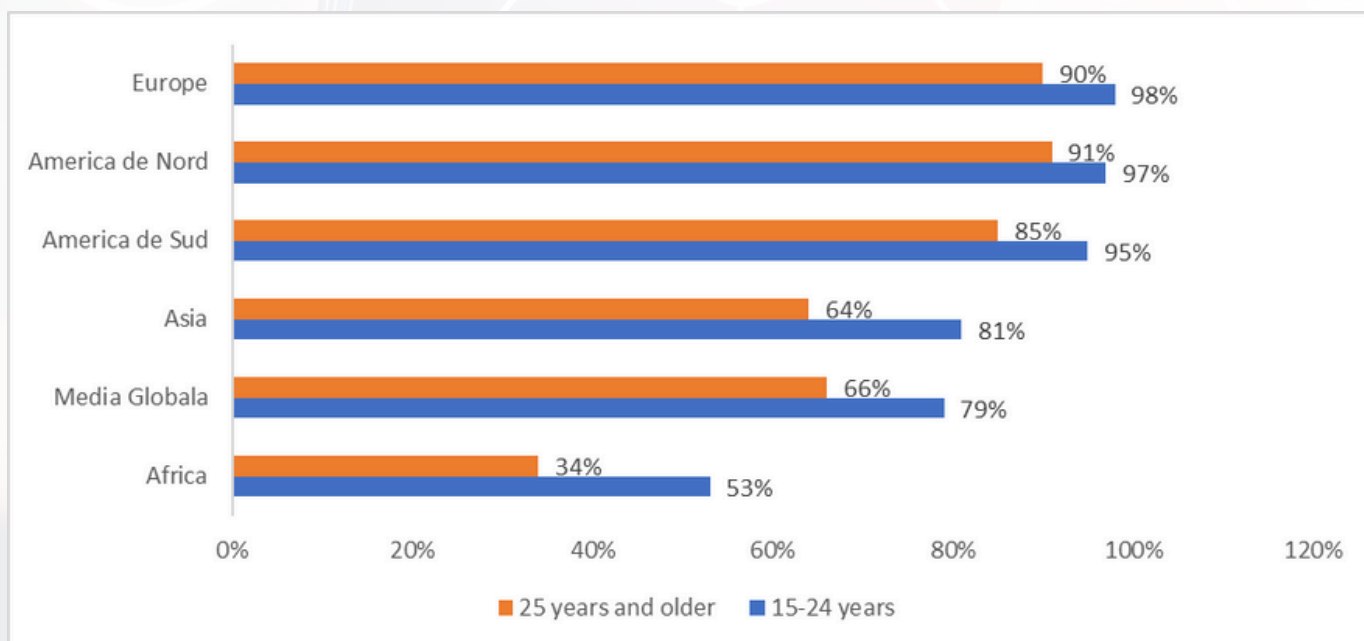
- Efectul de raritate: teama că oferta va fi pierdută determină acțiuni impulsive.
- Transferul de încredere: încrederea acordată platformei legitime este transferată, în mod eronat, către profilul fals.
- Presiunea socială: indicarea unor „alți cumpărători interesați” pentru a grăbi tranzacția.
- Confuzia procedurală: exploatarea necunoașterii diferenței dintre IBAN și datele cardului.

5. Vulnerabilitatea în fața fraudelor online a tinerilor

Interacțiunea tinerilor cu tehnologiile digitale încă de la vârste fragede este fundamental diferită de cea a generațiilor anterioare. Majoritatea tinerilor de astăzi nu au cunoscut o lume fără tehnologie digitală, iar acest lucru le influențează modul de comunicare, felul în care își formează prietenii, cum învață, cum se integrează în societate și chiar relația lor cu industria serviciilor financiare.

La nivel global, 79% dintre tineri sunt conectați la internet, comparativ cu 61% din populația generală (Figura 5.1). Importanța accesului la informații și servicii online a crescut atât de mult încât mai multe guverne naționale – precum cele din Costa Rica, Estonia, Finlanda, Franța, Grecia și Spania – au recunoscut oficial accesul la internet ca drept fundamental al omului (Burns & Gottschalk, 2019).

Figura 5.1. Ponderea utilizatorilor de internet (tineri vs restul populației) la nivel global și pe regiuni, în 2024



Sursa: Statista 2025

Această prezență omniprezentă a tehnologiei în viața tinerilor a dus la consacrarea termenului de „nativi digitali”. Noțiunea sugerează, în general, o abilitate naturală de a folosi în mod adecvat tehnologia și dispozitivele digitale care îi înconjoară. Totuși, cercetările recente avertizează că nu trebuie presupus automat că toți tinerii posedă competențe digitale reale. În paralel, s-a pus tot mai mult accent pe vulnerabilitățile asociate accesului nelimitat la mediul digital și pe recunoașterea faptului că există diviziuni digitale la mai multe niveluri: între țări, între regiuni, dar și între grupuri socio-economice din aceeași societate.

5.1. Factori care favorizează expunerea la fraude online

Există o expunere inegală a tinerilor la tehnologiile digitale și, în general, cei care sunt vulnerabili în viața de zi cu zi tind să fie mai vulnerabili și în online (Burns și Gottschalk, 2019). Există trei aspecte distincte care evidențiază acest lucru:

- **Accesul la internet:** Între cei care au acces la internet și cei care nu au există diferențe majore între țări, între mediile rurale și urbane sau între gospodăriile care aparțin unor medii socio-economice diferite. Acesta este primul și cel mai evident obstacol.
- **Utilizare și competențe:** Între modelele de utilizare și inegalitățile în competențele digitale: diferențele în utilizarea tehnologiilor și a internetului între tinerii avantajați și cei dezavantajați sunt semnificative, mai ales atunci când este luat în considerare modul în care elevii utilizează internetul și tehnologiile digitale. Tinerii avantajați au mai multe șanse să citească știrile și să folosească internetul pentru a obține informații practice decât colegii lor dezavantajați, care au mai multe șanse să-și petreacă timpul online jucând jocuri sau conversând. Astfel, chiar și atunci când accesul există, calitatea și utilitatea acestuia variază enorm.
- **Rezultate:** tinerii dezavantajați, mai puțin decât tinerii avantajați, utilizează internetul și tehnologiile digitale pentru a beneficia de servicii precum serviciile financiare sau platformele de căutare a locurilor de muncă, ceea ce are ca rezultat și reflectă inegalități în rezultatele offline. Aceste diferențe pot conduce la concluzia că disparitatea digitală se transformă în inegalitate socio-economică concretă.

Factorii precum mediul socio-economic și genul afectează inegalitățile digitale. Pentru tinerii vulnerabili, cum ar fi cei care trăiesc cu dizabilități, tehnologiile digitale și conectivitatea pot fie să agraveze vulnerabilitățile și excluziunea socială, fie să ofere oportunități de integrare. Potențialul de transformare este imens, însă în ce direcție înclină balanța depinde și de politicile și intervențiile deliberate pe care le implementăm.

Principalii factori care favorizează expunerea la fraudele online sunt: situația financiară personală și statutul de ocupare, gradul de alfabetizare financiară, percepția serviciilor financiare, infrastructura digitală și normele culturale, sociale sau religioase.

1. Situația financiară personală și statutul de ocupare influențează în mod semnificativ incluziunea financiară a tinerilor. Rata ridicată a șomajului în rândul tinerilor, precum și lipsa resurselor financiare, sunt frecvent menționate ca principale obstacole în accesul la servicii financiare. În unele contexte, șomajul tinerilor este perceput drept barieră majoră pentru economii de pensii sau alte produse financiare, iar lipsa unui venit stabil este unul dintre motivele principale pentru excluziunea financiară a tinerilor.

2. Nivelul scăzut de alfabetizare financiară reprezintă un factor important care contribuie la excluziunea financiară a tinerilor. Aceștia nu doar că au cunoștințe limitate despre finanțe, dar le lipsesc și competențele și conștientizarea privind serviciile și produsele financiare. Pentru a contracara această situație, factorii de decizie au implementat politici și programe de educație financiară, inclusiv în curricula școlară. Dovezile sugerează că astfel de inițiative conduc la o mai bună gestionare a creditelor, reducerea datoriilor și utilizarea unor metode de împrumut mai avantajoase.

3. Percepția tinerilor asupra necesității serviciilor financiare este influențată de mai mulți factori, inclusiv lipsa cunoștințelor și a resurselor financiare. Mulți tineri consideră că nu au nevoie de servicii financiare și nu le găsesc utile, ceea ce îi determină să nu acceseze produse precum conturi de economii, carduri de debit, împrumuturi sau asigurări. Această percepție redusă a necesității reprezintă un obstacol semnificativ în calea incluziunii financiare a tinerilor.

4. Lipsa accesului la infrastructură digitală limitează posibilitatea tinerilor de a fi incluși financiar în mediul digital. Pentru cei fără acces la internet sau la un telefon mobil, dezvoltarea unei infrastructuri digitale accesibile reprezintă o condiție esențială pentru promovarea incluziunii financiare digitale.

5. Normele culturale, sociale sau religioase, inclusiv controlul parental sau diferențele de gen, pot reprezenta un obstacol semnificativ pentru incluziunea financiară a tinerilor.

Diferențele de percepție digitală menționate anterior riscă să amplifice și mai mult inegalitățile dintre tineri în ceea ce privește accesul la învățarea digitală sau riscul de abandon școlar din educație și formare. Accesul tinerilor la dispozitive mobile și la internet accesibil servește drept condiție prealabilă pentru asigurarea incluziunii lor financiare digitale. Prin urmare, inegalitățile în accesul la tehnologiile digitale se pot reflecta în inegalități care au ca rezultat niveluri de incluziune financiară. În concluzie, dreptul la conectivitate devine, astfel, strâns legat de dreptul la participare economică și socială în societatea contemporană.

5.2. Aspecte comportamentale ale tinerilor care cresc gradul de vulnerabilitate

Digitalizarea aduce numeroase beneficii pentru incluziunea financiară a tinerilor, oferind servicii personalizate, mai accesibile și mai atractive, precum și posibilitatea evaluării alternative a bonității acestora. Totuși, utilizarea serviciilor financiare digitale implică și riscuri noi. Acestea includ fraude, probleme de securitate și confidențialitate, acces rapid la credite costisitoare pe termen scurt sau excluziune financiară datorată lipsei accesului la tehnologie sau conectivitate.

Tinerii sunt deosebit de vulnerabili la escrocherii, datorită lipsei de experiență și a supraîncrederii, iar utilizarea excesivă a creditului poate duce la îndatorare neadecvată și excluziune financiară pe termen lung. Expunerea frecventă la internet ridică riscuri suplimentare legate de securitatea cibernetică și protecția datelor personale. De asemenea, natura virtuală a plăților poate face ca banii să pară mai puțin reali, ceea ce poate conduce la cheltuieli necontrolate sau la acumularea unor datorii, ridicând astfel probleme de protecție a consumatorului financiar.

În același timp, din perspectivă comportamentală, ușurința de a realiza plăți online poate reprezenta o provocare pentru tinerii care utilizează produse financiare digitale. Opțiunile de achiziție fără numerar prin magazine online, rețele sociale sau carduri contactless pot face ca banii să pară mai puțin reali, iar tinerii s-ar putea să nu realizeze că plătesc bani reali, cum se întâmplă în cazul achizițiilor în aplicații sau jocuri, care pot fi legate de retrageri automate. Aceasta poate conduce la cheltuieli excesive și îndatorare, ridicând astfel preocupări legate de protecția consumatorului financiar.

Majoritatea tinerilor cu vârste între 16 și 24 de ani utilizează internetul, generând constant date personale care pot fi colectate și analizate de terți. Dezvoltările tehnologice și interacțiunile frecvente online contribuie la creșterea volumului de informații deținute de instituțiile financiare. Totuși, cercetările arată că mulți tineri nu înțeleg pe deplin termenii și condițiile atunci când își oferă consimțământul pentru partajarea datelor, inclusiv aspectele legate de confidențialitate (Obar și Oeldorf-Hirsch, 2020).

Atitudinea tinerilor față de propriile date digitale este variabilă și depinde adesea de contextul național și de situația specifică a fiecărei țări. În România există un număr mare de persoane tinere ce folosesc diverse platforme de socializare unde publică date cu caracter personal care i-ar putea face vulnerabili în fața unor fraude financiare online.

6. Combaterea fraudelor financiare online

6.1 Cadrul legislativ la nivel național și european

Fraudele financiare online reprezintă o amenințare persistentă și tot mai sofisticată la adresa ecosistemului financiar contemporan. Acestea afectează în mod direct **integritatea sistemelor de plăți**, periclitând funcționarea fluentă a tranzacțiilor digitale, inducând pierderi financiare semnificative atât pentru instituțiile implicate, cât și pentru consumatori. În paralel, afectarea **încrederii publicului în securitatea serviciilor financiare digitale** are consecințe negative asupra gradului de adopție a noilor tehnologii și, implicit, asupra eficienței generale a piețelor financiare. Nu în ultimul rând, prin amploarea și impactul sistemic al anumitor atacuri cibernetice, fraudele financiare online pot submina **stabilitatea financiară, atât la nivel național, cât și european**, în special în contexte de criză economică sau instabilitate geopolitică.

Complexitatea acestor fraude derivă din interconectarea mai multor dimensiuni fundamentale: tehnologică, operațională și comportamentală. Pe de o parte, evoluțiile tehnologice rapide – cum ar fi utilizarea infrastructurilor de plată moderne (ex. SEPA Instant Credit Transfer), a interfețelor de programare a aplicațiilor (API) pentru open banking sau a metodelor avansate de autentificare (ex. autentificare multifactorială sau biometrică) – au contribuit la crearea unui mediu de plată eficient, dar totodată vulnerabil la exploatare de către actori malițioși. Aceste tehnologii, deși menite să crească securitatea și accesibilitatea, sunt adesea ținta atacurilor sofisticate, precum fraudele de **tip man-in-the-middle, spoofing sau compromiterea canalelor API**.

Pe de altă parte, **componentele operaționale**, precum procesele interne de control, arhitectura de guvernanta a riscurilor și gestionarea incidentelor cibernetice, joacă un rol esențial în prevenirea și atenuarea impactului fraudelor. Deficiențele în aceste domenii – cum ar fi lipsa de instrumente adecvate de detectare a anomaliilor, timpul mare de reacție la incidente sau lipsa unor protocoale clare de remediere – pot facilita succesul atacurilor și pot amplifica pierderile.

Nu în ultimul rând, **factorul uman** rămâne una dintre cele mai mari vulnerabilități în fața fraudelor financiare online. Lipsa educației digitale a consumatorilor, gradul redus de conștientizare cu privire la tehnicile de inginerie socială (precum phishingul, vishingul, smishingul etc.), dar și comportamentele riscante în mediul online (utilizarea parolelor slabe, accesarea unor linkuri nesigure) contribuie la expunerea crescută a utilizatorilor la fraude. Astfel, protejarea infrastructurilor informatice nu este suficientă în absența unei culturi digitale de securitate în rândul utilizatorilor finali.

În acest context de **digitalizare accelerată a serviciilor financiare** și de creștere a interdependenței actorilor implicați, se impune cu stringență existența unui **cadru legislativ coerent și adaptabil**. Acesta trebuie să fie articulat la nivelul Uniunii Europene – având în vedere caracterul transfrontalier al fraudelor – și să fie transpus în mod uniform și eficient în dreptul național. Legislația trebuie să acopere toate formele de criminalitate financiară digitală, să impună standarde minime de securitate și conformitate, și să prevadă mecanisme clare de coordonare între autorități și entitățile din sectorul privat.

Rolul cadrului legislativ este să asigure un ecosistem de securitate adecvat pentru plăți, să stimuleze încrederea utilizatorilor și să asigure continuitatea operațională a infrastructurilor de plată, în timp ce se respectă drepturile fundamentale ale persoanelor (precum GDPR, drepturi de acces, de portabilitate, de rectificare). Într-un spațiu economic european caracterizat prin integrare și interdependențe, reglementările asigură un echilibru între deschiderea inovației (open banking, API-uri securizate) și controlul riscurilor de fraudă, cu o atenție sporită asupra rezilienței operaționale și a protecției datelor.

A. Directiva PSD2 - Payment Services Directive 2

Directiva (UE) 2015/2366 privind serviciile de plată în cadrul pieței interne, cunoscută sub denumirea de PSD2 (Payment Services Directive 2), este un instrument legislativ esențial adoptat de Uniunea Europeană în scopul modernizării, consolidării și securizării serviciilor de plată din spațiul economic european.

PSD2 a fost adoptată de Parlamentul European și Consiliul Uniunii Europene la data de 25 noiembrie 2015 și a înlocuit prima directivă în domeniul serviciilor de plată (PSD1 – Directiva 2007/64/CE), pentru a răspunde noilor provocări generate de digitalizarea accelerată, apariția fintech-urilor și creșterea numărului de tranzacții online.

Obiectivele noii Directive au vizat crearea unei piețe unice integrate pentru serviciile de plată electronice, prin armonizarea legislației între statele membre, îmbunătățirea siguranței tranzacțiilor electronice și a protecției consumatorilor, inclusiv prin introducerea autentificării stricte a clientului (SCA), promovarea inovației și concurenței, prin deschiderea accesului la conturi pentru furnizorii terți autorizați (TPP – Third Party Providers), cum ar fi fintech-urile, creșterea transparenței comisioanelor și a drepturilor utilizatorilor, precum și consolidarea cadrului de reglementare pentru soluționarea litigiilor.

PSD2 are un impact transformator asupra modului în care se realizează plățile online în Uniunea Europeană, introducând concepte-cheie care modifică fundamental relația dintre utilizatori, bănci și furnizorii de servicii:

Autentificarea strictă a clientului (Strong Customer Authentication – SCA)

Una dintre cele mai importante inovații ale PSD2 este introducerea SCA, o metodă de autentificare care impune utilizarea a cel puțin două din următoarele trei elemente:

- ceva ce numai utilizatorul cunoaște (ex: parolă, PIN),
- ceva ce numai utilizatorul deține (ex: telefon, token),
- ceva ce aparține utilizatorului (ex: amprentă, recunoaștere facială).

Această măsură are ca scop protejarea consumatorilor împotriva fraudelor, în special în tranzacțiile online cu cardul și în accesarea conturilor de la distanță.

Accesul terților la conturi (Open Banking)

PSD2 introduce conceptul de Open Banking, prin care băncile sunt obligate să permită accesul securizat la conturile clienților către terți autorizați, cum ar fi:

- PISP (Payment Initiation Service Providers) – furnizori care inițiază plăți în numele clientului;
- AISP (Account Information Service Providers) – furnizori care colectează și oferă informații despre conturile clientului din mai multe bănci.

Acest sistem permite, de exemplu, ca un client să își poată efectua plățile direct dintr-o aplicație fintech, fără a mai accesa interfața băncii, în condiții de securitate reglementată.

Pentru **utilizatorul final** (persoane fizice sau juridice), PSD2 aduce o serie de **beneficii concrete**:

- Creșterea securității tranzacțiilor, prin obligativitatea autentificării stricte;
- Acces la noi servicii financiare inovatoare, precum agregatoare de conturi, aplicații de management financiar personal sau plăți directe între conturi;
- Reducerea dependenței de un singur furnizor (bancă) – clienții pot gestiona conturile din mai multe bănci într-o singură aplicație;
- Creșterea transparenței și a drepturilor, inclusiv în ceea ce privește retragerile de consimțământ, răspunderea în caz de fraudă și comisioanele percepute.

În același timp, utilizatorii trebuie să fie mai bine informați cu privire la modul în care își partajează datele și la riscurile asociate serviciilor oferite de terți, chiar dacă aceștia sunt autorizați.

Pentru **băncile și instituțiile de plată**, PSD2 presupune o **schimbare fundamentală de paradigmă**:

- Obligația de a oferi acces la cont prin API-uri securizate către TPP-uri autorizate (Open API Banking);
- Costuri de conformare crescute, pentru implementarea cerințelor tehnice (autentificare, sisteme antifraudă, interfețe conforme);
- Pierderea parțială a monopolului asupra relației cu clientul, în favoarea fintech-urilor care oferă experiențe digitale superioare;
- Necesitatea transformării digitale accelerate, pentru a rămâne competitive într-un ecosistem financiar deschis și bazat pe colaborare.

De asemenea, băncile trebuie să își revizuiască modelele de business și să adopte o cultură a inovației, în paralel cu menținerea conformității cu reglementările.

Directiva PSD2 reprezintă un pas esențial în modernizarea ecosistemului financiar european, asigurând securitate sporită, concurență loială și inovație în sectorul serviciilor de plată. În același timp, aceasta presupune responsabilități crescute pentru toți actorii implicați: de la utilizatorii individuali, care trebuie să fie mai vigilenți în partajarea datelor, până la instituțiile financiare, care trebuie să își regândească modelele de afaceri.

La nivel national, transpunerea s-a făcut cu o întârziere semnificativă, Legea 209 intrând în vigoare în noiembrie 2019, înlocuind astfel Legea nr. 127/2011, care implementa anterior Directiva PSD1. Noua lege a fost publicată în Monitorul Oficial nr. 868/28.10.2019 și a introdus modificări structurale în reglementarea serviciilor de plată, conform noilor cerințe europene.

Adoptarea **Legii nr. 209/2019 privind serviciile de plată** și pentru modificarea unor acte normative a avut loc în contextul obligativității statelor membre UE de a transpune în legislația națională Directiva (UE) 2015/2366 privind serviciile de plată în cadrul pieței interne (PSD2), cu termen limită de transpunere 13 ianuarie 2018.

Obiectivele legii au fost să asigure alinierea completă la cerințele PSD2, să promoveze inovația în sistemul de plăți, în special prin sprijinirea Open Banking, de să întărească securitatea tranzacțiilor electronice și să protejeze mai eficient utilizatorii, să asigure accesul egal al furnizorilor terți la infrastructura bancară și să îmbunătățească supravegherea și controlul serviciilor de plată de către autoritatea competentă (BNR).

Principalele prevederi și adaptări din Directiva PSD2

1. Clasificarea serviciilor de plată

Legea preia și detaliază lista serviciilor de plată reglementate de PSD2, cum ar fi:

- Transferuri de credit și plăți prin card;
- Debit direct;
- Emiterea de instrumente de plată;
- Servicii de inițiere a plății (PISP) – nou introdusă;
- Servicii de informare privind conturile (AISP) – nou introdusă.
- Această clasificare este esențială pentru a delimita obligațiile și drepturile furnizorilor în funcție de natura activității desfășurate.

2. Accesul la conturi și deschiderea pieței (Open Banking)

Unul dintre cele mai importante elemente preluate din PSD2 este obligația băncilor (ASPSP – Account Servicing Payment Service Providers) de a permite accesul securizat și nediscriminatoriu al furnizorilor terți (TPP – Third Party Providers) la conturile de plăți ale clienților, cu consimțământul explicit al acestora.

Această prevedere a fost transpusă în legislația românească prin articolele referitoare la:

- Drepturile de acces la conturi ale PISP și AISP;
- Obligația instituțiilor financiare de a furniza interfețe dedicate (API);
- Stabilirea cerințelor de securitate și standarde tehnice, în conformitate cu reglementările Autorității Bancare Europene (EBA) și ale Băncii Naționale a României.

3. Autentificarea strictă a clientului (SCA)

Legea 209/2019 implementează cerința PSD2 privind utilizarea autentificării stricte a clientului (SCA) pentru accesarea contului de plată online și inițierea tranzacțiilor electronice, aplicabilă tuturor furnizorilor de servicii de plată. BNR, în colaborare cu instituțiile financiare, a emis reglementări privind modul de aplicare a SCA, iar instituțiile au fost obligate să se conformeze cerințelor până în 2021.

4. Autorizarea și supravegherea furnizorilor de servicii de plată

Legea extinde competențele Băncii Naționale a României ca autoritate competentă pentru:

- Autorizarea instituțiilor de plată și a celor emitente de monedă electronică;
- Menținerea unui registru public al furnizorilor autorizați, interoperabil cu registrul european EBA;
- Controlul și aplicarea sancțiunilor în caz de nerespectare a reglementărilor.

De asemenea, se stabilesc cerințe prudențiale, de capital minim și condiții de asigurare a răspunderii civile pentru TPP-uri.

5. Drepturile și obligațiile utilizatorilor

Legea reglementează în detaliu:

- Termenele de executare a tranzacțiilor;
- Responsabilitățile furnizorilor în caz de tranzacții neautorizate;
- Condițiile de retragere a consimțământului;
- Procedura de recuperare a fondurilor în caz de erori sau fraude.

Aceste prevederi întăresc **protecția utilizatorilor**, în special în fața fraudelor financiare online, sporind încrederea în utilizarea serviciilor digitale. Adoptarea și implementarea Legii nr. 209/2019 a avut un **impact semnificativ** asupra structurii, funcționării și reglementării sistemului financiar din România.

6. Modernizarea pieței de plăți

- Legea a impulsionat dezvoltarea de noi produse și servicii digitale, în special în sectorul fintech;
- A încurajat apariția de **TPP-uri locale**, care oferă servicii de inițiere a plății și informare privind conturile.

7. Creșterea concurenței și a inovației

- Instituțiile bancare au fost obligate să își deschidă infrastructura către terți, ceea ce a dus la **reconfigurarea relației cu clientul** și la accelerarea transformării digitale;
- Fintech-urile au devenit jucători activi în sistemul de plăți, contribuind la diversificarea ofertei și la reducerea costurilor pentru utilizatori.

8. Consolidarea securității în plățile online

- Aplicarea SCA a redus semnificativ riscul de fraudă în tranzacțiile electronice, deși a impus inițial **costuri tehnice** semnificative instituțiilor financiare;
- A crescut încrederea utilizatorilor în utilizarea platformelor digitale de plată.

9. Provocări în implementare

- Unele bănci au întâmpinat dificultăți în dezvoltarea API-urilor conforme;
- Gradul redus de alfabetizare digitală al unor segmente ale populației a întârziat adopția unor funcționalități noi (ex: agregatoare de conturi);
- Autoritățile au fost nevoite să **armonizeze reglementările secundare** într-un timp relativ scurt pentru a susține implementarea practică a legii.

B. Regulamentul DORA – Regulamentul (UE) 2022/2554 privind reziliența operațională digitală a sectorului financiar

Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar, cunoscut sub denumirea **DORA**, a fost adoptat la **14 decembrie 2022** și a intrat în vigoare pe **16 ianuarie 2023**, cu aplicabilitate directă începând cu **17 ianuarie 2025**.

DORA creează un cadru unitar la nivelul Uniunii Europene pentru asigurarea rezilienței operaționale digitale a instituțiilor financiare, adică capacitatea acestora de a preveni, rezista, răspunde și se recupera în fața incidentelor cibernetice și a disfuncționalităților IT.

Obiectivele DORA vizează consolidarea securității cibernetice în sectorul financiar european, armonizarea reglementărilor existente privind riscurile ICT (tehnologia informației și comunicațiilor), crearea unui cadru legal unitar și obligatoriu, aplicabil tuturor actorilor financiari, reducerea riscurilor sistemice generate de dependența de furnizorii terți de servicii IT (cloud, software, infrastructură etc.).

Spre deosebire de alte reglementări sectoriale, DORA are un caracter transversal, aplicându-se tuturor entităților financiare reglementate, inclusiv:

- Bănci, instituții de plată și de monedă electronică;
- Societăți de asigurare și reasigurare;
- Societăți de investiții și firme de administrare a activelor;
- Infrastructuri pieței financiare (depozitari centrali, contrapărți centrale etc.);
- Fintech-uri, firme de tehnologie financiară;
- Furnizori terți de servicii IT critice, cum ar fi furnizorii de cloud, software sau analiză de date.

Dintre prevederile esențiale, menționăm:

1. Gestionarea riscurilor TIC (IT/ICT risk management)

Instituțiile trebuie să implementeze politici și controale robuste pentru:

- Identificarea, prevenirea și monitorizarea riscurilor cibernetice și IT;
- Protejarea rețelilor, sistemelor și datelor sensibile;
- Audituri și testări periodice ale rezilienței sistemelor informatice;
- Continuitatea operațiunilor în cazul unor întreruperi digitale majore.

2. Raportarea incidentelor majore

- Instituțiile trebuie să raporteze rapid (în termen de 4 ore sau conform standardelor EBA) incidentele cibernetice majore către autoritățile naționale competente (ex. BNR în România);
- Se instituie un sistem comun de clasificare a incidentelor și o rețea europeană de schimb de informații privind atacurile cibernetice.

3. Testarea rezilienței digitale

- Instituțiile semnificative sunt obligate să efectueze teste avansate de penetrare (TLPT – Threat-Led Penetration Testing) cel puțin o dată la trei ani, cu implicarea unor echipe externe autorizate;
- Testele vor simula atacuri cibernetice sofisticate asupra sistemelor IT critice.

4. Gestionarea riscurilor externe și relația cu furnizorii IT

- DORA introduce cerințe stricte privind contractele cu furnizorii de servicii IT (SaaS, cloud, outsourcing IT);
- Se instituie monitorizarea directă a furnizorilor critici de tehnologie de către autoritățile europene (de ex. EBA, ESMA, EIOPA), în funcție de impactul lor sistemic;
- Instituțiile financiare trebuie să mențină o mapare completă a relațiilor cu furnizorii IT, inclusiv planuri de ieșire și continuitate.

5. Partajarea informațiilor privind amenințările cibernetice

- Se încurajează partajarea voluntară de informații între instituții cu privire la amenințări și incidente cibernetice;
- Aceasta are ca scop îmbunătățirea capacității colective de apărare și reacție.

DORA marchează o schimbare de paradigmă, trecând de la recomandări generale privind securitatea IT la obligații legale stricte, cu impact semnificativ asupra:

1. Structurilor de guvernare și management al riscurilor

- Conducerea instituției va fi direct responsabilă pentru gestionarea riscurilor TIC;
- Este necesară desemnarea unor responsabili IT și de securitate cibernetică, precum și implementarea unui cadru de control intern adaptat.

2. Procesele de achiziție și outsourcing IT

- Instituțiile trebuie să revizuiască contractele existente cu furnizorii de servicii IT;
- Cresc exigențele privind evaluarea prealabilă, monitorizarea și auditarea acestor furnizori.

3. Creșterea costurilor de conformitate

- Implementarea cerințelor DORA presupune investiții substanțiale în infrastructură, consultanță, audit, personal specializat și testare;

În același timp, aceste investiții vor reduce riscul de pierderi reputaționale și financiare cauzate de atacuri cibernetice. În România, fiind un regulament al UE, DORA s-a aplicat direct în toate statele membre, , fără a necesita transpunere prin legislație națională. Totuși, este necesară:

- Adaptarea reglementărilor secundare emise de autoritățile naționale (BNR, ASF);
- Dezvoltarea capacităților instituționale de supraveghere și intervenție în caz de incident;
- Stabilirea responsabilităților clare între instituțiile naționale (CERT-RO, BNR, ASF, etc.).

Pentru România, aplicarea DORA constituie o provocare majoră, dar și o oportunitate de a alinia sistemul financiar național la cele mai înalte standarde de reziliență digitală. Succesul implementării va depinde de colaborarea eficientă între autorități, instituții financiare, furnizori IT și sectorul de securitate cibernetică, într-un mediu marcat de riscuri tot mai sofisticate.

C. Regulamentul (UE) nr. 910/2014 – eIDAS - Identitate electronică și încredere în tranzacțiile financiare digitale

Regulamentul **eIDAS** (electronic IDentification, Authentication and trust Services) a fost adoptat de **Parlamentul European și Consiliul Uniunii Europene** la **23 iulie 2014** și a intrat în vigoare începând cu **1 iulie 2016**. Acesta stabilește un cadru juridic la nivelul UE pentru identificarea electronică și serviciile de încredere, menite să faciliteze tranzacțiile electronice sigure, transparente și transfrontaliere în cadrul pieței unice digitale.

Obiectivele Regulamentului eIDAS vizează crearea unui cadru european de încredere pentru identificarea electronică și semnăturile digitale, asigurarea recunoașterii reciproce a metodelor de identificare electronică între statele membre, consolidarea securității și încrederii în serviciile digitale publice și private și facilitarea dezvoltării pieței unice digitale, prin sprijinirea tranzacțiilor electronice transfrontaliere.

Dintre prevederile esențiale, menționăm:

a) Identificarea electronică (eID)

- Se referă la recunoașterea și validarea identității unei persoane fizice sau juridice într-un context digital (ex: autentificare pentru accesarea unui cont bancar online);
- Fiecare stat membru poate notifica sistemele sale naționale de identificare electronică, iar acestea vor fi recunoscute de toate celelalte state membre.

Exemplu de aplicare: un cetățean român poate accesa un serviciu financiar într-un alt stat membru utilizând un sistem de identificare electronică emis de autoritățile române (ex: semnătura electronică calificată).

b) Serviciile de încredere (Trust Services)

Acestea sunt servicii electronice care sporesc securitatea și încrederea în comunicațiile digitale. eIDAS reglementează:

- Semnătura electronică (simplă, avansată, calificată);
- Sigiliile electronice (echivalentul semnăturii pentru entități juridice);
- Timestamps (marcaje temporale calificate);
- Servicii de livrare electronică înregistrată (ERSD) – ex: echivalentul electronic al scrisorii recomandate;
- Certificatele pentru autentificarea website-urilor.

Regulamentul eIDAS are un rol crucial în ecosistemul serviciilor financiare digitale, prin furnizarea unui cadru legal pentru autentificare, semnare, comunicare și validare digitală sigură:

1. Autentificare și acces la servicii bancare online

- eIDAS permite autentificarea utilizatorilor pe platforme bancare folosind mijloace de identificare electronică recunoscute la nivel european;
- Este complementar cu PSD2, care prevede autentificarea strictă a clientului (SCA). eIDAS furnizează instrumentele tehnice și juridice pentru aplicarea acestor cerințe.

2. Semnătura electronică în deschiderea de conturi, contracte și autorizări

- Permite semnarea electronică a contractelor de credit, a cererilor de produse financiare sau a documentelor de identificare (KYC);
- Semnătura electronică calificată are valoare legală echivalentă semnăturii olografe în toate statele UE – esențială în relațiile digitale între bănci și clienți.

3. Reducerea riscurilor de fraudă și creșterea securității

- Serviciile de încredere permit verificarea integrității documentelor și comunicărilor, prevenind modificarea neautorizată a datelor;
- Contribuie la protecția împotriva fraudelor de tip phishing, spoofing, social engineering etc.

4. Reducerea riscurilor de fraudă și creșterea securității

- eIDAS face posibilă desfășurarea de operațiuni financiare transfrontaliere cu același nivel de încredere ca cele interne, facilitând mobilitatea financiară în cadrul UE.

În România, aplicarea Regulamentului eIDAS a fost sprijinită prin:

- **Legea nr. 455/2001 privind semnătura electronică** (actualizată ulterior pentru conformitate cu eIDAS);
- **Legea nr. 135/2020 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice**, care asigură compatibilitatea cadrului intern cu eIDAS și abrogă dispoziții depășite din legislația anterioară;
- Reglementările **Autorității pentru Digitalizarea României (ADR)**, care supraveghează prestatorii de servicii de încredere calificați.

Prestatori de servicii în România, cum sunt certSIGN, DigiSign, Trans Sped oferă semnături electronice calificate, certificate digitale, marcare temporală etc., folosite de instituții financiare, autorități și clienți.

Raportat la utilizarea practică în sistemul financiar, băncile permit semnarea electronică a contractelor, solicitărilor de credit, actelor adiționale etc, în timp ce platformele fintech folosesc identificarea video și semnătura electronică calificată pentru onboarding digital. Regulamentul eIDAS este o componentă esențială a infrastructurii digitale europene, care permite desfășurarea sigură, rapidă și legală a tranzacțiilor financiare online. Prin instituirea unui cadru de încredere unificat la nivelul UE, eIDAS facilitează nu doar eficiența operațională, ci și interoperabilitatea transfrontalieră, aspect crucial într-un ecosistem financiar din ce în ce mai globalizat.

În România, adoptarea și utilizarea eIDAS a progresat semnificativ, în special în mediul bancar și fintech, însă nivelul de penetrare în rândul populației rămâne relativ scăzut.

Sunt necesare măsuri suplimentare de educare digitală, sprijin instituțional și armonizare legislativă, pentru ca beneficiile eIDAS să fie valorificate pe deplin.

Cele trei reglementări: **PSD2, DORA, eIDAS** formează un cadru strategic unificat pentru digitalizarea sigură a serviciilor financiare în UE:

- **eIDAS** este fundația **identificării digitale** și a **semnăturii electronice**, oferind **încredere și legalitate** tranzacțiilor online, inclusiv în sectorul financiar.
- **PSD2** creează un ecosistem financiar digital competitiv și sigur, permițând **Open Banking** și impunând cerințe de securitate, în special pentru **plățile online**.
- **DORA** adaugă o componentă esențială de **reziliență operațională digitală**, vizând **protecția infrastructurii IT** și a serviciilor financiare în fața atacurilor cibernetice și a incidentelor.

Criteriu	eIDAS	PSD2	DORA
Denumire completă	Identificare & încredere digitală	Servicii de plată	Reziliență digitală
Scop principal	Identificare + semnături	Open Banking + securitate	Gestionarea riscurilor IT
Instrument legislativ	Regulament	Directivă	Regulament
Intrare în vigoare	2016	2018	2023 (aplicabil din 2025)
Aplicabilitate în România	Legea 135/2020	Legea 209/2019	Aplicabil direct din 2025
Autoritate competentă	ADR	BNR	BNR, ASF, CERT-RO

6.2 Rolul instituțiilor financiare în prevenirea și combaterea fraudelor

În contextul digitalizării accelerate a serviciilor financiare și al intensificării atacurilor cibernetice, rolul instituțiilor financiare în prevenirea și combaterea fraudelor financiare online devine nu doar esențial, ci și extrem de complex. Acest rol presupune o clarificare riguroasă a responsabilităților între toți actorii implicați în lanțul de furnizare a serviciilor financiare, începând cu băncile tradiționale și până la noile entități fintech, care operează în baza directivelor europene precum PSD2.

Se identifica astfel o necesitate a clarificării responsabilităților între actorii implicați: băncile și alte instituții financiare trebuie să asigure securitatea infrastructurii proprii și să implementeze mecanisme robuste de autentificare și monitorizare a tranzacțiilor; furnizorii de servicii de plată (Payment Service Providers – PSP) trebuie să respecte cerințele tehnice și de raportare prevăzute de reglementările europene (precum PSD2); entitățile terțe autorizate (Third Party Providers – TPP), inclusiv fintech-urile, trebuie să se conformeze standardelor de interoperabilitate și securitate; iar autoritățile de reglementare trebuie să supravegheze proactiv respectarea normelor și să coordoneze răspunsul instituțional la incidentele majore.

✓ **Băncile și instituțiile financiare tradiționale**

În contextul transformării digitale accelerate a sectorului financiar, **Băncile** dețin un rol central în asigurarea securității infrastructurii critice și a încrederii publice în sistemul de plăți. Fiind principalii intermediari între utilizatorii de servicii financiare și piața financiară în ansamblul său, băncile trebuie să adopte o abordare proactivă și integrată în ceea ce privește prevenirea și combaterea fraudelor financiare online.

În primul rând, este esențial ca băncile să asigure securitatea infrastructurii proprii, ceea ce presupune protejarea rețelelor interne, a canalelor de comunicare, a sistemelor de core-banking și a platformelor de internet banking și mobile banking. Acest lucru implică investiții continue în tehnologii de securitate cibernetică, în soluții de criptare, firewall-uri de ultimă generație și sisteme de prevenire a intruziunilor (IPS), precum și în politici de securitate interne riguroase. Lipsa unor măsuri eficiente în acest sens poate conduce la expunerea datelor financiare sensibile ale clienților și la compromiterea integrității tranzacțiilor. În al doilea rând, băncile trebuie să implementeze mecanisme robuste de autentificare a utilizatorilor, în conformitate cu cerințele impuse de Directiva (UE) 2015/2366 privind serviciile de plată (PSD2), care introduce conceptul de Autentificare Strictă a Clientului (Strong Customer Authentication – SCA). Aceasta presupune aplicarea unei autentificări multifactoriale care să combine cel puțin două elemente independente: ceva ce utilizatorul știe (ex. parolă), ceva ce deține (ex. dispozitiv mobil) și ceva ce este (ex. amprentă sau recunoaștere facială). Implementarea corectă a SCA reduce semnificativ riscurile de acces neautorizat și protejează clientul împotriva fraudelor de tip phishing sau spoofing. Un alt element esențial în arhitectura de securitate a băncilor îl reprezintă monitorizarea în timp real a tranzacțiilor financiare, în vederea detectării comportamentelor anormale sau suspecte. Această monitorizare se realizează prin utilizarea unor tehnologii avansate, precum inteligența artificială, învățarea automată (machine learning) și sisteme specializate de detectare a fraudei (fraud detection engines), care pot analiza volume mari de date și identifica tipare sau deviații comportamentale ce pot indica activități frauduloase. Astfel, băncile nu doar reacționează la incidente, ci pot preveni în mod activ producerea acestora. Totodată, băncile au obligația legală și etică de a colabora cu autoritățile de reglementare și supraveghere, precum Banca Națională a României (BNR), Autoritatea Bancară Europeană (EBA), precum și cu entități specializate în securitate cibernetică, precum CERT-RO sau CSIRT financiar.

Aceasta presupune aplicarea unei autentificări multifactoriale care să combine cel puțin două elemente independente: ceva ce utilizatorul știe (ex. parolă), ceva ce deține (ex. dispozitiv mobil) și ceva ce este (ex. amprentă sau recunoaștere facială). Implementarea corectă a SCA reduce semnificativ riscurile de acces neautorizat și protejează clientul împotriva fraudelor de tip phishing sau spoofing. Un alt element esențial în arhitectura de securitate a băncilor îl reprezintă monitorizarea în timp real a tranzacțiilor financiare, în vederea detectării comportamentelor anormale sau suspecte. Această monitorizare se realizează prin utilizarea unor tehnologii avansate, precum inteligența artificială, învățarea automată (machine learning) și sisteme specializate de detectare a fraudei (fraud detection engines), care pot analiza volume mari de date și identifica tipare sau deviații comportamentale ce pot indica activități frauduloase. Astfel, băncile nu doar reacționează la incidente, ci pot preveni în mod activ producerea acestora. Totodată, băncile au obligația legală și etică de a colabora cu autoritățile de reglementare și supraveghere, precum Banca Națională a României (BNR), Autoritatea Bancară Europeană (EBA), precum și cu entități specializate în securitate cibernetică, precum CERT-RO sau CSIRT financiar. Această colaborare presupune nu doar respectarea reglementărilor în vigoare, ci și raportarea promptă a incidentelor de securitate care ar putea afecta confidențialitatea, integritatea sau disponibilitatea datelor financiare. O comunicare eficientă cu autoritățile contribuie la o reacție coordonată în fața amenințărilor emergente și la consolidarea rezilienței sistemului financiar.

Prin urmare, băncile nu trebuie privite exclusiv ca simpli procesatori de plăți, ci ca actori fundamentali în ecosistemul de securitate financiară digitală, cu responsabilitate directă în prevenirea pierderilor financiare cauzate de fraude. Rolul lor transcende granițele operaționale tradiționale și implică asumarea unui leadership activ în dezvoltarea unei culturi organizaționale orientate spre securitate, inovare și conformitate.

✓ **Furnizorii de servicii de plată (PSP)**

În arhitectura modernă a sistemelor financiare digitale, furnizorii de servicii de plată (**Payment Service Providers – PSP**), care includ atât instituțiile bancare, cât și entitățile nebancare autorizate, joacă un rol esențial în menținerea integrității, securității și eficienței infrastructurii de plăți. Funcționarea acestora este reglementată în principal prin Directiva (UE) 2015/2366 privind serviciile de plată în cadrul pieței interne (PSD2), care stabilește cadrul juridic pentru facilitarea plăților electronice, creșterea concurenței, dar și consolidarea protecției consumatorilor și a securității tranzacțiilor.

Un prim aspect fundamental al activității PSP-urilor îl constituie respectarea cerințelor tehnice și de securitate elaborate de Autoritatea Bancară Europeană (European Banking Authority – EBA), în special prin Standardele Tehnice de Reglementare (Regulatory Technical Standards – RTS). Acestea includ obligații privind autentificarea strictă a clientului (Strong Customer Authentication – SCA), protejarea datelor sensibile și controlul accesului la informațiile financiare. În acest sens, PSP-urile trebuie să adopte măsuri tehnice și organizaționale care să prevină accesul neautorizat, interceptarea datelor și manipularea tranzacțiilor, asigurând totodată conformitatea cu normele de protecție a datelor cu caracter personal (GDPR).

De asemenea, PSD2 impune PSP-urilor implementarea de interfețe de programare a aplicațiilor (Application Programming Interfaces – API-uri) securizate, care permit accesul controlat al entităților terțe autorizate (Third Party Providers – TPP) la informațiile privind conturile bancare ale clienților, în baza consimțământului explicit al acestora. Acest model de open banking favorizează inovația și diversificarea serviciilor financiare, însă presupune și o răspundere crescută din partea PSP-urilor în ceea ce privește prevenirea fraudelor generate prin interceptarea sau compromiterea canalelor de comunicare digitală.

În plus, PSP-urile sunt obligate să transmită raportări periodice privind incidentele operaționale și de securitate majoră, în conformitate cu cerințele de transparență prevăzute de PSD2 și de ghidurile EBA. Aceste raportări trebuie efectuate într-un interval de timp bine definit și să conțină informații detaliate privind natura incidentului, impactul asupra clienților și măsurile corective implementate. Prin acest mecanism de supraveghere continuă, autoritățile naționale de reglementare – precum Banca Națională a României (BNR) – pot evalua în timp real gradul de expunere la risc al sistemului și pot coordona un răspuns instituțional eficient.

O componentă crucială în activitatea PSP-urilor este și verificarea riguroasă a identității clienților (know your customer – KYC), atât în etapa de onboarding, cât și pe parcursul întregii relații comerciale. Evaluarea continuă a riscurilor asociate cu comportamentul financiar al clienților, proveniența fondurilor sau potențialul de implicare în activități de spălare a banilor sau finanțare a terorismului face parte din cadrul extins al obligațiilor legale privind combaterea fraudelor și a criminalității economice.

Având în vedere complexitatea și dinamismul mediului digital, PSP-urile nu pot funcționa doar ca simpli intermediari de plăți, ci devin noduri critice în ecosistemul financiar digital, responsabilizate deopotrivă în plan tehnologic, juridic și operațional. Ele trebuie să asigure un echilibru între eficiența operațională și vigilența cibernetică, între accesibilitate și securitate, contribuind la consolidarea încrederii în serviciile financiare digitale și la protejarea utilizatorilor împotriva riscurilor emergente din spațiul cibernetic.

Astfel, rolul PSP-urilor este fundamental nu doar în facilitarea tranzacțiilor financiare, ci și în construirea unei arhitecturi robuste și reziliente de apărare împotriva fraudelor, în concordanță cu obiectivele strategice ale Uniunii Europene în domeniul digitalizării și securității financiare.

✓ **Entități terțe autorizate (TPP) și fintech-uri**

În contextul creșterii riscurilor asociate cu fraudele financiare online, entitățile terțe autorizate (**Third Party Providers – TPP**), inclusiv fintech-urile, joacă un rol crucial în prevenirea și combaterea acestor amenințări în cadrul ecosistemului financiar digital. Datorită poziției lor strategice de intermediari între utilizatori și instituțiile financiare tradiționale, aceste entități trebuie să adopte măsuri riguroase care să asigure securitatea și integritatea datelor și tranzacțiilor.

Un aspect esențial în prevenirea fraudelor constă în respectarea strictă a standardelor de interoperabilitate și securitate, precum cele impuse de Autoritatea Bancară Europeană și exprimate în standardele tehnice pentru API-uri (de exemplu, Berlin Group, Open Banking UK). Implementarea acestor standarde previne accesul neautorizat și manipularea datelor clienților, reducând astfel vulnerabilitățile care ar putea fi exploatate de fraudatori.

Gestionarea transparentă și auditabilă a consimțământului utilizatorilor este un alt element fundamental pentru prevenirea fraudelor. Prin asigurarea faptului că utilizatorii sunt pe deplin informați cu privire la accesul și utilizarea datelor lor, TPP-urile contribuie la reducerea riscurilor de acces neautorizat și la întărirea încrederii consumatorilor în serviciile digitale.

În plan tehnic, TPP-urile trebuie să implementeze controale IT solide și proceduri de securitate riguroase, cum ar fi criptarea datelor, autentificarea multifactorială și monitorizarea continuă a activităților suspecte. Aceste măsuri sunt vitale pentru a preveni ca aceste entități să devină „verigi slabe” în lanțul de securitate și pentru a detecta proactiv tentativele de fraudă sau atacurile cibernetic.

Mentținerea certificărilor de conformitate și colaborarea continuă cu autoritățile de reglementare asigură un cadru instituțional eficient pentru prevenirea și răspunsul prompt la incidentele de securitate. Raportarea incidentelor și schimbul de informații între părți facilitează identificarea tiparelor frauduloase și întărirea mecanismelor de apărare.

În cazul fintech-urilor, care sunt adesea caracterizate prin ritm accelerat de inovare, este deosebit de important să existe un echilibru între rapiditatea dezvoltării și implementarea unor mecanisme riguroase de control și prevenire a fraudelor, comparabile cu cele ale instituțiilor financiare tradiționale. Aceasta contribuie nu doar la protejarea utilizatorilor, ci și la sustenabilitatea și reputația pe termen lung a acestui segment emergent.

Astfel, entitățile terțe autorizate și fintech-urile nu sunt doar facilitatori ai serviciilor financiare digitale, ci și actori esențiali în arhitectura de prevenire a fraudelor, asumându-și responsabilități clare în protejarea ecosistemului financiar digital împotriva amenințărilor cibernetice și financiare.

✓ **Autoritățile de reglementare și supraveghere**

Autoritățile de reglementare și supraveghere reprezintă pilonii fundamentali în cadrul sistemului de prevenire și combatere a fraudelor financiare online. În România, instituții precum **Banca Națională a României (BNR)**, **Autoritatea pentru Supraveghere Financiară (ASF)** și **Autoritatea pentru Digitalizarea României (ADR)** dețin responsabilitatea de a supraveghea, coordona și reglementa activitatea tuturor actorilor implicați în ecosistemul financiar, asigurând implementarea coerentă a cadrului legislativ european și național, precum și menținerea stabilității și securității sistemului.

Unul dintre rolurile principale ale acestor instituții este emiterea normelor, ghidurilor și instrucțiunilor care facilitează transpunerea și aplicarea în practică a legislației europene. De exemplu, Legea nr. 209/2019 privind serviciile de plată reprezintă implementarea directă în dreptul românesc a Directivei PSD2 (Directiva (UE) 2015/2366). BNR, în calitate de autoritate de reglementare, a elaborat astfel norme care stabilesc cerințe stricte privind autentificarea clienților, raportarea incidentelor de securitate și protecția datelor utilizatorilor. Aceste reglementări sunt esențiale în prevenirea accesului neautorizat și reducerea riscurilor de fraudă la nivelul sistemului bancar și al serviciilor de plată.

În paralel, aceste autorități desfășoară controale și audituri de conformitate pentru a verifica respectarea cerințelor legale și tehnice de către furnizorii de servicii financiare, inclusiv bănci, PSP-uri și fintech-uri. De exemplu, BNR și ASF efectuează periodic inspecții și revizuri ale sistemelor IT și proceselor operaționale, identificând astfel potențiale vulnerabilități și impunând măsuri corective. În anul 2022, BNR a intensificat controalele în sectorul financiar digital, constatând deficiențe în implementarea autentificării stricte a clienților și solicitând remedieri urgente pentru a preveni tentativele de acces fraudulos la conturile clienților.



Gestionarea incidentelor majore de securitate cibernetică este o altă dimensiune critică a responsabilității autorităților. În România, **colaborarea strânsă între BNR, ASF, ADR și echipele specializate precum CERT-RO și CSIRT financiar** asigură un răspuns rapid și coordonat în cazul atacurilor cibernetice cu potențial impact sistemic. Un exemplu concret îl reprezintă reacția promptă la atacurile de tip phishing și malware care au vizat instituții financiare în 2023, când autoritățile au emis alerte publice, au coordonat investigații și au sprijinit implementarea unor măsuri tehnice suplimentare pentru a limita impactul și pentru a preveni repetarea acestor incidente.

În plus, autoritățile au un rol important în promovarea educației financiare și digitale ca mijloc de reducere a vulnerabilităților utilizatorilor în fața tacticilor de social engineering, care reprezintă una dintre cele mai frecvente cauze ale fraudelor financiare online. De exemplu, campanii publice inițiate de ADR și BNR au vizat creșterea gradului de conștientizare în rândul populației cu privire la riscurile tranzacțiilor online nesigure, metodele de protejare a datelor personale și importanța verificării autenticității solicitărilor financiare prin canale oficiale. Programe educaționale derulate în parteneriat cu mediul academic și organizațiile neguvernamentale au contribuit la reducerea numărului de victime ale fraudelor prin tehnici de manipulare psihologică, cum ar fi phishing-ul sau ingineria socială.

6.3 Colaborarea interinstituțională

Colaborarea interinstituțională este pilonul esențial al unei strategii eficiente de combatere a fraudelor financiare online. Aceasta trebuie să includă schimburi rapide și sigure de informații între instituții financiare, autorități naționale (poliție, parchet, CERT, ANAF, BNR etc.) și organisme europene (Europol, ENISA, EBA), dar și parteneriate public-private în domeniul securității cibernetice. O astfel de cooperare este indispensabilă pentru detectarea timpurie a amenințărilor, răspunsul coordonat în cazul unor atacuri la scară largă și consolidarea rezilienței operaționale a infrastructurilor critice de plată, într-un mediu digital în continuă transformare.

Colaborarea interinstituțională constituie pilonul central al unei strategii integrate și eficiente de prevenire, detectare și sancționare a fraudelor financiare online, într-un ecosistem digital caracterizat de interconectivitate sporită, convergență tehnologică și mutații rapide ale vectorilor de atac. Un cadru matur de cooperare presupune arhitecturi instituționale și procedurale capabile să faciliteze schimburi operative, securizate și standardizate de date între instituții financiare, autorități naționale cu atribuții complementare (poliție, parchet, CERT/DNSC, ANAF, BNR, autorități de supraveghere financiară și de protecție a datelor) și organisme europene cu rol de coordonare strategică și suport operațional (Europol/EC3, ENISA, EBA, Eurojust, OLAF), la care se adaugă parteneriate public-private robuste în domeniul securității cibernetice și al combaterii spălării banilor. În acest sens, mecanismele de partajare a informațiilor despre amenințări (Threat Intelligence) bazate pe standarde deschise (de exemplu, STIX/TAXII), platformele interorganizaționale de cooperare (ISAC-uri sectoriale, centre de fuziune informațională) și acordurile de cooperare (MoU-uri, protocoale de urgență) devin instrumente indispensabile pentru a asigura atât detecția timpurie, cât și răspunsul coordonat la incidente de amploare.

Eficacitatea cooperării depinde, totodată, de alinierea la cadrele normative și de supraveghere europene care introduc obligații de raportare, standarde tehnice și cerințe de reziliență: DORA pentru reziliența operațională digitală în sectorul financiar, NIS2 pentru securitatea rețelilor și a sistemelor informatice, PSD2/PSR și EBA Guidelines pentru plăți și autentificare puternică a clienților, respectiv regimul AML/CFT și cooperarea dintre unitățile de informații financiare (FIU). Integrarea acestor cerințe cu normele de protecție a datelor (GDPR) reclamă guvernanta clară a datelor, principii de minimizare și proporționalitate, precum și mecanisme de audit și trasabilitate care să asigure legitimitatea și responsabilizarea actorilor implicați. În plan operațional, capacitatea de reacție este consolidată prin exerciții comune de tip red/blue team și simulări paneuropene (de pildă, Cyber Europe), prin playbook-uri interinstituționale pentru categorii de fraude (phishing, fraudă de transfer autorizat – APP, malware bancar, compromiterea e-mailului de business – BEC) și prin canale de notificare în timp aproape real pentru blocarea fondurilor și înghețarea activelor transfrontaliere.

Nu în ultimul rând, un model de cooperare matur presupune guvernanta multi-nivel cu roluri și responsabilități explicit definite, indicatori de performanță (timp de detectare și răspuns, rata de recuperare a fondurilor, calitatea și latența informațiilor partajate), precum și mecanisme de învățare continuă care să transforme lecțiile din incidente în actualizări de politici, controale și standarde tehnice. Obstacolele inerente—diferențe jurisdicționale, asimetrii de capabilități, reticențe privind schimbul de date, fragmentare tehnologică—pot fi atenuate prin interoperabilitate tehnică, cadre de încredere și confidențialitate (de ex., enclave securizate, partajare federată), stimulente de conformare și programe comune de formare.

În plan concret, Europol susține această cooperare printr-un portofoliu consistent de acțiuni operaționale și instrumente tehnice care vizează direct fraudele online:

- Coordonarea operațiunilor paneuropene împotriva rețelilor de “money mules” (seria EMMA), în parteneriat cu bănci, fintech-uri și unități de informații financiare, cu efecte imediate în identificarea conturilor de tranzit, înghețarea rapidă a fondurilor și destructurarea celulelor implicate în phishing, BEC și escrocherii cu investiții.

-
- Destructurarea infrastructurilor criminale utilizate la scară largă în fraude: sprijin analitic, digital forensics și coordonare pentru operațiunile împotriva botnet-urilor și piețelor ilicite (de ex., Emotet, FluBot), a platformelor de vânzare a identităților/credentialelor furate (Genesis Market – “Operation Cookie Monster”), a serviciilor de spoofing telefonic (iSpoof), precum și a forumurilor și piețelor de pe dark web (RaidForums, DarkMarket); intervenții împotriva grupărilor de ransomware cu componente de extorcare și fraudă (de ex., Ragnar Locker), în cooperare strânsă cu Eurojust și autorități naționale.
 - Operarea infrastructurii SIENA (Secure Information Exchange Network Application) pentru schimbul securizat și în timp util de date operaționale între autoritățile de aplicare a legii și, în formate dedicate, cu sectorul privat, facilitând alinierea indicatorilor de fraudă și blocarea tranzacțiilor suspecte transfrontaliere.
 - Activitatea EC3 (European Cybercrime Centre) și a J-CAT (Joint Cybercrime Action Taskforce), care furnizează analiză de intelligence, corelarea probelor digitale, identificarea trendurilor de fraudă și coordonarea “action days” multinaționale pe vectori precum phishing/smishing, APP fraud și compromiterea e-mailului de business.
 - Inițiativa public–privată No More Ransom, ce pune la dispoziție instrumente gratuite de decriptare și ghiduri de remediere, reducând impactul economic al incidentelor care combină ransomware cu mecanisme de fraudare a plăților și de monetizare ilicită.
 - Proiectul SIRIUS, care oferă ghiduri, instrumente și canale standardizate pentru solicitări legale de date către furnizori online, accelerând obținerea de probe în anchetele de fraudă digitală.
 - Produsele strategice precum IOCTA (Internet Organised Crime Threat Assessment) și coordonarea priorităților EMPACT pentru “fraudă”, care alimentează cu analize de risc, recomandări de politici și planuri operaționale comune, inclusiv exerciții și formări dedicate investigatorilor financiari și echipelor CERT/CSIRT.

Prin aceste intervenții, Europol nu doar facilitează detectarea timpurie și răspunsul coordonat la fraudele online, ci și consolidează capacitatea instituțională a statelor membre și a partenerilor privați de a preveni, perturba și urmări penal ecosistemele frauduloase la nivel transfrontalier.

Astfel, cooperarea interinstituțională devine nu doar o condiție a detectării timpurii a amenințărilor și a gestionării coordonate a atacurilor la scară largă, ci și vectorul principal al consolidării rezilienței operaționale a infrastructurilor critice de plată, în consonanță cu dinamica și complexitatea mediului digital contemporan.

La nivel național, un exemplu relevant îl constituie proiectul „SiguranțaOnline”(www.sigurantaonline.ro), inițiativă de educație și prevenție derulată în parteneriat între comunitatea bancară și autorități precum Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC/CERT), BNR. Proiectul operationalizează cooperarea public–privată printr-un portal unificat de informare despre tipologii de fraudă (phishing, vishing, smishing, BEC, investiții false, APP), alerte și recomandări la zi, un „test de siguranță” pentru autoevaluarea nivelului de risc, ghiduri de igienă digitală și materiale didactice pentru școli și seniori, webinare tematice cu bănci și forțe de ordine, precum și trasee clare de raportare rapidă a incidentelor către bancă și Poliție. Integrarea cu fluxurile de alertare ale DNSC, campaniile media coordonate și mesageria unitară în aplicațiile de mobile/internet banking permit notificarea timpurie a clienților și blocarea accelerată a tranzacțiilor suspecte. Din perspectivă de guvernare și impact, proiectul aliniază comunicarea și procedurile operaționale ale băncilor cu cerințele NIS2/DORA privind conștientizarea și managementul incidentelor, impune indicatori comuni (timp de raportare, rata de escaladare către autorități, procentul de fonduri recuperate) și transformă lecțiile din cazuri reale în actualizări periodice de conținut și playbook-uri interinstituționale.

Astfel, „SiguranțaOnline” funcționează ca nod național de prevenție și răspuns împotriva fraudelor online, întărind reziliența consumatorilor și capacitatea de reacție a sectorului financiar.

7. Tranzacții online în siguranță – sfaturi esențiale pentru tineri

În contextul accelerării transformării digitale și al extinderii ecosistemului de plăți către aplicații mobile, portofele electronice, platforme de e-commerce și fintech, tinerii – nativi digital – devin simultan cei mai activi utilizatori și o categorie vulnerabilă la riscuri cibernetice și financiare emergente. Expunerea la scheme sofisticate de inginerie socială (phishing, smishing, vishing, impersonare pe rețele sociale), fraudă de plăți autorizate (APP), utilizarea necritică a linkurilor și codurilor QR, precum și gestionarea deficitară a datelor personale și a autentificării pe dispozitive multiple, amplifică probabilitatea compromiterii conturilor, a identității și a fondurilor.

În acest peisaj, **alfabetizarea financiară și igiena cibernetică** devin competențe de bază, comparabile ca relevanță cu cele digitale generale, aplicarea unor recomandări pentru efectuarea în siguranță a tranzacțiilor financiare online, fundamentate pe bune practici internaționale și pe cerințe de reglementare relevante (de exemplu, autentificare puternică a clientului conform PSD2/PSR, protecția datelor cu caracter personal, reziliența operațională DORA) contribuind la prevenție. Abordarea îmbină perspectiva tehnică (configurare securizată a dispozitivelor, gestionarea credențialelor, recunoașterea indicatorilor de compromitere) cu cea comportamentală (decizii informate în situații de presiune temporală, validarea identității interlocutorilor, igienă informațională pe rețele sociale) și cu elemente de protecție juridică și financiară (drepturi ale consumatorilor, proceduri de raportare și recuperare a fondurilor).

Dezvoltarea de competențe operaționale ușor de aplicat, cultivarea unei atitudini critice față de riscurile digitale contribuie la creșterea autonomiei și a rezilienței în gestionarea banilor în mediile online.

7.1. Verificarea site-urilor și platformelor de plată

Evaluarea credibilității comercianților și a intermediarilor de plată este premisa fundamentală a tranzacțiilor sigure. Legitimitatea se confirmă printr-o combinație de indicatori tehnici, juridici și reputaționali, iar incongruențele între aceste elemente constituie un risc major.

 **Indicatori tehnici:** utilizați doar site-uri cu conexiune criptată (https), verificați certificatul digital (emis de o autoritate recunoscută, numele domeniului corespunde mărcii), evitați domeniile cu substituții vizuale (ex.: rn în loc de m) sau extensii atipice pentru branduri consacrate.

Exemple: site-ul oficial al unei bănci ar trebui să fie pe domeniul băncii (ex.: banca.ro), nu pe subdomenii generice (ex.: banca-secure-pay.xyz).

 **Trasabilitate și conformitate:** existența unor politici clare de retur, termeni și condiții, identificare fiscală (CUI), adrese și canale de contact verificabile; pentru procesatorii de plăți, mențiuni privind conformitatea Payment Card Industry Data Security Standard (PCI DSS) și listarea publică a partenerilor (Visa, Mastercard).

Exemplu: platformele mari de e-commerce afișează politicile de protecție a cumpărătorului și procedurile de dispută.

 **Reputație și istoric:** consultați recenzii independente și scoruri pe multiple surse (ex.: Google Reviews, forumuri de consumatori, comparatoare de preț), cu atenție la conturile nou-înființate, recenzii identice sau excesiv de laudative postate într-un interval scurt.

Exemplu: un magazin apărut recent cu sute de recenzii aproape identice poate fi indiciu de manipulare.

 **Comportament la checkout:** site-urile legitime nu cer credențiale bancare complete prin e-mail/mesagerie; redirecționează către ferestre securizate ale procesatorului de plăți. Evitați formulare care solicită PIN, parole de internet banking sau coduri OTP pentru „verificare cont”.

 **Mediile de tranzacționare:** pe marketplace-uri, preferați plățile prin mecanisme de escrow/protecție cumpărător, evitați transferurile directe la presiunea vânzătorului („trimite banii prin link de curier”).

Exemple: fraudele „curierul” pe platforme de anunțuri folosesc linkuri false care imită pagini de plată.

7.2. Importanța protejării datelor personale și bancare

Datele personale și financiare au valoare economică directă pentru infractori, fiind utilizate pentru autentificări frauduloase, deschiderea de conturi, împrumuturi sau tranzacții neautorizate. Principiile de minimizare și control al difuzării datelor reduc suprafața de atac.

Minimizați divulgarea: nu partajați CNP, adresa completă, copii de acte sau IBAN în spații publice; furnizați doar datele strict necesare tranzacției. Exemplu: pentru livrare e suficientă adresa și telefonul curierului, nu și CNP-ul.

Segregați identitățile digitale: utilizați e-mailuri dedicate pentru plăți, aliasuri și numere virtuale acolo unde serviciul permite; limitați conectările prin conturi social media la comercianți necunoscuți (reduceți riscul de „account linking” abuziv).

Protejați datele cardului: preferați tokenizarea (Apple Pay/Google Wallet), carduri virtuale sau de unică folosință și limite de cheltuire. Exemplu: setați un card virtual cu plafon zilnic mic pentru abonamente online.

Gestionarea parolelor și a secretelor: folosiți un manager de parole, parole unice și complexe, activați autentificarea multifactor (MFA); nu stocați coduri 3D Secure/OTP în aplicații de notițe necriptate.

Controlul permisiunilor: acordați aplicațiilor bancare doar permisiunile necesare; fiți atenți la solicitări de acces la accesibilitate sau ecran, asociate cu troieni bancari.

Exemple: o aplicație de „scanare documente” care cere acces la SMS poate intercepta coduri OTP, solicitarea de a instala aplicații de remote control pe device pe motiv de acordare suport tehnic

Drepturi și protecție: cunoașteți drepturile GDPR (acces, ștergere) și politicile băncii privind răspunderea în caz de tranzacții neautorizate; raportați imediat breșele suspectate pentru a limita prejudiciul.

7.3. Semnale de alarmă (phishing, oferte false, investiții, aplicații periculoase)

Identificarea precoce a indicatorilor de fraudă reprezintă un element critic al igienei cibernetice, în special în contexte în care atacatorii mizează pe presiune temporală, autoritate aparentă și disimularea canalelor oficiale. Din perspectivă analitică, semnalele de alarmă pot fi grupate în patru categorii principale: (a) phishing/inginerie socială, (b) oferte comerciale nerealiste, (c) oportunități de investiții „garantate”, (d) aplicații malitioase. Fiecare categorie se caracterizează printr-un set recurent de indicatori tehnici și comportamentali.

Phishing / inginerie socială: apel la urgență („cont blocat”, „verificare imediată”), solicitarea datelor sensibile (PIN, parole, coduri 3D Secure/OTP), linkuri scurtate sau către domenii care imită brandul, atașamente executabile, spoofing de identitate (nume afișat sau Caller ID fals). Canalele folosite includ SMS, e-mail, mesagerie instant sau apeluri telefonice cu scenarii prestabilite

Oferte comerciale nerealiste: reduceri excesive, presiuni de tip „numai azi”, cerere de plată în afara platformei sau prin link necunoscut, lipsa politicilor de retur/protecție a cumpărătorului. Se exploatează în special marketplace-urile și rețelele sociale.

Investiții „garantate”: randamente fixe ridicate, lipsa riscului declarat, promisiuni de retrageri imediate, presiunea de a depune „taxe de deblocare” sau comisioane în avans; deseori implică criptomonede sau platforme nereglementate.

Aplicații periculoase: Android Package Kit (APK-uri) distribuite în afara magazinelor oficiale, aplicații care cer permisiuni necorelate (Accesibilitate, SMS, ecran), clone ale aplicațiilor bancare sau „actualizări” livrate prin link; includ și fleeceware (abonamente ascunse, costuri recurente greu de anulat).

Exemple de mesaje frauduloase (simulări educaționale)

Notă: exemplele de mai jos sunt fictive și oferite exclusiv în scop de instruire. Nu urmați astfel de instrucțiuni, nu accesați linkurile și nu divulgați date.

1. Pretins “de la bancă” – SMS de blocare cont

Text: [Banca]: Contul dvs. a fost SUSPENDAT pentru activitate neobișnuită. Verificați imediat datele: <https://banca-verificare-secure.com>

Semnale de alarmă

- Domeniu care nu corespunde domeniului oficial al băncii (formă compusă, cuvinte precum “secure”, “verify”).
- Apel la urgență + sancțiune iminentă.
- Solicitare de “verificare” ce va conduce la pagini care cer date de card sau coduri OTP.

Cum verificați?

- Intrați pe site-ul oficial al băncii sau sunați la numărul de pe site-ul oficial.
- Băncile nu cer niciodată PIN/OTP prin SMS sau linkuri.

2. Pretins „e-mail de securitate” al băncii – atașament malițios

Subiect: Acțiune necesară – extras PDF securizat

Conținut: Stimate client, pentru a preveni suspendarea internet banking-ului, deschideți documentul atașat “Extras_Securizat.zip” și urmați pașii.

Semnale de alarmă

- Atașament arhivă (zip/exe) – vector comun de malware.
- Limbaj generic (“Stimate client”), erori gramaticale fine, lipsa personalizării.
- Amenințare cu suspendarea serviciului.

Cum verificați?

- Băncile comunică în aplicație sau prin documente PDF semnate digital;
- Băncile nu trimit executabile și nu cer instalarea de “actualizări” prin e-mail.

3. Pretins apel telefonic „departament antifraudă” – inginerie socială

Script: “Sunt de la banca X. Observăm o plată de 2.350 lei către Y. Pentru a o anula, am nevoie să-mi dictați codul OTP primit acum pe telefon.”

Semnale de alarmă

- Solicitare de OTP/PIN/parolă la telefon – interzis în bunele practici.
- Presiune temporală (“acum, altfel plata se finalizează”).
- Caller ID poate fi falsificat (spoofing).

Cum verificați?

- închideți și apălați banca la numărul oficial;
- verificați în aplicația de mobile banking dacă există o tranzacție în curs;
- nu divulgați coduri.

4. Oferte false de pe marketplace – „curierul” și plata în afara platformei

Mesaj: “Sunt interesat, plătesc acum. Pentru siguranță, folosiți linkul oficial de curier: <https://livrare-verificata-pay.co> și introduceți datele cardului ca să primiți banii.”

Semnale de alarmă

- Solicitare de date de card “pentru a primi bani”.
- Link care imită pagini ale curierilor, fără conexiune cu platforma reală.

Cum verificați?

- folosiți doar fluxurile de plată ale platformei;
- pentru vânzări, nu se cer niciodată datele cardului pentru încasare.

5. Pretins „investitor/analist” – randamente garantate

Mesaj (WhatsApp/Telegram): “Suntem parteneri autorizați ai unei platforme europene. Profit garantat 12% pe lună, retrageri zilnice. Deschideți cont aici: <https://eu-invest-secure.net>. Pentru bonus, depuneți azi minim 500 EUR.”

Semnale de alarmă

- “Garantat” + randamente nerealiste,
- presiune de timp, bonus de înscriere.
- Domeniu obscur;
- lipsa licenței și a detaliilor privind entitatea juridică. Ulterior, pot solicita “taxe de retragere” – un semn clasic de scam.

Cum verificați?

- consultați registrul autorității de supraveghere (de ex., ASF/EBA/ESMA pentru entități licențiate);
- nu investiți prin linkuri primite pe chat.

6. Pretins „BNR” – solicitare de actualizare a datelor

SMS/e-mail: BNR: În contextul noilor reglementări, actualizați urgent datele de identitate pentru a evita blocarea conturilor: <https://bnr-verificare-id.eu>

Semnale de alarmă

- BNR nu contactează clienți bancari și nu colectează date personale pentru conturile acestora.
- Domeniu neoficial, formulare care solicită CNP, CI, selfie cu document/ card.

Cum verificați?

- ignorați, raportați mesajul băncii și autorităților;
- orice actualizare KYC se face prin banca unde aveți contul, pe canale oficiale.

7. Aplicație periculoasă – “actualizare bancă” prin APK

Mesaj (SMS/WhatsApp): “Actualizați aplicația bancară la versiunea de securitate 5.4. Descărcare: <http://banca-app-update.apk>”

Semnale de alarmă

- Distribuție în afara magazinului oficial (Google Play/App Store).
- Fișier APK și solicitări ulterioare de permisiuni la SMS/Accesibilitate.

Cum verificați?

- actualizați exclusiv din magazinele oficiale;
- dezinstalați aplicațiile necunoscute,
- rulați un scan și schimbați parolele dacă ați instalat astfel de fișiere.

8. „Informare” falsă despre securitatea depozitelor – abuz de autoritate publică

E-mail: “BNR anunță: din cauza instabilității, transferați economiile în contul de siguranță al programului național până la ora 18:00. IBAN: ROxx...”

Semnale de alarmă

- Autoritățile nu solicită transferuri către “conturi de siguranță”.
- Limbaj incitant la panică, termen-limită artificial.

Cum verificați?

- ignorați informarea și raportați băncii;
- consultați doar comunicatele de pe site-ul oficial al BNR și al băncii.

Recomandări operaționale de verificare

- **Verificarea sursei:** nu folosiți linkurile din mesaj; accesați manual site-ul oficial sau aplicația instalată din surse legitime. Confirmați telefonic la numărul oficial (din aplicație/site).
- **Analiza domeniului:** atenție la substituții vizuale (rn vs m), subdomenii lungi, TLD-uri neobișnuite; căutați certificat valid și identitatea organizației în certificat (EV/OV când disponibil).
- **Conținutul:** căutați greșeli gramaticale, formule generice, promisiuni nerealiste, solicitări de date sensibile sau plăți neobișnuite (vouchere, cripto, carduri cadou).
- **Tehnic:** nu deschideți atașamente .zip/.exe; nu instalați APK-uri; limitați permisiunile aplicațiilor; mențineți sistemul actualizat.
- **Proceduri post-incident:** dacă ați interacționat, deconectați dispozitivul de la internet, blocați cardul, schimbați parolele, activați scanarea antimalware, contactați banca și depuneți sesizare la Poliție/DNSC; păstrați dovezile (capturi, header-e, linkuri).

Încorporarea acestor semnale de alarmă în rutina utilizatorului – coroborată cu verificarea prin canale oficiale și cu prudență sporită față de mesaje care invocă autoritatea (banca, „investitori”, BNR) – reduce semnificativ expunerea la fraude și întărește reziliența individuală în mediul financiar digital.

7.4 Utilizarea metodelor sigure de plată și autentificare

Adoptarea consecventă a metodelor moderne de plată (tokenizare, carduri virtuale, 3DS2) și a autentificării rezistente la Phishing (Fast Identity Online / passkeys, semnare tranzacțională cu dynamic linking), dublată de controale operaționale (limite, alerte, geolocație) și disciplină digitală (dispozitive curate, parole unice), reduce semnificativ probabilitatea și impactul fraudelor.

Acest mix tehnologic și comportamental, aliniat cadrului normativ european, constituie fundamentul unei experiențe de plată online sigure și robuste. Selecția instrumentelor de plată și a mecanismelor de autentificare trebuie să echilibreze uzabilitatea cu cerințele de securitate (autentificare puternică a clientului, criptare, control tranzacțional).

Definiții esențiale

Autentificare multifactor (MFA): mecanism prin care identitatea utilizatorului este verificată folosind cel puțin doi factori din categorii diferite: cunoaștere (ce știe – parolă, PIN), posesie (ce are – telefon, token, cheie hardware) și inerent (ce este – biometrie).

Exemplu: confirmarea unei plăți în aplicația bancară prin amprentă (inerent) pe un telefon înregistrat (posesie).

Autentificare puternică a clientului (SCA, conform PSD2/PSR): tip particular de MFA aplicat plăților electronice în UE, care impune combinarea a cel puțin doi factori independenți și „dynamic linking” – legarea criptografică a autentificării de suma și beneficiarul tranzacției.

Exemplu: aprobarea unei plăți către IBAN specific, valoare 250 lei, vizibile în ecranul de autorizare.

3D Secure (versiunea 2.x): protocol de autentificare pentru plăți cu cardul pe internet, care permite „step-up” (autentificare suplimentară) la risc crescut și fluxuri mai ergonomice (ex. notificare push în aplicație). Înlocuiește parole statice cu autentificare contextuală.

Tokenizare: înlocuirea datelor sensibile (de ex. PAN – numărul cardului) cu un token (ex. DPAN pentru plăți mobile), inutilizabil în afara contextului propriu.

Exemplu: la Apple Pay/Google Wallet, comerciantul primește un token, nu numărul real de card.

Chei FIDO2 /WebAuthn (passkeys): metode de autentificare criptografică fără parolă, rezistente la phishing, bazate pe perechi cheie publică/privată stocate în dispozitiv sau chei hardware; confirmarea se face local (PIN/biometrie).

OTP (One-Time Password): coduri unice, cu valabilitate limitată, trimise prin SMS, generate în aplicații sau tokenuri. Sunt utile, dar mai vulnerabile la interceptare/ingenierie socială decât notificările push sau FIDO2.

Semnare tranzacțională: confirmarea unei tranzacții prin generarea unei semnături criptografice care include atributele esențiale (sumă, beneficiar). Implementări: TAN-uri dinamice, QR-TAN, challenge-response în aplicația băncii.

7.4.1 Metode de plată recomandate și controlul riscului

Carduri cu 3D Secure 2 și SCA: standardul minim pentru plăți online cu cardul în UE.

Exemplu: la checkout, sunteți redirectionat către o pagină de autorizare a băncii sau primiți o notificare push în aplicație pentru aprobare.

Portofele digitale cu tokenizare (Apple Pay, Google Wallet): reduc expunerea datelor de card; tranzacțiile sunt autorizate local (biometrie) și protejate de un „secure element”.

Exemplu: plata pe un site acceptat prin butonul „Pay with Apple Pay”.

Carduri virtuale și de unică folosință: generate din aplicația băncii/fintech-ului pentru abonamente sau comercianți noi; pot avea limite scăzute sau valabilitate limitată.

Exemplu: card virtual cu plafon de 100 lei pentru o singură achiziție.

Mecanisme escrow/protecție cumpărător: pe marketplace-uri consacrate, plata rămâne reținută până la confirmarea livrării; reduce riscul de neconformitate.

Exemplu: „Payments” ale platformei care permite deschiderea disputei și recuperarea sumelor.

Transferuri bancare cu verificare beneficiar (SANB): confirmați identitatea beneficiarului prin canal secundar; utilizați liste de „beneficiari de încredere” și verificări suplimentare (name check, acolo unde banca oferă).

Plăți instant (SEPA Instant) cu notificări: oferiți-vă alerte în timp real pentru a detecta imediat tranzacții neautorizate; pentru plăți P2P, confirmați verbal detaliile cu destinatarul.

Plăți prin coduri QR verificate: scanați doar coduri generate în aplicații oficiale (banca, comercianți certificați); vizualizați datele tranzacției (beneficiar, sumă) înainte de confirmare.

7.4.2 Practici de autentificare sigure și exemple concrete

Preferința pentru autentificare rezistentă la phishing

Alegeți passkeys/FIDO2 sau aprobări prin aplicația băncii cu afișarea clară a sumei și destinatarului. Exemplu:

- Cheie hardware (YubiKey) pentru login la fintech și semnare tranzacții
- Evitați OTP prin SMS când aveți opțiune de push/biometrie; OTP poate fi sustras prin SIM swapping sau malware care citește SMS-uri.

Izolarea dispozitivului de autorizare

- Nu folosiți dispozitive „rootate/jailbreak”; activați blocarea biometrică și criptarea.
- Separați profilul de utilizare pentru plăți de cel de test/aplicații neesențiale.

Dynamic linking și atenție la ecranul de autorizare

- Verificați suma și beneficiarul afișate în aplicație

Exemplu: dacă autorizați 2.500 lei către „SC EXEMPLE SRL” dar intenționați 250 lei către alt beneficiar, anulați imediat – e un semnal de redirectionare frauduloasă.

Politici de parole și manager dedicat

- Parole unice, lungi, generate în manager de parole;
- MFA activ pentru conturile de e-commerce și e-mail (piesa centrală a recuperării).
- Evitați reutilizarea parolelor între bancă și alte site-uri.

7.4.3 Configurări de control tranzacțional

Limite și geolocalizare

- Setati plafoane zilnice/săptămânale, dezactivați plățile online sau contactless când nu le folosiți;
- Blocați geografic tranzacții din regiuni unde nu operați.

Alerte și aprobări explicite

- Activați notificările push/SMS pentru fiecare plată;
- Cereți aprobare în aplicație pentru tranzacții peste un prag.

Liste albe/negre

- Utilizați liste de comercianți de încredere;
- Blocați comercianți recurenți nedorți sau MCC-uri specifice atunci când banca oferă această granularitate.

Monitorizare comportamentală și step-up

- Acceptați „challenge”-uri suplimentare atunci când banca detectează risc crescut (dispozitiv nou, locație neobișnuită); aceste controale vă protejează contul.

7.4.4 Scenarii uzuale și soluții

Cumpărături la comercianți noi

- Folosiți card virtual cu plafon mic + 3DS2;
- Verificați domeniul și certificatul site-ului. Dacă se solicită salvarea obligatorie a cardului, renunțați.

Abonamente și „free trial”

- Utilizați carduri dedicate sau tokenizate;
- Setări mementouri înainte de termenul de facturare;
- Verificați opțiunile de anulare în cont.

P2P și marketplace

- Folosiți măsurile pentru protecția cumpărătorului;
- Refuzați linkuri de plată trimise prin mesagerie;
- Nu introduceți datele cardului „ca să primiți banii”.

Plăți către entități „de investiții”

- confirmați licențierea pe registrele autorităților (ASF/ESMA/EBA);
- evitați transferuri în cripto la presiunea „consilierilor”.



7.4.5 Cele mai frecvente greșeli și cum pot fi evitate

Divulgarea codurilor OTP la telefon: „agentul antifraudă” cere OTP pentru anulare – este fraudă. **Banca nu solicită OTP/PIN/parole prin telefon sau chat.**

Instalarea de APK din linkuri: „actualizați aplicația băncii” prin WhatsApp – poate instala troieni bancari care interceptează SMS și suprapun ecrane.

Autorizarea în orb: aprobarea notificărilor push fără a citi detaliile tranzacției („push fatigue”). **Verificați întotdeauna suma/beneficiarul.**

Reutilizarea parolelor: compromiterea unui magazin online duce la „credential stuffing” pe e-mail și apoi pe contul bancar.

7.4.6 Proceduri de răspuns în caz de suspiciune

Blocați imediat instrumentul (card, portofel) din aplicația băncii; activați „freeze” temporar dacă nu sunteți sigur.

Contactați banca pe canalul oficial și raportați incidentul; solicitați contestarea plății (chargeback acolo unde se aplică).

Schimbați parolele, revocați sesiunile active, dezactivați dispozitive necunoscute din setările contului.

Notificați autoritățile competente (Poliție, DNSC) și păstrați probele (capturi de ecran, e-mailuri, URL-uri, loguri).

Concluzii

Educația financiară reprezintă o competență esențială pentru tineri. Este crucial ca inițiativele de educație financiară de calitate să fie introduse și menținute în momentele critice de tranziție ale tinerilor, să fie implementate la scară largă și sistematic, astfel încât cei care au nevoie de sprijin să aibă acces efectiv la el. Educația financiară trebuie să se bazeze pe dovezi și să fie orientată către tinerii care se află în situații de vulnerabilitate socio-economică.

Pe lângă competențele financiare, abilitățile digitale devin indispensabile pentru tineri, pentru a valorifica pe deplin oportunitățile oferite de tehnologie și pentru a minimiza riscurile asociate acestora. Educația digitală contribuie, totodată, la reducerea decalajelor digitale și la incluziunea socială și economică. Succesul educației financiare și digitale se sprijină pe competențe fundamentale, precum alfabetizarea și abilitățile socio-emoționale, care trebuie cultivate încă din primii ani de formare ai copiilor.

Totodată, educația financiară nu ar trebui să fie percepută doar ca un instrument de creștere a incluziunii financiare. În multe țări, lipsa accesului la servicii financiare nu reprezintă o problemă majoră pentru tineri, însă analfabetismul financiar rămâne o prioritate. În state cu piețe financiare dezvoltate, provocările pot fi legate de utilizarea ineficientă a produselor financiare mai costisitoare și cu risc mai mare de către tineri sau de dificultățile generațiilor mai tinere în gestionarea banilor, planificarea bugetului și economisirea pentru viitor. În astfel de contexte, educația financiară devine prioritatea principală, având un rol central în formarea unor obiceiuri financiare sănătoase, precum și a unei gândiri critice privind resursele economice.

Combaterea fraudelor digitale financiare reprezintă o prioritate strategică în România în contextul transformării digitale accelerate, iar educația financiară digitală joacă un rol central în acest proces. Conștientizarea riscurilor și dobândirea unor competențe digitale adecvate nu reduc doar vulnerabilitatea utilizatorilor în fața amenințărilor cibernetice, dar contribuie și la consolidarea încrederii în serviciile financiare online. Prin promovarea unei culturi a responsabilității și a vigilenței în mediul digital, societatea poate asigura un cadru sigur și incluziv pentru toți participanții la economia modernă, prevenind pierderile financiare și stimulând o utilizare sustenabilă a tehnologiilor financiare. Astfel, educația financiară digitală devine nu doar un instrument de protecție individuală, ci și un pilon al stabilității și rezilienței sistemului financiar în ansamblu.

Educația financiară reprezintă o competență esențială pentru tineri. Este crucial ca inițiativele de educație financiară de calitate să fie introduse și menținute în momentele critice de tranziție ale tinerilor, să fie implementate la scară largă și sistematic, astfel încât cei care au nevoie de sprijin să aibă acces efectiv la el. Educația financiară trebuie să se bazeze pe dovezi și să fie orientată către tinerii care se află în situații de vulnerabilitate socio-economică.

Bibliografie

- [1] Beetham, H. & Sharpe, R., 2019. An introduction to rethinking pedagogy. In: Rethinking pedagogy for a digital age. London: Routledge, pp.1-14.
- [2] Burns, T. & Gottschalk, F., 2019. Educating 21st Century Children: Emotional Well-Being in the Digital Age. Paris: OECD Publishing.
- [3] Furnham, A. & Fenton-O'Creevy, M.A.R.K., 2024. Money attitudes, budgeting and habits. *Journal of Financial Management, Markets and Institutions*, 12(02), p.2450001.
- [4] Gutierrez-Angel, N., Sanchez-Garcia, J.N., Mercader-Rubio, I., Garcia-Martin, J. & Brito-Costa, S., 2022. Digital literacy in the university setting: A literature review of empirical studies between 2010 and 2021. *Frontiers in Psychology*, 13, p.896800.
- [5] Johnson, E. & Sherraden, M.S., 2007. From financial literacy to financial capability among youth. *Journal of Sociology & Social Welfare*, 34, pp.119.
- [6] Kossev, K., 2020. OECD/INFE 2020 international survey of adult financial literacy.
- [7] Livingstone, S., Mascheroni, G. & Stoilova, M., 2023. The outcomes of gaining digital skills for young people's lives and wellbeing: A systematic evidence review. *New Media & Society*, 25(5), pp.1176-1202.
- [8] Obar, J.A. & Oeldorf-Hirsch, A., 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1), pp.128-147.
- [9] OECD, 2020. Advancing the digital financial inclusion of youth. Paris: OECD Publishing.
- [10] OECD, 2023. OECD Digital Education Outlook 2023. [online] Available at: https://www.oecd.org/en/publications/oecd-digital-education-outlook-2023_c74f03de-en/full-report.html
- [11] OECD, 2024. Shaping students' financial literacy. [online] Available at: https://www.oecd.org/en/publications/shaping-students-financial-literacy_c3f3dc74-en.html
- [12] Regulamentul (UE) 2022/2554 privind reziliența operațională digitală a sectorului financiar (DORA).
- [13] Strategia Națională de Educație Financiară – SNEF Romania 2024-2030. [online] Available at: https://www.edu.ro/sites/default/files/_fi%C8%99iere/Strategii/SNEF_2024_2030.pdf
- [14] Van Veldhoven, Z. & Vanthienen, J., 2022. Digital transformation as an interaction-driven perspective between business, society, and technology. *Electronic Markets*, 32(2), pp.629-644.

