

Document analitic

Minorii în Spațiul Digital: Diagnostic Legislativ și Opțiuni de Reglementare Aliniate la Standardele UE (DSA, GDPR, AI Act)

*[Minorul nu este nici pe departe doar vulnerabil, ci și titular activ de drepturi:
la informare, exprimare, educație, socializare, participare civică, etc.*

*Într-un spațiu digital în care copiii sunt deja prezenți, protecția nu trebuie să însemne
excludere, ci reguli care fac mediul online mai sigur și transparent.]*

Autori:

Andrei NASU
Iulian CIOBANU

Coordonator ediție:

Roman BANARI

Chișinău, iunie 2026

Pagină **1** din **82**

Cuprins

Termeni utilizați în studiu	4
Sumar executiv	6
Introducere și scopul analizei	9
Metodologia de lucru	10
Cadrul european relevant	11
Digital Services Act (DSA): protecția minorilor prin responsabilizarea platformelor	11
Regulamentul privind protecția datelor (GDPR): protecția copiilor și limitele verificării vârstei	13
Regulamentul privind inteligența artificială: interzicerea manipulării și exploatarei vulnerabilităților	15
Practica recentă de aplicare a DSA: teoria fără practică este inutilă	16
Concluzii intermediare: sinergia instrumentelor și relevanța pentru Republica Moldova	17
Diagnosticul cadrului normativ și instituțional al Republicii Moldova	18
Drepturile copilului ca temelie a sistemului	18
Conținutul dăunător: o reglementare construită pe o paradigmă învechită	19
Audiovizualul: protecție reală, dar într-un domeniu limitat	20
Protecția datelor cu caracter personal: un regim în tranziție	21
Serviciile societății informaționale: un cadru general util, dar insuficient	22
Protecția consumatorilor minori în mediul digital.....	23
Infracțiunile în mediul digital și violența digitală: un cadru recent consolidat	24
Comunicațiile electronice și securitatea cibernetică: o carcasă solidă pentru viitoarele politici	25
Reforme pendinte: transpunerea DSA și primele inițiative în materie de inteligență artificială	25
Cadrul instituțional și capacitatea de aplicare	27
Sinteza lacunelor sistemice și concluzie de diagnostic intern.....	28
Aspecte conceptuale: minorul - subiect vulnerabil, dar activ digital	30
Cine este „minorul”? O definiție în evoluție	30
Tabloul statistic privind prezența minorilor în spațiul digital	31
Vulnerabilitatea digitală: un risc sporit pentru minori	33
Drepturile copilului ca fundament transversal	34
Prevederile internaționale	34
Prevederile europene	35
Analiza comparativă a situației din alte țări	37

Franța și Danemarca: modelul hibrid, bazat pe praguri de vârstă, consimțământ parental și restricționare parțială	38
Germania și Irlanda: modelul non-prohibiționist, bazat pe responsabilizarea furnizorilor și supravegherea instituțională	42
Regatul Unit și Australia: modelul restrictiv, bazat pe interdicție generală	44
Concluzii comparative și relevanța pentru Republica Moldova	46
Evaluarea scenariilor de reglementare	47
Scenariul 1 – Model restrictiv: interdicția generală de acces sub 16 ani	47
Scenariul 2 – Model moderat: acces condiționat	51
Scenariul 3 – Model progresiv: responsabilizarea platformelor, fără interdicții pentru minori	53
În loc de concluzii: identificarea celui mai potrivit scenariu	56
 Recomandări	 58
1.Recomandări legislative pe termen scurt (0–12 luni)	58
2.Recomandări instituționale pe termen scurt (0–12 luni)	62
3.Recomandări legislative pe termen mediu (12–24 luni)	64
4.Recomandări instituționale pe termen mediu (12–24 luni)	65
5.Anexa 1 – Foaie de parcurs	1
6.Anexa 2 – Interviu de Feedback	4



Termeni utilizați în studiu

În scopul unei lecturi clare, prezentul studiu utilizează următorii termeni în sensul indicat mai jos. Definițiile au rol explicativ și nu înlocuiesc definițiile legale aplicabile, acolo unde acestea există.

Termen	Sens utilizat în studiu
Minor	Persoană care nu a împlinit vârsta de 18 ani. Termenul este folosit atât pentru copilul aflat în nevoie de protecție specială, cât și pentru titularul activ de drepturi în mediul digital.
Platformă digitală	Serviciu online care permite crearea de conturi, distribuirea de conținut, comunicarea, urmărirea altor utilizatori sau primirea de recomandări automatizate.
Rețea socială	Platformă digitală care permite crearea unui profil, interacțiunea cu alți utilizatori, publicarea sau distribuirea de conținut și accesul la fluxuri recomandate algoritmic.
Verificarea vârstei (Age verification)	Metodă mai strictă prin care platforma confirmă că utilizatorul a depășit un anumit prag de vârstă, de exemplu 13, 16 sau 18 ani. Poate implica document de identitate, portofel digital, confirmare de la un terț sau alt mecanism cu grad mai mare de certitudine.
Asigurarea vârstei (Age assurance)	Noțiune mai largă decât verificarea strictă a vârstei. Include metode prin care se estimează, confirmă sau gestionează probabilitatea ca un utilizator să aparțină unei categorii de vârstă.
Verificare proporțională a vârstei	Principiu potrivit căruia nivelul de verificare trebuie adaptat riscului serviciului sau funcționalității accesate. O platformă nu ar trebui să colecteze documente de identitate, date biometrice sau alte date sensibile dacă riscul poate fi gestionat prin metode mai puțin intruzive. De exemplu, pentru acces la o funcție de comentarii poate fi suficientă o setare de cont sau control parental, în timp ce pentru acces la conținut pentru adulți poate fi necesară o verificare mai robustă.
Dublu anonim	Arhitectură tehnică de verificare a vârstei care aplică principiul proporționalității: furnizorul de identitate confirmă doar îndeplinirea condiției de vârstă, fără să afle platforma accesată, iar platforma primește doar rezultatul verificării, fără să identifice utilizatorul. Exemplu: un serviciu confirmă doar „utilizatorul are peste 16 ani”, fără a transmite numele, CNP-ul, adresa sau copia actului de identitate.
Portofel digital de identitate	Instrument digital care poate permite dovedirea unor atribute, inclusiv vârsta sau depășirea unui prag de vârstă, fără transmiterea tuturor datelor de identitate către platformă.
EUDI Wallet	Portofelul european de identitate digitală. În acest studiu este relevant ca posibil reper tehnic pentru verificarea vârstei cu divulgare minimă de date.
Consimțământ parental	Acordul părintelui sau reprezentantului legal pentru accesul minorului la anumite servicii ori funcționalități digitale.

Control parental	Instrumente prin care părinții sau alți adulți responsabili pot limita, monitoriza sau ghida folosirea dispozitivelor, aplicațiilor și serviciilor digitale de către minori.
Siguranță prin proiectare (Safety by Design)	Integrarea protecției minorilor încă din etapa de proiectare a serviciului digital, nu doar prin măsuri reactive după producerea riscului. Exemple: cont privat implicit pentru minori, limitarea mesajelor de la adulți necunoscuți, dezactivarea recomandărilor agresive, buton vizibil de raportare.
Setări implicite de siguranță	Configurații aplicate automat conturilor minorilor, cum ar fi profil privat implicit, limitarea contactului din partea adulților necunoscuți sau reducerea recomandărilor nocive.
Profilare	Prelucrarea automată a datelor despre utilizator pentru a evalua sau anticipa comportamente, preferințe, interese ori vulnerabilități.
Publicitate bazată pe profilare	Publicitate personalizată în funcție de datele, comportamentul sau interesele estimate ale utilizatorului.
Sistem de recomandare	Sistem automatizat care selectează, ordonează sau promovează conținutul afișat utilizatorului.
Design manipulator	Mod de proiectare a interfeței sau a fluxului de utilizare care împinge utilizatorul spre decizii pe care nu le-ar lua în mod liber sau informat. Exemple: buton de acceptare foarte vizibil și opțiuni de refuz ascunsă, notificări repetate, fluxuri care fac greu de găsit setările de confidențialitate.
Conținut dăunător	Conținut care poate afecta dezvoltarea, siguranța, demnitatea sau bunăstarea minorilor, chiar dacă nu este întotdeauna ilegal. Spre exemplu provocări periculoase, conținut sexualizat, promovarea autovătămării, umilire publică, conținut violent sau materiale generate cu AI care imită persoane reale.
Grooming	Proces prin care o persoană manipulează treptat un minor, de regulă online, pentru a câștiga încrederea acestuia și a-l exploata sexual, emoțional sau în alte scopuri.
Deepfake	Conținut audio, video sau imagine generat ori modificat prin inteligență artificială pentru a crea impresia falsă că o persoană a spus sau a făcut ceva.
Eludarea interdicției	Ocolirea unei restricții de acces prin declararea unei vârste false, folosirea conturilor adulților, VPN-uri, conturi alternative, dispozitive partajate sau alte tehnici similare.
VPN	Serviciu care poate masca locația reală a utilizatorului și poate face mai dificilă aplicarea restricțiilor bazate pe teritoriu.
Raportare accesibilă copiilor	Mecanism simplu prin care copilul poate semnala o problemă. Exemplu: buton vizibil „Raportează”, limbaj clar, câțiva pași ușor de parcurs, confirmare că raportarea a fost primită și posibilitatea de a bloca imediat utilizatorul abuziv.

Coordonator al serviciilor digitale	Autoritate competentă responsabilă de supravegherea aplicării regimului privind serviciile digitale, inclusiv în raport cu obligațiile platformelor privind protecția minorilor.
DSA	Regulamentul privind serviciile digitale al Uniunii Europene. Relevant pentru obligațiile platformelor privind protecția minorilor, transparența, raportarea, sistemele de recomandare și reducerea riscurilor.
GDPR	Regulamentul general privind protecția datelor. Relevant pentru prelucrarea datelor personale, consimțământ, minimizarea datelor și protecția specială a copiilor.
AI Act	Regulamentul Uniunii Europene privind inteligența artificială. Relevant pentru interzicerea practicilor AI care exploatează vulnerabilitățile legate de vârstă și pentru reglementarea sistemelor AI cu impact asupra minorilor.

Sumar executiv

Prezentul studiu pornește de la o realitate care poate fi neglijată: minorii se află masiv și permanent în spațiul digital, în special pe rețele sociale, iar reglementarea nu vine să prevină un potențial acces, ci să structureze și să facă mai sigur un mediu în care copiii sunt deja actori activi.

Documentul nu susține nici interzicerea accesului minorilor la rețelele sociale, nici liberalizarea lui necondiționată. Rolul său este să clarifice ce soluții sunt proporționale, fezabile și compatibile cu parcursul european al Republicii Moldova. În calitate de stat candidat, cu negocierile de aderare formal deschise, țara și-a asumat alinierea legislației la acquis-ul comunitar, inclusiv în domeniul serviciilor digitale, al protecției datelor, al inteligenței artificiale și al drepturilor copilului.

În acest scop, studiul își propune să analizeze fezabilitatea și oportunitatea a trei scenarii de reglementare a accesului minorilor la rețelele sociale:

- i. scenariul restrictiv**, bazat pe interdicția generală de acces sub un anumit prag de vârstă;
- ii. scenariul moderat**, bazat pe acces condiționat, verificarea proporțională a vârstei, consimțământ parental și limitarea unor funcționalități cu risc; și
- iii. scenariul progresiv**, bazat pe responsabilizarea platformelor digitale, interzicerea profilării comerciale a minorilor, transparență algoritmică, siguranță prin design și supraveghere eficientă.

Analiza cadrului european arată că, carcasa pe care se sprijină siguranța minorilor în spațiul digital gravitează în jurul a trei acte: Regulamentul privind serviciile digitale (DSA), Regulamentul general privind protecția datelor (GDPR) și Regulamentul privind inteligența artificială (AI Act). Acestea conturează un model nuanțat de protecție, care nu se construiește prin excluderea copilului din mediul online, ci, în principal, prin responsabilizarea platformelor. Cadrul european pune accentul pe transparență algoritmică, interzicerea publicității bazate pe profilarea minorilor, siguranță prin proiectare și evaluarea riscurilor sistemice. Verificarea vârstei rămâne un instrument auxiliar, util doar dacă este proporțională și nu conduce la colectarea excesivă de date. La fel de importantă este aplicarea reală a acestor reguli, ilustrată de practica recentă a Comisiei Europene, care a constatat cu titlu preliminar că, algoritmi care creează dependență – încalcă principiile DSA. Lecția pentru Republica Moldova este că o protecție eficientă nu rezultă dintr-un singur amendament sau lege, ci din armonizarea coerentă a legislației, dublată de capacitatea reală a autorităților de supraveghere.

Diagnosticul cadrului normativ național poate fi rezumat printr-o metaforă: țara dispune de cărămizi, dar nu de o construcție. Drepturile copilului sunt protejate la nivel general, regimul protecției datelor personale este în proces de modernizare, audiovizualul are reguli solide, iar cadrul penal a fost recent consolidat, însă niciuna dintre aceste piese nu acoperă, singură, modul în care platformele digitale funcționează și îi afectează pe minori. Analiza identifică șapte lacune sistemice:

-  1) Legea privind drepturile copilului oferă un cadru general al drepturilor copilului, dar nu îl extinde explicit asupra mediului digital;
-  2) Legea privind protecția copiilor împotriva impactului negativ al informației operează cu logica filtrării conținutului dăunător, depășită în raport cu abordarea DSA;
-  3) Codul serviciilor media audiovizuale protejează minorii în audiovizual, dar nu acoperă rețelele sociale ca atare;
-  4) Regimul protecției datelor personale reglementează consimțământul minorului, dar nu și verificarea proporțională a vârstei sau accesul la platforme;
-  5) Legea serviciile societății informaționale (comerțul electronic) rămâne ancorată în logica clasică a comerțului electronic, fără a prelua logica DSA de responsabilizare a furnizorilor;
-  6) Protecția consumatorului-minor este acoperită generic de Legea privind protecția consumatorilor, care, deși aliniată standardelor UE, nu abordează separat protecția consumatorilor-minori;
-  7) Codul penal consolidat sancționează abuzul după producerea sa, dar nu acoperă partea preventivă.

Pe plan instituțional, nicio autoritate nu deține un mandat de supraveghere a platformelor comparabil cu cel al unui Coordonator al serviciilor digitale. Reforma aflată în curs, în special proiectul de lege privind serviciile digitale și primele inițiative în materie de inteligență artificială, răspunde în bună parte acestor lacune, dar se află într-un stadiu incipient și nu pare a fi construită specific în jurul protecției minorilor.

Din perspectivă conceptuală, minorul trebuie privit simultan ca subiect vulnerabil și ca actor activ digital, titular de drepturi. Vulnerabilitatea sa nu se reduce la lipsa de experiență, ci este amplificată de însuși modul în care sunt proiectate serviciile digitale, prin mecanisme de captare a atenției și personalizare algoritmică ce produc efecte mai intense asupra copiilor. De aceea, protecția nu se mai poate construi exclusiv pe educarea copilului, ci trebuie să se adreseze mediului însuși, prin echilibrarea designului platformelor, algoritmilor și modelelor comerciale. Drepturile copilului constituie fundamentul transversal al întregii analize și impun ca orice măsură de protecție să rămână proporțională, fără a se transforma în excludere sau cenzură. Protecția nu trebuie confundată cu restricția. Scopul reglementării nu trebuie să fie eliminarea copilului din spațiul digital, ci transformarea acestuia într-un mediu mai sigur, transparent, adecvat vârstei.

Perspectiva de gen arată că riscurile digitale nu se distribuie uniform între fete și băieți. Pentru Republica Moldova lipsesc încă date naționale privind minorii dezagregate pe sexe, ceea ce limitează măsurarea exactă a diferențelor de expunere și victimizare. Sursele analizate indică însă o expunere disproporționată a fetelor și adolescentelor la hărțuire sexistă, abuzuri sexualizate, distribuirea neconsensuală a imaginilor intime și materiale sexualizate de tip deepfake, precum și la presiunea legată de imaginea corporală. Pentru băieți, datele disponibile sunt mai fragmentare, dar semnalează vulnerabilități distincte, inclusiv în mediile de joc, în raportarea abuzurilor și în racolarea online pentru activități infracționale. Aceste diferențe confirmă necesitatea ca protecția minorilor în mediul digital să țină cont atât de vârstă, cât și de gen și să asigure o legătură funcțională între mecanismele de protecție a copilului și cele de prevenire și combatere a violenței împotriva femeilor și fetelor.

Analiza comparativă a șase state, grupate în trei modele de reglementare, confirmă că nu există o soluție unică care poate fi transpusă mecanic. Modelul hibrid (Franța, Danemarca) folosește praguri de vârstă și

consimțământ parental. Modelul non-prohibiționist (Germania, Irlanda) mizează pe responsabilizarea furnizorilor și supraveghere instituțională. Modelul restrictiv (Regatul Unit, Australia) recurge la interdicția generală. Un reper rămâne constant: la data analizei, niciun stat membru al Uniunii Europene nu a adoptat o interdicție totală și operațională a accesului minorilor la rețelele sociale.

Din experiența comparată se desprind trei lecții: (i) orice soluție întemeiată pe vârstă depinde de o verificare proporțională și sigură a vârstei; (ii) responsabilitatea nu poate fi transferată exclusiv părinților și copiilor, întrucât platformele controlează arhitectura serviciilor, ceea ce face siguranța prin proiectare indispensabilă; (iii) iar instituțiile contează la fel de mult ca regulile. Datele statistice din Australia arată, în plus, cât de ușor poate fi eludată o interdicție generală în absența unor mecanisme solide de aplicare.

Pe baza acestor constatări, **studiul evaluează cele trei scenarii** și conchide că scenariul restrictiv nu este, pentru Republica Moldova, nici opozabil, nici eficace. Experiența franceză cu o lege adoptată în 2023, dar rămasă neoperaționalizată din cauza conflictului cu DSA și cu principiul țării de origine, precum și jurisprudența recentă a Curții de Justiție a Uniunii Europene, potrivit căreia un stat nu poate impune furnizorilor stabiliți în alt stat o obligație generală și abstractă, fiind posibilă o derogare individualizată doar în condiții stricte, confirmă fragilitatea juridică a interdicției generale. Scenariile moderat și progresiv, în schimb, operează în interiorul logicii europene și se dovedesc complementare. Concluzia analizei este că opțiunea opozabilă și adecvată pentru Republica Moldova constă într-o simbioză între modelul progresiv, care construiește coloana structurală de tip DSA dublată de o autoritate de supraveghere cu capacitate reală, și modelul moderat, care adaugă pe acest fundament garanții proporționale de acces. Limitarea accesului sub un anumit prag de vârstă (de exemplu, 16 ani) ar trebui analizată doar ca ipoteză strict condiționată și suplimentară, în cazuri strict necesare, dar nu ca o soluție implicită.

Pornind de la aceste concluzii, studiul formulează nouăsprezece recomandări, grupate în patru blocuri după termen și natură. Direcția generală este responsabilizarea platformelor, alinierea la DSA, GDPR și AI Act, consolidarea autorităților competente și introducerea unor mecanisme proporționale de verificare a vârstei, control parental și raportare, printr-o intervenție graduală. Pe termen scurt, recomandările legislative vizează accelerarea adoptării proiectului de lege privind serviciile digitale și a viitorului cadru privind inteligența artificială, cu integrarea protecției minorilor încă din faza de proiectare; completarea Legii privind drepturile copilului cu dimensiunea digitală și consacrarea verificării proporționale a vârstei pe principiul „dublului anonim”. Recomandările instituționale pe termen scurt urmăresc consolidarea unui Coordonator național al serviciilor digitale funcțional, cu o linie de lucru dedicată protecției minorilor, cooperarea interinstituțională permanentă, implicarea altor autorități și consultarea structurată a tinerilor.

Pe termen mediu, prioritățile privesc modernizarea legislației privind protecția copiilor împotriva impactului negativ al informației, delimitarea competențelor între audiovizual, platforme video și servicii digitale, protecția consumatorului-minor, corelarea cadrului penal cu mecanismele preventive, dezvoltarea capacității tehnice a autorităților și integrarea educației digitale în programele școlare. Dimensiunea de gen este tratată transversal, fiind integrată în colectarea dezagregată a datelor, mecanismele de raportare, formarea specialiștilor și evaluarea riscurilor, în special în raport cu violența digitală care afectează disproporționat fetele și tinerele.

În concluzie, protecția minorilor în spațiul digital poate și trebuie realizată fără a le limita disproporționat dreptul la informare, exprimare, educație, socializare și participare civică. Pentru Republica Moldova, **simbioza dintre modelul progresiv și cel moderat** reprezintă opțiunea proporțională, opozabilă și compatibilă cu parcursul european, întrucât marja reală de manevră a unui stat candidat nu constă în construirea unor soluții divergente, ci în adoptarea standardelor și procedurilor definite la nivel european. În

special, având în vedere potențialul redus al Republicii Moldova de a influența marile platformele transatlantice („Big Tech”), alinierea la standardele și mecanismele europene rămâne a fi unica opțiune sustenabilă. Soluția potrivită nu este nici inacțiunea, nici interdicția generală, ci un cadru coerent care se aliniază la standardele europene, care tind să responsabilizeze platformele, să capaciteze autoritățile și să păstreze copilul în centrul protecției, ca titular de drepturi, iar nu ca simplu obiect al acesteia.

Introducere și scopul analizei

Prezentul studiu are caracter aplicat și urmărește să ofere factorilor de decizie, instituțiilor de reglementare, organizațiilor de tineret și societății civile o bază analitică echilibrată pentru reglementarea siguranței minorilor în spațiul digital. Studiul nu pornește de la ideea că accesul minorilor la rețelele sociale trebuie interzis sau liberalizat fără condiții. Punctul de plecare este diferit: minorii sunt deja prezenți masiv în mediul digital, iar statul trebuie să stabilească un cadru normativ care reduce riscurile reale, fără a limita disproporționat dreptul copiilor la informare, exprimare, educație, socializare și participare civică.

Contextul actual este important. Republica Moldova a obținut statutul de țară candidată la aderarea la Uniunea Europeană în iunie 2022, iar deschiderea negocierilor de aderare, în iunie 2024, a transformat alinierea legislativă la *acquis-ul comunitar* într-o obligație practică, nu doar într-un obiectiv politic. Această obligație privește inclusiv domeniul serviciilor digitale, protecția datelor personale, inteligența artificială, mass-media, drepturile copilului și combaterea abuzurilor online.

În paralel, atât în spațiul public european, cât și cel din Republica Moldova, se discută tot mai des ideea restricționării accesului minorilor sub 16 ani la rețelele sociale. Preocuparea este legitimă și stringentă. Totuși, o asemenea opțiune nu poate fi tratată izolat, fără analizarea compatibilității cu reglementările europene, drepturile copilului și capacitatea tehnică reală de aplicare. Rolul documentului nu este de a promova o interdicție sau de a respinge orice intervenție, ci de a clarifica ce soluții sunt proporționale, fezabile și compatibile cu parcursul european al Republicii Moldova.

Miza abordată în această analiză se reflectă direct în Programul național de aderare a Republicii Moldova la Uniunea Europeană 2025–2029, adoptat prin Hotărârea Guvernului nr. 306/2025. Activitățile relevante temei studiului sunt concentrate pentru anii 2025–2027. Capitolul 10 „Societatea informațională și mass-media”, din Clusterul 3, include transpunerea Regulamentului (UE) 2022/2065 privind serviciile digitale, prin proiectul de lege privind serviciile digitale, cu termen de adoptare planificat pentru octombrie 2026. În acest cadru, Programul prevede desemnarea ANRCETI (în prezent ARCOM) în calitate de Coordonator al serviciilor digitale și consolidarea capacității sale instituționale, inclusiv prin crearea unei subdiviziuni dedicate supravegherii serviciilor societății informaționale și coordonării serviciilor digitale, fiind planificat în acest sens alocarea unui buget estimat de 5,2 milioane lei. Consiliul Audiovizualului urmează să fie autoritate competentă pentru serviciile de platformă de partajare a materialelor video.

Capitolul 10 include și alinierea la Regulamentul (UE) 2024/1689 privind inteligența artificială, prin elaborarea unei legi naționale privind inteligența artificială, cu termen de adoptare planificat pentru decembrie 2026. Această direcție este relevantă pentru minori deoarece sistemele de recomandare, moderarea automată, publicitatea personalizată, conținutul generat artificial și interacțiunile automate pot exploata vulnerabilitățile legate de vârstă. Din această perspectivă, studiul ridică întrebarea dacă viitorul cadru privind inteligența artificială va integra suficient protecția copilului sau va rămâne axat preponderent pe inovare, economie digitală și guvernanta datelor.

O componentă distinctă este protecția minorilor pe platformele video și pe rețelele sociale utilizate pentru distribuirea de conținut audiovizual. Aceasta se intersectează cu Codul serviciilor media audiovizuale, Legea

nr. 30/2013 privind protecția copiilor împotriva impactului negativ al informației și viitorul cadru privind serviciile digitale. Programul național de aderare stabilește măsuri privind introducerea mecanismelor de verificare a vârstei pe platformele digitale, obligarea furnizorilor de platforme de partajare video de a implementa măsuri pentru protejarea minorilor de pornografie sau violență, limitarea comunicărilor comerciale dăunătoare, mecanismele de raportare și delimitarea competențelor autorități.

Complementar, Capitolul 24 „Justiție, libertate și securitate”, din Clusterul 1, tratează protecția copiilor împotriva abuzului sexual, inclusiv online. Programul național de aderare include modificări legislative pentru alinierea la *Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor, a exploatarei sexuale a copiilor și a pornografiei infantile*, transpunerea instrumentelor europene privind detectarea abuzului sexual online asupra copiilor, precum și măsuri operaționale privind investigarea cazurilor, sistarea accesului la pagini web cu conținut de abuz sexual și dezvoltarea serviciilor integrate pentru copiii victime. Această dimensiune este importantă pentru studiu deoarece dreptul penal sancționează formele grave de abuz, dar prevenirea efectivă depinde și de obligațiile platformelor, de raportare, moderare, reacție rapidă și cooperare cu autoritățile.

Astfel, studiul își propune să stabilească în ce măsură activitățile legate de protecția și siguranța minorilor în spațiul digital, propuse de decidenți în drumul Republicii Moldova spre aderarea europeană, au fost deja realizate și cât de suficiente sau opozabile sunt acestea.

Metodologia de lucru

Metodologic, studiul combină patru componente. Prima este analiza juridică a cadrului european și național relevant, cu accent pe lacunele de compatibilitate și pe capacitatea reală de aplicare a normelor. A doua este analiza comparativă a modelelor din alte state, utilizate nu ca soluții de copiat, ci ca repere pentru înțelegerea avantajelor și riscurilor diferitelor opțiuni de reglementare. A treia este analiza aspectelor conceptuale cu privire la copii și drepturile fundamentale ale acestora. Iar cea de-a patra componentă vizează evaluarea scenariilor de reglementare posibile pentru Republica Moldova (modelul restrictiv; modelul moderat; modelul progresiv) și selectarea celui mai potrivit.

Studiul a fost elaborat prin conlucrarea a doi experți cu roluri complementare. Expertul juridic a coordonat arhitectura analitică a raportului, analiza cadrului european și național, evaluarea juridică a scenariilor, identificarea lacunelor legislative și formularea recomandărilor. Expertul tehnic a evaluat fezabilitatea soluțiilor propuse, în special mecanismele de verificare a vârstei, riscurile de securitate cibernetică, protecția datelor minorilor, verificarea biometrică, blocarea accesului, sistemele de recomandare, auditul algoritmic și cerințele tehnice minime pentru platforme. Recomandările cu impact tehnic au fost formulate numai în măsura în care au putut fi verificate din perspectiva implementării practice și a riscurilor suplimentare pentru minori.

Scenariile au fost evaluate după aceleași criterii: compatibilitatea cu normele europene, respectarea drepturilor copilului, impactul asupra siguranței minorilor, protecția datelor, fezabilitatea tehnică, riscurile de securitate cibernetică, capacitatea instituțională, efectele asupra participării tinerilor și, transversal, dimensiunea de gen. Abordarea utilizată a urmărit să evite concluziile prestabilite și să permită factorilor de decizie să urmărească raționamentul de la diagnostic până la recomandare.

Studiul are limite asumate. Acesta nu include audituri tehnice ale algoritmilor platformelor și nu poate verifica direct funcționarea internă a sistemelor de recomandare, moderare sau verificare a vârstei. Din acest motiv, analiza se bazează pe surse oficiale, documente europene, legislație națională, proiecte aflate în lucru,

cercetări disponibile și evaluarea juridico-tehnică a experților. Acolo unde măsurile sunt încă la nivel de proiect sau inițiativă anunțată, ele sunt tratate ca atare, nu ca reglementări aplicabile.

Cadrul european relevant

Înțelegerea opțiunilor de reglementare a accesului minorilor în spațiul digital relevante pentru Republica Moldova nu poate fi efectuată prin ignorarea cadrului normativ european, care reprezintă, în același timp, standardul de compatibilitate impus de procesul de aderare la Uniunea Europeană și sursa celor mai avansate instrumente juridice existente astăzi pentru protecția minorilor în mediul online. Abordarea europeană privind siguranța minorilor în spațiul digital nu este construită în jurul unui singur act normativ. Aceasta funcționează ca o arhitectură compusă din mai multe instrumente juridice și de politici publice, care se completează reciproc.

Trei regulamente europene formează nucleul dur al cadrului european relevant analizei:

- I. Regulamentul privind serviciile digitale (DSA);**
- II. Regulamentul general privind protecția datelor (GDPR);**
- III. Regulamentul privind inteligența artificială (AI Act).**

Deși adoptate în momente diferite și cu finalități distincte, cele trei regulamente se completează reciproc, acoperind în mod diferit riscuri similare la care sunt expuși minorii în spațiul digital.

Regulamentele prenotate urmează a fi aplicate în coroborare cu alte acte normative sau cadru normativ subsidiar relevant (*soft law*), precum: Carta drepturilor fundamentale a Uniunii Europene, Strategia *Better Internet for Kids Plus* BIK+, Convenția ONU privind drepturile copilului, Convenției privind protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale (Convenția de la Lanzarote), Convenția privind criminalitatea informatică (Convenția de la Budapesta), Convenția-cadru privind AI, drepturile omului, democrația și statul de drept, etc.

Pentru Republica Moldova, acest cadru are o relevanță specială. În prezent, actele UE nu se aplică direct în același mod ca într-un stat membru. Totuși, ele reprezintă reperul principal de compatibilitate în procesul de aderare la Uniunea Europeană.

Orice reglementare națională privind accesul minorilor la platformele digitale trebuie evaluată printr-un raportare la aceste standarde. O soluție națională pripită, dar incompatibilă cu DSA, GDPR, AI Act, sau altele acte relevante, ar risca să fie revizuită ulterior în procesul de armonizare legislativă.

Digital Services Act (DSA): protecția minorilor prin responsabilizarea platformelor

DSA¹ este cel mai important instrument european pentru reglementarea platformelor online. Logica sa nu este de a interzice accesul utilizatorilor la servicii digitale, ci de a impune obligații clare furnizorilor care controlează infrastructura digitală. Această abordare este esențială pentru tema prezentului studiu, deoarece multe riscuri pentru minori apar din modul în care platformele sunt proiectate, monetizează atenția, folosesc datele personale și recomandă conținut.

Articolul 28 din DSA impune platformelor online accesibile minorilor obligația de a adopta măsuri adecvate și proporționale pentru a asigura un nivel ridicat de confidențialitate, siguranță și securitate pentru minori.

¹ Parlamentul European și Consiliul, *Regulamentul (UE) 2022/2065 din 19 octombrie 2022 privind o piață unică pentru serviciile digitale (Regulamentul privind serviciile digitale / DSA)*, JO L 277, 27.10.2022, disponibil online: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

Același articol, la alineatul (2), interzice platformelor să prezinte publicitate bazată pe profilare, adică pe analiza comportamentului online al utilizatorului pentru a-i construi un profil și a-i adresa reclame personalizate, atunci când platforma știe, cu o certitudine rezonabilă, că destinatarul serviciului este minor. Această interdicție elimină practic una dintre cele mai profitabile practici comerciale ale platformelor de socializare, și anume oferirea de reclamă țintită personal. Această normă are efecte imediate pentru platformele cu milioane de utilizatori europeni și este unul dintre cele mai clare standarde europene: **minorii**

nu trebuie transformați în ținte comerciale prin profilare comportamentală.

Formularea articolului 28 este deliberat flexibilă, legiuitorul european a preferat o abordare bazată pe risc și proporționalitate față de soluții uniforme și rigide, tocmai pentru a permite adaptarea obligațiilor la natura diversă a platformelor digitale. Alineatul (3) al aceluiași articol precizează că respectarea obligațiilor derivate din acest articol nu impune platformelor să prelucreze date cu caracter personal suplimentare pentru a evalua dacă destinatarul serviciului este minor. Acesta este o garanție care previne ca protecția copilului să devină un pretext pentru colectarea excesivă de date și informații despre utilizatori.

DSA obligă, prin articolul 14 alineatul (3), furnizorii de servicii intermediare să ofere utilizatorilor informații clare și accesibile despre condițiile de utilizare a serviciilor. Dacă serviciul este destinat în principal minorilor sau este folosit predominant de aceștia, condițiile și restricțiile trebuie explicate într-un limbaj pe care minorii îl pot înțelege. Astfel, furnizorul nu trebuie doar să informeze utilizatorii, ci să o facă într-un mod simplu, adecvat vârstei și ușor de perceput de către minori.

O altă linie de protecție oferită de DSA vizează designul manipulator al interfețelor, denumit de către specialiștii – *dark patterns*, adică modele înșelătoare de design. Articolul 25 interzice furnizorilor de platforme online să proiecteze, să organizeze sau să exploateze interfețele lor online într-un mod care înșală sau manipulează utilizatorii ori care le afectează semnificativ capacitatea de a lua decizii libere și în cunoștință de cauză. Concret, această interdicție acoperă practici nocive frecvent întâlnite în rândul marilor platforme:

-  ordinea și modul mai avantajos de afișare a butoanelor de acceptare față de cele de refuz;
-  obstacolele nejustificate puse în calea ștergerii unui cont sau a exercitării unui drept;
-  asimetria vizuală deliberată între opțiuni, în avantajul platformelor.

Pentru minori, aceste practici sunt cu atât mai periculoase, cu cât capacitatea lor de evaluare critică a interfețelor digitale este, prin natura vârstei, mai redusă.

DSA introduce și obligații privind transparența sistemelor de recomandare algoritmică, adică a mecanismelor prin care platformele decid ce conținut apare în feed-ul (fluxul postărilor) utilizatorului. Prin articolul 27, platformele trebuie să prezinte utilizatorilor, într-un limbaj simplu, principalii parametri ai sistemelor lor de recomandare și să le ofere posibilitatea de a le influența.

Platformele online foarte mari (*Very Large Online Platform, VLOP*) și motoarelor de căutare foarte mari (*Very Large Online Search Engine, VLOSE*), adică cele cu peste 45 de milioane de utilizatori activi lunari în Uniunea Europeană, așa cum este prevăzut de articolul 33 alineatul (1) DSA, sunt supuse mai multor obligații suplimentare. Articolului 38 impune obligația de a oferi cel puțin o opțiune de recomandare care să nu se bazeze pe profilarea utilizatorilor. Aceasta este o măsură cu relevanță directă pentru minori, întrucât sistemele algoritmice de recomandare sunt principalul mecanism prin care platformele amplifică expunerea copiilor la conținut potențial dăunător.

Un set distinct de obligații, aplicabil exclusiv platformelor online și motoarelor de căutare foarte mari, sunt prevăzute la articolele 34 și 35 ale DSA. Acestea privesc evaluarea și atenuarea riscurilor sistemice.

Platformele date trebuie să identifice și să analizeze periodic orice riscuri semnificative generate de funcționarea și utilizarea serviciilor lor, inclusiv efectele negative asupra minorilor, și să adopte măsuri rezonabile și proporționale de atenuare a acestora. Riscurile avute în vedere explicit de DSA includ comportamentele adictive generate de designul platformei, cunoscute și sub denumirea de efectul *rabbit hole*, adică tendința algoritmilor de a propulsa utilizatorul spre conținut din ce în ce mai captivant sau mai radical. Totodată, riscurile se referă la efectele negative asupra bunăstării fizice și mentale a utilizatorilor, precum și riscurile specifice legate de violența de gen în mediul digital.

În final, conchidem că, protecția minorilor prin DSA este tratată ca o obligație transversală pentru furnizorii de servicii digitale, în special pentru platformele online accesibile copiilor.

- ✓ Articolul 14, susținut de considerentul (46), stabilesc că furnizorii de servicii intermediare destinate în principal minorilor sau utilizate predominant de aceștia trebuie să explice condițiile generale de utilizare într-un mod ușor de înțeles pentru copii.
- ✓ Articolul 28, susținut de considerentul (71), stabilesc că protecția minorilor este un obiectiv important al Uniunii Europene. Platformele online utilizate de minori trebuie să adopte măsuri adecvate și proporționale, inclusiv interfețe mai sigure, protecție implicită a confidențialității și standarde sau coduri de conduită pentru protecția minorilor. Același considerent interzice publicitatea bazată pe profilare atunci când platforma știe cu un grad rezonabil de certitudine că utilizatorul este minor.
- ✓ Articolul 34, susținut de considerentul (80), includ în categoria riscurilor sistemice diseminarea de conținut ilegal, inclusiv materiale care conțin abuzuri sexuale asupra copiilor, sau care afectează drepturile fundamentale. Acest risc trebuie evaluat în special de platformele online și motoarele de căutare foarte mari.
- ✓ Articolul 35, susținut de considerentul (81) cere acestor platforme să evalueze impactul serviciilor asupra drepturilor fundamentale, inclusiv drepturile copilului. Evaluarea trebuie să ia în calcul cât de ușor pot minorii înțelege funcționarea serviciului și dacă pot fi expuși la conținut care le afectează sănătatea sau dezvoltarea fizică, mentală și morală. Sunt vizate inclusiv interfețele care exploatează vulnerabilitățile minorilor sau pot crea dependență.
- ✓ Articolul 25, susținut de considerentul (83), completează această abordare prin includerea riscurilor asupra protecției minorilor și asupra bunăstării fizice și psihice a persoanelor, inclusiv riscurile generate de manipulare, dezinformare sau interfețe care pot stimula dependențe comportamentale.

Prin urmare, DSA nu tratează protecția minorilor doar ca obligație de informare, ci ca obligație de proiectare, evaluare și prevenire a riscurilor. Accentul cade pe limbaj accesibil, transparență, confidențialitatea datelor, siguranță, interzicerea profilării publicitare a copiilor, precum și evaluarea și atenuarea riscurilor sistemice pentru drepturile și bunăstarea copiilor.

Regulamentul privind protecția datelor (GDPR): protecția copiilor și limitele verificării vârstei

GDPR² este un alt pilon fundamental al cadrului european, care asigură protecția minorilor în spațiu digital. Relevanța sa derivă din faptul că aproape toate platformele digitale funcționează prin colectarea, analizarea și monetizarea datelor utilizatorilor. În cazul minorilor, această realitate ridică riscuri sporite, precum:

² Parlamentul European și Consiliul, *Regulamentul (UE) 2016/679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor / GDPR)*, JO L 119, 4.5.2016, disponibil online: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

profilare comercială, publicitate personalizată, urmărirea comportamentului online, inferențe despre interese, sănătate, vulnerabilități, stare emoțională.

GDPR reglementează dreptul fundamental la protecția datelor personale și constituie fundamentul juridic pe care se construiesc celelalte instrumente sectoriale din domeniul digital.

Articolul 8 din GDPR stabilește regulile privind consimțământul digital al copilului în relație cu serviciile societății informaționale, adică serviciile online furnizate contra cost sau gratuit, inclusiv platformele de socializare, aplicațiile de mesagerie sau jocurile online. Regula generală este că prelucrarea datelor unui copil pe baza consimțământului este legală doar dacă acesta are cel puțin 16 ani. Sub această vârstă, prelucrarea este legală numai dacă consimțământul este dat sau autorizat de titularul răspunderii părintești. GDPR permite statelor membre să coboare pragul de la 16 la 13 ani, dar nu sub această limită minimă. Această marjă de apreciere națională a generat o anumită fragmentare în Uniunea Europeană, deoarece unele state membre au menținut pragul de 16 ani, altele l-au stabilit la 14 sau 13 ani. Această diferențiere a ridicat probleme practice semnificative pentru platformele care operează la nivel paneuropean, pe motiv că trebuie să gestioneze reguli diferite pentru utilizatorii din state membre diferite.

Totuși, GDPR nu trebuie interpretat simplist. Articolul 8 nu oferă, singur, o soluție completă pentru accesul minorilor la platforme. Pe lângă regula consimțământului, GDPR include mai multe prevederi care reflectă preocuparea specifică pentru protecția datelor copilului. Considerentul 38 recunoaște că minorii au nevoie de o protecție specifică, întrucât pot fi mai puțin conștienți de riscurile, consecințele și garanțiile legate de prelucrarea datelor lor, în special în scopuri de marketing și creare de profiluri. Considerentul 71, la rândul său, precizează că procesul decizional automatizat nu ar trebui să se refere la copii, ceea ce limitează semnificativ aplicabilitatea profilării algoritmice în privința minorilor. Deși aceste texte nu au forță juridică egală cu dispozițiile articolelor propriu-zise, ele orientează interpretarea sistematică a regulamentului și sunt invocate în mod constant de autoritățile de supraveghere și în jurisprudență.

Articolul 12 din GDPR prevede obligația generală de transparență, impunând furnizorilor de servicii să ofere informațiile privind prelucrarea datelor într-o formă concisă, transparentă, inteligibilă și ușor accesibilă. În cazul minorilor, această cerință se traduce în obligația de a folosi un limbaj adaptat capacității lor de înțelegere. Aceasta este exact logica pe care o urmăresc și Orientările Comisiei din 14 iulie 2025³ în privința DSA, cerând platformelor să redacteze termenii și condițiile de utilizare într-un limbaj accesibil minorilor.

O problemă centrală pentru orice reglementare națională privind accesul minorilor la platforme este **verificarea vârstei**. Din perspectiva GDPR, verificarea vârstei nu poate justifica orice formă de colectare a datelor. O soluție care cere, în mod general, acte de identitate, date biometrice sau imagini faciale ale minorilor poate crea riscuri mai mari decât cele pe care încearcă să le prevină.

O contribuție importantă la clarificarea standardelor aplicabile pentru prelucrarea datelor minorilor o aduce Declarația 1/2025 privind asigurarea vârstei (*age assurance*)⁴, adoptată de Comitetul European pentru Protecția Datelor (EDPB) la 11 februarie 2025. Documentul stabilește zece principii pentru prelucrarea conformă a datelor cu caracter personal în contextul determinării vârstei sau a intervalului de vârstă al unui

³ Comisia Europeană, *Orientări din 14 iulie 2025 privind măsurile de asigurare a unui nivel ridicat de confidențialitate, siguranță și securitate pentru minori în mediul online, în temeiul articolului 28 alineatul (4) din Regulamentul (UE) 2022/2065*, JO C, C/2025/5519, 10.10.2025, disponibil online: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=OJ%3AC_202505519.

⁴ Comitetul European pentru Protecția Datelor (EDPB), Declarația 1/2025 privind asigurarea vârstei, adoptată la 11 februarie 2025, disponibil online: https://www.edpb.europa.eu/system/files/2025-07/edpb_statement_20250211ageassurance_ro.pdf.

utilizator. Acesta avertizează explicit împotriva soluțiilor tehnice excesive sau disproporționate, cum ar fi colectarea sistematică a actelor de identitate sau a datelor biometrice ale tuturor utilizatorilor, și solicită o evaluare riguroasă a impactului oricărei metode de verificare a vârstei asupra protecției datelor. Concluzia esențială a declarației este că verificarea vârstei este un instrument necesar pentru protecția minorilor, dar nu poate fi realizată cu orice cost. Metodele utilizate trebuie să fie:

- ✓ proporționale și cât mai puțin intruzive posibil;
- ✓ să respecte principiul minimizării datelor (adică să colecteze strict datele necesare scopului urmărit);
- ✓ să evite utilizarea datelor în scopuri secundare și să prevină discriminarea / excluderea nejustificată;
- ✓ să nu devină ele însele o sursă de riscuri suplimentare pentru confidențialitatea și securitatea utilizatorilor.

Pentru Republica Moldova, acest aspect este crucial. **Orice scenariu de acces condiționat trebuie să fie analizat nu doar juridic, ci și tehnic.** Verificarea vârstei poate fi necesară în anumite situații, dar nu trebuie transformată într-un mecanism de supraveghere generalizată a utilizatorilor. Soluția compatibilă cu standardele europene trebuie să fie proporțională cu riscul, să protejeze identitatea minorului și să evite colectarea excesivă și generală a datelor personale.

Regulamentul privind inteligența artificială (AI Act): interzicerea manipulării și exploatării vulnerabilităților

AI Act⁵ completează DSA și GDPR printr-o abordare bazată pe evaluarea nivelului de risc al sistemelor de inteligență artificială. Regulamentul nu este destinat exclusiv protecției minorilor, dar include garanții importante pentru copii și adolescenți. În special, el interzice anumite practici considerate incompatibile cu drepturile fundamentale și cu autonomia persoanei.

AI Act, a intrat în vigoare la 1 august 2024 și introduce o abordare bazată pe clasificarea sistemelor de inteligență artificială în funcție de nivelul de risc pe care îl generează. Cea mai severă categorie – practicile interzise, este reglementată la articolul 5, care a devenit aplicabil de la 2 februarie 2025.

Dintre practicile interzise prin articolul 5, cea mai direct relevantă pentru protecția minorilor este interdicția sistemelor de inteligență artificială care exploatează vulnerabilitățile utilizatorilor determinate de vârsta acestora, în scopul de a le distorsiona în mod semnificativ comportamentul și de a le cauza sau a risca să le cauzeze un prejudiciu. Aplicată în contextul platformelor digitale utilizate de minori, această interdicție vizează algoritmi care folosesc lipsa de experiență de viață a copiilor, capacitatea lor redusă de evaluare critică, sau tendința lor de a forma comportamente adictive, pentru a-i menține cât mai mult timp pe platformă sau pentru a-i determina să adopte decizii pe care nu le-ar lua în condiții normale. Comisia Europeană a publicat, la 4 februarie 2025, Orientări de interpretare a articolului 5 al AI Act⁶, care explică condițiile cumulative ale fiecărei interdicții și oferă exemple practice de sisteme aflate sau nu sub prohibiție.

⁵ Parlamentul European și Consiliul, *Regulamentul (UE) 2024/1689 din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul privind inteligența artificială / AI Act)*, JO L, 2024/1689, 12.07.2024, disponibil online: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

⁶ Comisia Europeană, *Orientări din 4 februarie 2025 privind practicile interzise în domeniul inteligenței artificiale, așa cum sunt definite în AI Act*, Brussels, 04.02.2025, C(2025) 5052 final din 29.07.2025, disponibil online: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

O altă categorie, introdusă de AI Act prin articolul 6, sunt sistemele cu grad ridicat de risc. Aceste sisteme, deși nu sunt interzise, sunt supuse unor cerințe stricte de conformitate, transparență și control uman. Spre exemplu, sunt considerate cu risc sporit sistemele care sunt folosite în domeniile ce țin de educație, formare profesională, acces la servicii esențiale sau evaluări cu impact semnificativ asupra persoanelor. În cazul minorilor, utilizarea sistemelor de inteligență artificială în educație, orientare, evaluare sau monitorizare trebuie analizată cu prudență. Aceste sisteme trebuie să îndeplinească standarde riguroase privind calitatea și reprezentativitatea datelor de antrenare, transparența funcționării lor și capacitatea operatorilor umani de a supraveghea și corecta deciziile automatizate.

Articolul 50 din AI Act stabilește obligațiile de transparență pentru sistemele de inteligență artificială destinate interacțiunii directe cu persoane fizice. Utilizatorii trebuie informați că interacționează cu un sistem de inteligență artificială, iar conținutul generat sau manipulat artificial, inclusiv imagini, videoclipuri și înregistrări audio sintetice, cunoscute sub denumirea de *deepfake*, trebuie marcate corespunzător. Pentru minori, această obligație are o importanță aparte, deoarece capacitatea de a distinge conținutul autentic de cel generat artificial se prezumă a fi, în general, mai limitată la copii decât la adulți, ceea ce îi expune la riscuri mai mari de manipulare și înșelare.

Pentru Republica Moldova, AI Act oferă un reper important pentru orice viitoare reglementare a platformelor digitale. O legislație națională modernă nu ar trebui să se limiteze la întrebarea dacă minorii pot sau nu pot accesa rețelele sociale sau platformele digitale. Legislația trebuie să abordeze întrebarea mai profundă – ce tipuri de sisteme algoritmice pot fi folosite în raport cu minorii și ce practici trebuie interzise, deoarece exploatează vulnerabilitățile acestora. În acest context, semnarea de către Republica Moldova a Convenției-cadru a Consiliului Europei privind inteligența artificială⁷, la Vilnius, pe 5 septembrie 2024, marchează un angajament internațional important în direcția alinierii la standardele europene în acest domeniu

[Practica recentă de aplicare a DSA: teoria fără practică este inutilă](#)

Practica recentă a Comisiei Europene confirmă caracterul aplicat al DSA. În februarie 2024, Comisia a deschis proceduri formale împotriva TikTok pentru posibile încălcări legate de protecția minorilor, transparența publicității, accesul cercetătorilor la informații importante și riscurile generate de designul adictiv și conținutul dăunător⁸.

În februarie 2026, Comisia Europeană a comunicat constatări preliminare⁹ potrivit cărora TikTok ar fi încălcat DSA prin designul adictiv al serviciului, inclusiv prin funcții precum derularea infinită, redarea automată, notificările push și sistemul personalizat de recomandare. Comisia a apreciat preliminar că platforma nu a evaluat și nu a atenuat suficient riscurile acestor mecanisme asupra bunăstării fizice și psihice a utilizatorilor, în special a minorilor și a persoanelor vulnerabile. Procedura nu este finalizată, iar constatările nu constituie încă o sancțiune. TikTok are dreptul să răspundă și să își prezinte apărările. Dacă încălcarea va fi confirmată

⁷ Consiliul Europei, *Convenția-cadru din 5 septembrie 2024 privind inteligența artificială, drepturile omului, democrația și statul de drept*, CETS nr. 225, deschisă spre semnare la Vilnius, semnată și de către Republica, disponibil online: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>.

⁸ Comisia Europeană, Comunicat de presă *Comisia deschide proceduri oficiale împotriva TikTok în temeiul Actului legislativ privind serviciile digitale*, 19 februarie 2024, disponibil online: https://ec.europa.eu/commission/presscorner/detail/ro/ip_24_926.

⁹ Comisia Europeană, Comunicat de presă *Comisia constată, cu titlu preliminar, că modul în care TikTok creează dependență încalcă Regulamentul privind serviciile digitale*, 6 februarie 2026, disponibil online: https://ec.europa.eu/commission/presscorner/detail/ro/ip_26_312.

printr-o decizie finală de neconformitate, Comisia poate impune măsuri corective și o amendă de până la 6% din cifra de afaceri anuală mondială a furnizorului.

În aprilie 2026, Comisia Europeană a comunicat constatări preliminare¹⁰ potrivit cărora Meta ar fi încălcat DSA prin faptul că nu ar fi identificat, evaluat și atenuat suficient riscurile asociate accesului minorilor sub 13 ani la Instagram și Facebook. Această procedură este deosebit de relevantă pentru studiu, deoarece vizează direct obligațiile platformelor de a preveni accesul minorilor sub vârsta permisă de propriile condiții de utilizare și de a gestiona riscurile pentru copii.

Aceste exemple arată că standardele europene nu sunt doar principii abstracte. Ele sunt deja folosite pentru investigarea modului în care platformele proiectează serviciile, verifică vârsta, gestionează riscurile pentru minori și reduc designul adictiv. Pentru Republica Moldova, această evoluție este importantă deoarece viitoarea reglementare națională trebuie să fie compatibilă nu doar cu textul actelor UE, ci și cu direcția de aplicare a acestora.

Concluzii intermediare: sinergia instrumentelor și relevanța pentru Republica Moldova

Cadrul european relevant indică o direcție clară: protecția minorilor în spațiul digital trebuie realizată printr-o combinație de obligații pentru platforme, protecție a datelor, limitarea profilării, transparență algoritmică, siguranță prin design, verificare proporțională a vârstei, mecanisme de raportare și consolidarea instituțională. Nici DSA, nici GDPR, nici AI Act nu impun, ca standard general, interzicerea totală a accesului minorilor la rețelele sociale. Modelul european este mai nuanțat. El urmărește să reducă riscurile create de platforme și de modelele lor de afaceri, fără a exclude automat beneficiile participării minorilor în spațiul digital, precum educare, informare, exprimare, etc. Această concluzie nu elimină posibilitatea analizării unor restricții de acces în situații de risc ridicat, dar impune ca orice măsură să fie justificată, proporțională, tehnic fezabilă și compatibilă cu drepturile copilului.

Un exemplu ilustrativ care scoate în evidență modul de conlucrare a regulamentelor europene analizate este interzicerea profilării publicitare adresată minorilor:

-  DSA interzice explicit platformelor, prin articolul 28 alineatul (2), să prezinte publicitate profilată, atunci când știe, cu o certitudine rezonabilă, că destinatarul este minor;
-  GDPR recunoaște că minorii necesită o protecție sporită față de marketing și profilare, interzicând, prin articolul 8 alineatul (1), prelucrarea datelor minorilor sub vârsta de 16 ani (13 ani prin excepție) pe baza de consimțământ;
-  AI Act interzice la general, prin articolul 5, sistemele bazate pe inteligență artificială care exploatează vulnerabilitățile legate de vârstă.

Coerența sistemului este consolidată și prin documentele de soft law și practicile recente ale Comisiei Europene privind aplicarea DSA.

Un reper european recent este raportul Child Safety Online: Protecting and Empowering Minors in a Digital World, elaborat în iulie 2026 de copreședinții Special Panel on Child Safety Online. Fără a avea caracter normativ, raportul completează cadrul juridic prin șase principii directe, dintre care sunt relevante în mod special abordarea diferențiată în funcție de etapa de dezvoltare și principiul egalității și diversității. Acesta din urmă presupune recunoașterea faptului că expunerea minorilor la riscurile digitale este influențată nu doar

¹⁰ Comisia Europeană, Comunicat de presă *Comisia constată, cu titlu preliminar, că Meta încalcă Regulamentul privind serviciile digitale pentru că nu a împiedicat minorii sub 13 ani să utilizeze Instagram și Facebook*, 29 aprilie 2026, disponibil online: https://ec.europa.eu/commission/presscorner/detail/ro/ip_26_920.

de vârstă, ci și de gen, situația socioeconomică, apartenența la grupuri minoritare, nevoile educaționale speciale sau problemele de sănătate mintală. Astfel, măsurile de siguranță nu trebuie proiectate pentru un copil abstract, ci adaptate diversității experiențelor și vulnerabilităților minorilor, menținând concomitent drepturile copilului, participarea sa și responsabilitatea principală a furnizorilor de servicii digitale.

Pentru Republica Moldova, lecția principală este că reglementarea trebuie construită gradual și coerent. O soluție eficientă nu poate rezulta dintr-un singur amendament legislativ. Ea presupune armonizarea legislației, în principal cu DSA și AI Act, consultarea tinerilor și integrarea dimensiunii de gen, coroborate cu capacitatea reală a autorităților de supraveghere. Această abordare este mai dificilă decât o interdicție generală, dar este mai compatibilă cu standardele europene.

Diagnosticul cadrului normativ și instituțional al Republicii Moldova

Analiza cadrului Uniunii Europene a arătat că protecția minorilor în spațiul digital se construiește ca un set coerent de instrumente care se completează reciproc. Întrebarea firească este în ce măsură dispunem de o arhitectură similară. Diagnosticul care urmează examinează, mai întâi, ce reguli există în prezent, apoi unde se află lacunele față de standardele europene și, în final, cine ar trebui să aplice aceste reguli și cu ce mijloace. Vom examina cadrul normativ și instituțional al Republicii Moldova relevant pentru protecția minorilor în mediul digital, având drept scop de a stabili în ce măsură normele existente pot răspunde riscurilor descrise în secțiunile anterioare și cât de compatibile sunt acestea cu standardele europene relevante, în special DSA, GDPR și AI Act.

De precizat că, Republica Moldova nu este stat membru al Uniunii Europene, prin urmare regulamentele europene nu se aplică direct pe teritoriul său. Totuși, în calitate de stat candidat, țara s-a angajat să își armonizeze treptat legislația cu acquis-ul comunitar. Aceasta înseamnă că actele naționale urmează a fi studiate nu doar prin raportare la realitatea internă și necesitățile contemporane, ci și prin gradul lor de apropiere de standardele europene analizate anterior.

Vor fi analizate actele normative interne care reglementează drepturile copilului, protecția datelor cu caracter personal, serviciile societății informaționale, comunicațiile electronice, audiovizualul, protecția consumatorilor, prevenirea violenței și răspunderea penală pentru faptele comise împotriva minorilor în mediul digital. Accentul va fi pus pe dispozițiile cu relevanță directă pentru accesul minorilor la platforme digitale, protecția datelor acestora, prevenirea expunerii la conținut dăunător, combaterea exploatarei și responsabilitatea instituțiilor competente.

Analiza nu urmărește o prezentare exhaustivă a fiecărui act normativ, ci identificarea acelor prevederi care pot susține o politică publică privind siguranța digitală a minorilor. Vor fi semnalate limitele cadrului existent în raport cu riscurile în online, cum ar fi: profilarea, publicitatea comportamentală, sistemele de recomandare, designul manipulator, verificarea vârstei, etc.

Drepturile copilului ca temelie a sistemului

Legea nr. 370/2023 privind drepturile copilului¹¹ este actul-cadru național în materia protecției și promovării drepturilor copilului. Pentru prezentul studiu, relevanța legii constă în faptul că aceasta oferă baza generală pentru orice intervenție normativă care vizează minorii, inclusiv în mediul digital. Legea a fost adoptată pentru

¹¹ Parlamentul Republicii Moldova, Legea nr. 370/2023 privind drepturile copilului, Monitorul Oficial al Republicii Moldova nr. 488-491, art. 864, 21.12.2023, disponibil online: https://www.legis.md/cautare/getResults?doc_id=153186&lang=ro.

a transpune în dreptul național principiile Convenției ONU din 1989 cu privire la drepturile copilului, în vigoare pentru Republica Moldova din 25 februarie 1993¹².

Articolul 3 din lege preia definiția internațională a copilului ca persoană sub vârsta de 18 ani și consacră interesul superior al copilului ca principiu director care constă în asigurarea unor condiții adecvate pentru creștere și dezvoltare armonioasă, ținând cont de particularitățile individuale. Articolul 4 prevede printre altele respectarea cu prioritate a interesului superior al copilului, egalitatea de șanse și nediscriminarea, respectarea demnității copilului, ascultarea opiniei copilului, precum și protecția împotriva abuzului, neglijării, exploatarei și oricărei forme de violență. Aceste principii susțin ideea că minorii trebuie protejați în mediul digital, dar și consultați atunci când sunt adoptate politici care îi afectează direct.

Articolul 15 garantează copilului dreptul de a-și exprima opinia asupra oricărei probleme care îl privește și obligă statul să asigure o participare sistematică și incluzivă a copiilor, cu accent pe cei aflați în situații de dificultate. Articolul 16 consacră dreptul copilului la libera exprimare, inclusiv libertatea de a căuta, primi și difuza informații și idei prin orice mijloace alese de copil; iar articolul 17 întărește dreptul la libertatea de gândire și conștiință, care sunt indispensabile de posibilitatea reală a primi informații și exprimare liberă. Articolul 18 recunoaște importanța mijloacelor de informare și obligă statul să asigure accesul copilului la surse de informare și cele materiale care îi susțin bunăstarea socială, spirituală, morală și sănătatea fizică și mentală. Statul trebuie să asigure dezvoltarea instrumentelor de informare, care sunt o utilitate socială și culturală pentru copil, asigurând concomitent, prin aprobarea standardelor corespunzătoare, ca fiecare copil să fie protejat de informații dăunătoare.

În același timp, articolul 23 obligă statul să întreprindă măsuri pentru prevenirea și protecția copilului față de orice formă de violență, abuz, neglijare, exploatare sau trafic. Această normă acoperă și situațiile din mediul digital, cum ar fi hărțuirea online, groomingul (adică procesul prin care un adult câștigă treptat încrederea unui minor, de regulă prin manipulare emoțională, atenție, cadouri, complimente sau promisiuni, cu scopul de a-l exploata sexual ori de a-l determina să accepte contacte, conversații sau materiale cu caracter sexual), exploatarea sexuală online sau distribuirea de conținut prejudiciabil. Totuși, legea nu dezvoltă mecanisme specifice pentru riscurile generate de platforme, cum ar fi profilarea minorilor, publicitatea comportamentală, sistemele de recomandare sau designul manipulator.

Pentru tema studiului, Legea nr. 370/2023 este importantă. Ea construiește un cadru general al drepturilor copilului, dar nu dezvoltă un regim specific modern adaptat mediului digital. Spre deosebire de Comentariul general nr. 25 (2021) al Comitetului ONU, care va fi analizat mai jos, care traduce drepturile copilului în obligații concrete pentru furnizorii de servicii digitale, legea națională nu conține obligații dedicate platformelor online, nu reglementează designul serviciilor digitale și nu abordează riscurile generate de algoritmi de recomandare sau de modelele comerciale bazate pe captarea atenției. Drepturile copilului în spațiul digital rezultă, prin deducție, din aplicarea principiilor generale ale legii, dar nu beneficiază de o concretizare normativă proprie. Aceasta este **prima lacună sistemică: temelia există, dar nu a fost încă extinsă explicit asupra mediului online.**

Conținutul dăunător: o reglementare construită pe o paradigmă învechită

¹² Consiliul Național pentru Protecția Drepturilor Copilului: <https://cnpdc.gov.md/ro/content/conven%C5%A3ia-onu-cu-privire-la-drepturile-copilului>.

Cel mai direct act normativ național în legătură cu tema studiului probabil ar fi Legea nr. 30/2013 cu privire la protecția copiilor împotriva impactului negativ al informației¹³. Ea stabilește criteriile pentru calificarea informației publice cu impact negativ asupra copiilor, restricții privind difuzarea acesteia, precum și obligații pentru o serie de actori, inclusiv pentru furnizorii de servicii de acces la internet, care trebuie să ofere utilizatorilor posibilitatea de a instala aplicații de filtrare a conținutului nociv, iar pentru producătorii și difuzorii de jocuri obligația de a aplica marcaje pe categorii de vârstă.

Această lege rămâne relevantă, dar reflectă paradigma momentului în care a fost adoptată – cu 13 ani în urmă. Logica sa este una axată pe conținut și pe filtrare: identifică tipuri de informație dăunătoare, precum cea care promovează violența, conținutul pornografic, jocurile de noroc sau auto-vătămarea, și caută să limiteze accesul copiilor la acestea, în principal prin instrumente de control parental și prin clasificare pe vârste. Este o abordare proiectată pentru o lume a televiziunii, a jocurilor și a paginilor de internet cu conținut relativ static, nu pentru ecosistemul actual al rețelelor sociale, în care riscul nu provine doar din conținutul difuzat, ci din însuși modul în care platformele sunt proiectate, recomandă conținut și rețin atenția utilizatorului. Filtrarea conținutului, oricât de utilă a fost anterior, nu răspunde riscurilor generate de design, de profilare sau de mecanismele care creează dependență, analizate pe larg în secțiunea privind analiza cadrului normativ

european. Aici se conturează **a doua lacună structurală: reglementarea națională a conținutului dăunător operează cu o logică învechită în raport cu cea a DSA**, care mută accentul de pe filtrarea conținutului pe responsabilizarea și rolul pro-activ al platformelor.

Audiovizualul: protecție reală, dar într-un domeniu limitat

Codul serviciilor media audiovizuale¹⁴ conține un regim mai dezvoltat de protecție a minorilor față de conținutul audiovizual, care transpune standardele europene din domeniul. Articolul 15 consacră obligația furnizorilor de servicii media de a respecta interesul superior al minorului, dreptul acestuia la imagine și viață privată, precum și interdicția difuzării programelor susceptibile să afecteze dezvoltarea fizică, mintală sau morală a minorilor, în special a celor care conțin pornografie sau violență nejustificată. Același articol prevede posibilitatea restricționării accesului prin clasificare, intervale orare, acces condiționat sau alte măsuri tehnice. Codul reglementează clasificarea programelor în funcție de impactul asupra dezvoltării fizice, mintale sau morale a minorilor.

Articolul 61¹ obligă furnizorii de platformă de partajare a materialelor video aflați în jurisdicția Republicii Moldova să ia măsuri pentru protecția minorilor față de programe, materiale video generate de utilizatori și comunicări comerciale care le pot afecta dezvoltarea. Măsurile includ mecanisme de raportare, sisteme de verificare a vârstei, control parental, proceduri de soluționare a sesizărilor și instrumente de educație media. Alineatul (8) al aceluiași articol prevede expres că datele minorilor colectate sau generate prin sistemele de verificare a vârstei și control parental nu pot fi prelucrate în scopuri comerciale, inclusiv marketing direct, creare de profiluri sau publicitate comportamentală. Furnizorii trebuie să instituie un mecanism intern de soluționare, pe cale amiabilă, a litigiilor cu utilizatorii.

Codul prevede și obligația ca, în serviciile media audiovizuale neliniare (serviciile la cerere, de tipul platformelor de streaming video), conținutul care ar putea afecta dezvoltarea minorilor să fie pus la dispoziție

¹³ Parlamentul Republicii Moldova, Legea nr. 30/2013 cu privire la protecția copiilor împotriva impactului negativ al informației, Monitorul Oficial al Republicii Moldova nr. 69-74 art. 221, 05.04.2013, disponibil online: https://www.legis.md/cautare/getResults?doc_id=133289&lang=ro#.

¹⁴ Parlamentul Republicii Moldova, Codul serviciilor media audiovizuale nr. 174/2018, Monitorul Oficial al Republicii Moldova nr. 462-466 art. 766, 12.12.2018, disponibil online: https://www.legis.md/cautare/getResults?doc_id=150538&lang=ro#.

numai cu măsuri de restricționare a accesului. Potrivit articolului 61, aceștia au obligația să respecte cerințele privind protecția minorilor. Articolul 15 alineatul (16) din Cod prevede că, Consiliul Audiovizualului contribuie la protecția minorilor prin stabilirea și promovarea unor reguli pentru furnizorii de servicii media, în special privind comunicările comerciale audiovizuale, serviciile media neliniare și clasificarea programelor destinate minorilor sau care necesită autorizare prealabilă.

Protecția oferită de Cod este, în domeniul său, una serioasă și aliniată standardelor europene din audiovizual. Limita ține însă de sfera de aplicare. Codul reglementează furnizorii de servicii media audiovizuale, adică televiziunile, distribuitorii și serviciile la cerere, platformelor de streaming video, însă nu acoperă rețelele sociale și platformele cu conținut generat de utilizatori, care reprezintă tocmai spațiul în care minorii își petrec cea mai mare parte a timpului online. O rețea de socializare nu este, în sensul Codului, un furnizor de servicii media audiovizuale, prin urmare cele mai relevante platforme pentru tema studiului rămân, în mare parte, în

afara acestui regim. Aceasta este **a treia lacună sistemică: protecția audiovizuală există, dar nu acoperă spațiul digital** în care se manifestă cele mai multe riscuri.

Protecția datelor cu caracter personal: un regim în tranziție

Un alt palier relevant analizei privește protecția datelor personale ale copiilor, domeniul în care decalajul față de standardul european este cel mai aproape de a fi acoperit. Particularitatea constă în faptul că Republica Moldova se află într-o perioadă de tranziție între două regimuri juridice diferite.

Regimul aflat în vigoare la data prezentei analize este cel stabilit de Legea nr. 133/2011 privind protecția datelor cu caracter personal¹⁵. Această lege definește consimțământul ca temei principal al prelucrării datelor, dar nu conține o prevedere specifică privind consimțământul digital al copiilor și nu stabilește un prag de vârstă de la care un minor poate consimți singur la prelucrarea datelor sale în relația cu serviciile online. Cu alte cuvinte, regimul actual tratează copilul, sub acest aspect, în mod similar oricărui alt subiect de date, fără garanțiile suplimentare pe care GDPR le consideră esențiale pentru minori.

Această situație se va schimba odată cu intrarea în vigoare a Legii nr. 195/2024 privind protecția datelor cu caracter personal¹⁶, adoptată pentru a transpune în principal GDPR și care urmărește protecția drepturilor și libertăților fundamentale ale persoanei, în special dreptul la viață privată în legătură cu prelucrarea datelor. Noua lege va intra în vigoare la 23 august 2026, iar până atunci continuă să se aplice legea veche.

Relevanța acestei legi pentru protecția minorilor în mediul digital este directă. Platformele online funcționează prin colectarea și prelucrarea unui volum mare de date despre utilizatori: vârstă, locație, preferințe, comportament online, interacțiuni, timp petrecut pe platformă și reacții la conținut. În cazul minorilor, aceste date pot fi folosite pentru profilare, publicitate personalizată, recomandări algoritmice sau alte forme de influențare a comportamentului, interzise prin standardele UE.

Legea nr. 195/2024 introduce principiile de bază ale prelucrării datelor la articolul 5: legalitate, echitate și transparență, limitarea scopului, reducerea la minimum a datelor, exactitate, limitarea stocării, integritate și confidențialitate, precum și responsabilitate. Pentru prezentul studiu, cele mai importante sunt transparența

¹⁵ Parlamentul Republicii Moldova, Legea nr. 133/2011 privind protecția datelor cu caracter personal, Monitorul Oficial nr. 170-175, art. 492, 14.10.2011, disponibil online:

https://www.legis.md/cautare/getResults?doc_id=144823&lang=ro#.

¹⁶ Parlamentul Republicii Moldova, Legea nr. 195/2024 privind protecția datelor cu caracter personal, Monitorul Oficial nr. 367-369, art. 574, 23.08.2024 (în vigoare din 23.08.2026), disponibil online:

https://www.legis.md/cautare/getResults?doc_id=144681&lang=ro.

și minimizarea datelor. Aceste principii sunt relevante mai ales pentru mecanismele de verificare a vârstei, care nu trebuie să ducă la colectarea excesivă de date despre utilizatori.

Articolul 6 stabilește temeiurile legale ale prelucrării, inclusiv consimțământul. Noul act introduce, la articolul 8, un regim special al consimțământului copiilor în legătură cu serviciile societății informaționale, și anume: prelucrarea datelor unui copil pe baza consimțământului este legală dacă acesta are cel puțin vârsta de 14 ani. Sub această vârstă, prelucrarea este legală numai cu consimțământul ori autorizarea de reprezentantul legal al copilului. Norma prevede obligația furnizorului de a depune eforturi rezonabile pentru a verifica dacă reprezentantul legal a acordat sau a autorizat consimțământul.

Merită de subliniat aspectul alegerii pragului de 14 ani. GDPR stabilește un prag general de 16 ani, dar permite expres statelor membre să îl coboare până la minimum 13 ani. Pragul moldovenesc de 14 ani se înscrie, așadar, în marja permisă de standardul european și este comparabil cu opțiunile mai multor state membre. Sub aspectul protecției datelor, convergența cu acquis-ul comunitar este asigurată.

Totuși, noua lege privind protecția datelor cu caracter personal nu este un instrument specializat de reglementare a platformelor online. Ea oferă un cadru solid pentru protecția datelor, dar nu conține, în sine, obligații echivalente cu articolul 28 din DSA privind interzicerea publicității bazate pe profilare pentru minori, nici obligații privind sistemele de recomandare, designul adecvat vârstei sau evaluarea riscurilor sistemice. Din acest motiv, protecția datelor trebuie privită ca o componentă necesară, dar insuficientă, a unui viitor cadru național privind siguranța digitală a minorilor.

Rămâne totodată deschisă o întrebare de fond, care va reveni în analiza scenariilor de reglementare, și anume: pragul de vârstă pentru consimțământul la prelucrarea datelor nu echivalează cu un prag de acces la platforme și nu rezolvă, singur, problema verificării vârstei. Concluzia preliminară ar fi că, orice model bazat pe verificarea vârstei sau consimțământ parental trebuie construit strict pe principiile minimizării datelor, proporționalității, securității și transparenței. O soluție care ar impune colectarea generalizată a actelor de identitate, imaginilor faciale sau datelor biometrice ale minorilor sau părinților ar ridica neconcordanțe cu principiile stabilite prin Declarația 1/2025 privind asigurarea vârstei (*age assurance*), analizată mai sus, care avertizează expres că necesitatea stabilirii vârstei utilizatorului nu trebuie folosită drept pretext pentru colectarea exagerată a datelor personale. De aici derivă **a patra lacună sistemică:**

regimul protecției

datelor reglementează consimțământul minorului, dar nu și verificarea proporțională a vârstei sau

accesul la platforme. Pragul de 14 ani rezolvă cine poate consimți la prelucrarea datelor, însă nu oferă un mecanism prin care platformele să confirme vârsta fără colectarea excesivă de date și nu instituie un regim de acces. În dreptul european aceste chestiuni îi revin DSA, iar în dreptul național sunt inexistente.

Serviciile societății informaționale: un cadru general util, dar insuficient

Legea nr. 284/2004 privind serviciile societății informaționale¹⁷ (anterior fiind cunoscută ca Legea privind comerțul electronic) este la fel relevantă studiului, deoarece reglementează cadrul general al prestării serviciilor online. Acest act transpune Directiva 2000/31/CE privind comerțul electronic¹⁸, instrumentul

¹⁷ Parlamentul Republicii Moldova, Legea nr. 284-XV din 22 iulie 2004 privind serviciile societății informaționale, Monitorul Oficial Nr. 40-47 art. 104, 09.02.2018, disponibil online: https://www.legis.md/cautare/getResults?doc_id=150486&lang=ro#.

¹⁸ Parlamentul European și Consiliul, Directiva 2000/31/CE din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic), JO L 178 17.07.2000, disponibil online: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02000L0031-20240217>.

europene care au precedat Regulamentul privind serviciile digitale, și stabilește principiile de furnizare a serviciilor online, precum și regimul de răspundere al furnizorilor și al intermediarilor.

Potrivit articolului 4 din lege, furnizorul de servicii este persoana fizică sau juridică ce pune la dispoziția unui număr determinat sau nedeterminat de persoane servicii ale societății informaționale, acestea fiind orice serviciu prestat în scopul obținerii unei remunerații, la distanță, prin mijloace electronice și la cererea individuală a destinatarului serviciului, inclusiv vânzări de bunuri on-line. Această definiție permite includerea unui spectru larg de servicii digitale, inclusiv platforme, magazine online, aplicații și alte servicii furnizate prin mijloace electronice.

Legea conține unele garanții utile pentru utilizatori. Articolul 10 reglementează protecția datelor cu caracter personal în cadrul serviciilor societății informaționale, iar articolul 12 obligă furnizorul să asigure acces ușor, direct și permanent la informații despre identitatea sa, datele de contact, condițiile de prestare, prețuri, tarife și alte informații relevante pentru destinatarul serviciului. Aceste obligații sunt importante pentru transparența serviciilor online, inclusiv atunci când utilizatorii sunt minori. Articolele 14–17 reglementează răspunderea furnizorilor de servicii și a intermediarilor. Aceste prevederi sunt importante deoarece stabilesc cadrul în care furnizorii pot răspunde pentru informația furnizată, transmisă sau stocată.

Totuși, regimul existent este construit pe logica clasică a comerțului electronic și a serviciilor intermediare, nu pe logica actuală a DSA, care impune furnizorilor obligații pozitive de diligență, transparență, evaluare și atenuare a riscurilor sistemice și pune accent pe protecția specială a minorilor. Dreptul Uniunii a evoluat de la o abordare pasivă către una activă, axată pe responsabilizarea platformelor. Republica Moldova a rămas, sub acest aspect, ancorată în cadrul moștenit. Aceasta este **a cincea lacună sistemică: absența unui regim modern al serviciilor digitale**. Prin urmare, Legea nr. 284/2004 oferă un cadru general util pentru transparența serviciilor online și răspunderea furnizorilor, dar nu conține obligații speciale privind platformele accesibile minorilor. Ea nu reglementează expres interdicția publicității bazate pe profilare pentru minori, sistemele de recomandare, designul manipulator, verificarea vârstei sau obligațiile de evaluare a riscurilor sistemice. Aceste lacune trebuie avute în vedere la elaborarea politicilor publice.

Protecția consumatorilor minori în mediul digital

Legea nr. 105/2003 privind protecția consumatorilor¹⁹ este relevantă în măsura în care minorii pot fi și consumatori de servicii digitale, jocuri online, conținut digital, abonamente, aplicații sau produse promovate prin platforme. Această lege, armonizată în 2023, interzice practicile comerciale incorecte și clauzele abuzive, fiind completată cu noțiuni precum conținutul digital și interfața online, precum și cu reguli privind rezultatele afișate în urma căutărilor efectuate online. Aceste evoluții apropie legislația de problematica digitală.

Pentru mediul digital, mai sunt importante articolele 13–15 privind practicile comerciale incorecte. Acestea pot acoperi situații precum publicitatea înșelătoare, prezentarea incompletă a prețului, abonamentele ascunse, presiunea comercială sau alte practici care afectează decizia economică a consumatorului, inclusiv minor. Articolul 15 permite încetarea sau interzicerea practicilor comerciale incorecte și prevede remedii pentru consumatorii afectați. Legea conține și garanții generale utile pentru raporturile digitale. Articolul 6 consacră drepturile fundamentale ale consumatorilor, inclusiv protecția intereselor economice, protecția sănătății și securității și dreptul la informare. Articolul 16 prevede dreptul consumatorului de a lua liber decizii la achiziționarea produsului sau serviciului, fără clauze abuzive ori practici incorecte.

¹⁹ Parlamentul Republicii Moldova, Legea nr. 105/2003 privind protecția consumatorilor, Monitorul Oficial Nr. 122-124 art. 195, 28.03.2024, disponibil online: https://www.legis.md/cautare/getResults?doc_id=150997&lang=ro#.

Cu toate acestea, protecția minorului-consumator în mediul digital rămâne acoperită doar la nivel general. Legea nu conține o interdicție specifică a publicității bazate pe profilare adresate minorilor, echivalentă celei prevăzute de DSA, și nu reglementează în mod special interfețele care manipulează deciziile copiilor, fenomen cunoscut sub denumirea de *dark patterns* (modele de design înșelătoare), sistemele de recomandare intruzive sau obligațiile platformelor de evaluare a riscurilor sistemice. Riscurile de consumator la care sunt expuși minorii, analizate în secțiunea privind vulnerabilitatea digitală, precum abonamentele cu costuri ascunse, publicitatea comportamentală sau profilarea comercială, sunt tratate, în prezent, prin instrumente gândite pentru consumatorul adult generic. Aceasta constituie **a șasea lacună sistemică: lipsa protecției țintite a consumatorului-minor**. Prin urmare, Legea nr. 105/2003 oferă un instrument complementar util, mai ales pentru riscurile generale ale consumatorilor în mediul online, dar nu poate substitui un cadru special de tip DSA pentru protecția minorilor în spațiul digital.

Infrațiunile în mediul digital și violența digitală: un cadru recent consolidat

Un palier care a cunoscut o evoluție notabilă este cel al răspunderii penale pentru faptele comise împotriva minorilor, în special prin mijloace digitale. Codul penal al Republicii Moldova²⁰ conține mai multe norme relevante pentru protecția minorilor împotriva abuzului și exploatarei, inclusiv atunci când faptele sunt comise sau facilitate prin mijloace digitale. Articolul 175¹ incriminează ademenirea minorului în scopuri sexuale, normă importantă pentru cazurile de grooming online, iar articolul 208¹ vizează circulația materialelor privind abuzul sexual asupra copilului.

Un pas important l-au constituit modificările operate prin Legea nr. 252/2025²¹, intrate în vigoare la 14 februarie 2026, care au introdus instrumente suplimentare pentru combaterea violenței comise online. Codul penal a fost completat cu articolul 169¹ privind actele de persecuție, care sancționează persecutarea sistematică a unei persoane, inclusiv prin tehnologii informaționale sau rețele de comunicații electronice, atunci când aceasta provoacă anxietate, teamă pentru siguranța proprie sau a rudelor apropiate și determină victima să își modifice conduita de viață. Aceste modificări sunt relevante pentru minori, deoarece *stalkingul*, adică contactarea repetată, supravegherea online, amenințările digitale și hărțuirea prin platforme pot afecta direct siguranța, viața privată și dezvoltarea psihologică a minorului. Totodată, actul legislativ a înăsprit sancționarea pentru hărțuirea sexuală comisă prin tehnologii informaționale sau comunicații electronice, inclusiv prin modificarea articolului 173 din Codul penal, fiind extins cadrul de protecție împotriva violenței digitale. Reforma a avut drept scop realizarea angajamentelor asumate prin Convenția de la Istanbul²². Această evoluție este relevantă în mod direct pentru dimensiunea de gen a studiului. Datele și analizele privind violența facilitată digital arată că aceasta afectează în mod disproporționat fetele și tinerele, prin fenomene precum hărțuirea online, urmărirea digitală, distribuirea neconsensuală a imaginilor intime sau materialele sexualizate generate inclusiv cu ajutorul inteligenței artificiale. Noul cadru penal oferă un instrument important de protecție.

Totuși, dreptul penal intervine, de regulă, după producerea sau tentativa producerii prejudiciului. El nu poate substitui obligațiile preventive ale platformelor: mecanisme accesibile de raportare, moderarea eficientă a

²⁰ Parlamentul Republicii Moldova, Codul penal al Republicii Moldova nr. 985/2002, Monitorul Oficial Nr. 72-74 art. 195, 14.04.2009, disponibil online: https://www.legis.md/cautare/getResults?doc_id=153235&lang=ro#.

²¹ Parlamentul Republicii Moldova, Legea nr. 252/2025 pentru modificarea unor acte normative, Monitorul Oficial Nr. 430-433 art. 596, 14.08.2025, disponibil online: https://www.legis.md/cautare/getResults?doc_id=150197&lang=ro.

²² Consiliul Europei, Convenția privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice Istanbul, 11.V.2011, ratificată de către Republica Moldova prin Legea nr. 14/2021, disponibil online: https://www.legis.md/cautare/getResults?doc_id=128240&lang=ro.

conținutului, reacția rapidă la sesizări, limitarea contactului abuziv cu minorii și cooperarea cu autoritățile. Din acest motiv, componenta penală trebuie privită ca parte a unui sistem mai larg de protecție, nu ca soluție suficientă în sine. Astfel, suntem în fața celei de **a șaptea lacună sistemică: cadrul penal nu acoperă segmentul de prevenire**. Pentru prezentul studiu, concluzia practică este că Republica Moldova dispune de norme penale relevante pentru combaterea unor forme grave de abuz digital asupra minorilor, iar modificările recente consolidează această protecție. Totuși, prevenirea eficientă a acestor riscuri reclamă și obligații clare pentru platforme, în special privind raportarea, gestionarea conținutului ilegal, evaluarea riscurilor și protecția minorilor, în logica DSA.

Comunicațiile electronice și securitatea cibernetică: o carcasă solidă pentru viitoarele politici

Legea comunicațiilor electronice nr. 72/2025²³ este relevantă pentru prezentul studiu prin faptul că reglementează infrastructura generală de conectivitate, accesul la servicii de comunicații electronice și raporturile dintre furnizori și utilizatori. Legea transpune mai multe directive UE relevante și creează cadrul național pentru integrarea Republicii Moldova în piața digitală europeană. Din perspectiva protecției minorilor, această lege are o relevanță indirectă. Ea nu reglementează conținutul platformelor digitale și nici obligațiile acestora privind profilarea, publicitatea comportamentală sau sistemele de recomandare. Totuși, este importantă pentru accesul efectiv la internet, calitatea serviciilor, drepturile utilizatorilor finali și competențele autorității de reglementare în domeniul comunicațiilor.

Complementar, Legea nr. 48/2023 privind securitatea cibernetică²⁴ stabilește cadrul primar în domeniul securității rețelelor și sistemelor informatice. Această lege are ca scop asigurarea securității rețelelor și sistemelor informatice utilizate de persoanele juridice publice sau private care prestează servicii esențiale pentru activități societale și economice critice. Agenția pentru Securitate Cibernetică este desemnată drept autoritate publică responsabilă de gestionarea incidentelor și crizelor cibernetice la nivel național.

Aceste reglementări sunt importante pentru măsurile de protecția a minorilor în spațiul digital care implică verificarea vârstei, consimțământ parental sau colectarea unor date suplimentare despre minori. Orice asemenea mecanism creează riscuri de securitate cibernetică: scurgeri de date, furt de identitate, compromiterea conturilor sau utilizarea secundară a datelor colectate. De aceea, soluțiile de acces condiționat nu pot fi evaluate doar juridic, ci verificate și fezabilitatea tehnică, inclusiv din perspectiva Legii nr. 48/2023 și a capacității instituționale a Agenției pentru Securitate Cibernetică.

Prin urmare, legislația privind comunicațiile electronice și securitatea cibernetică oferă cadrul tehnic și instituțional necesar pentru funcționarea serviciilor digitale, dar nu constituie, în sine, un regim de protecție a minorilor. Ea trebuie conectată cu viitoarele norme care vor transpune DSA și AI Act, mai ales în privința verificării vârstei, securității datelor și gestionării incidentelor cibernetice care afectează copiii.

Reforme pendinte: transpunerea DSA și primele inițiative în materie de inteligență artificială

Tabloul de mai sus arată că Republica Moldova nu dispune încă de o lege specială dedicată serviciilor digitale și responsabilizării platformelor online și nici de un cadru normativ aplicabil sistemelor de inteligență artificială. Aceste goluri sunt însă recunoscute de autorități și se află, la data analizei, în diferite stadii de

²³ Parlamentul Republicii Moldova, Legea nr. 72/2025 comunicațiilor electronice, Monitorul Oficial Nr. 226-228 art. 266, 13.05.2025, disponibil online: https://www.legis.md/cautare/getResults?doc_id=151457&lang=ro#.

²⁴ Parlamentul Republicii Moldova, Legea nr. 48/2023 privind securitatea cibernetică, Monitorul Oficial Nr. 151-153 art. 225, 28.04.2023, disponibil online: https://www.legis.md/cautare/getResults?doc_id=152655&lang=ro.

remediere. Trei inițiative aflate în curs merită prezentate împreună, deoarece ele conturează direcția în care se îndreaptă cadrul național și, totodată, arată cât de timpuriu este acest proces.

Prima și cea mai avansată este **proiectul de lege privind serviciile digitale**²⁵, elaborat de Ministerul Dezvoltării Economice și Digitalizării (MDED) pentru transpunerea parțială a Regulamentului privind serviciile digitale în dreptul național. Proiectul preia elementele centrale ale modelului european, printre care obligațiile furnizorilor de servicii intermediare, mecanismele de notificare a conținutului ilegal, statutul notificatorilor de încredere și, probabil cel mai important pentru dimensiunea instituțională, instituirea unui Coordonator al serviciilor digitale – autoritatea națională responsabilă de supravegherea și aplicarea regulilor, după modelul prevăzut de regulament pentru statele membre. Proiectul a parcurs deja avizarea interinstituțională și expertiza anticorupție, ceea ce îl plasează într-un stadiu relativ avansat al procesului legislativ. Cu toate acestea, la data prezentei analize documentul are statutul de proiect și nu a fost încă adoptat de Parlament. Calendarul concret al adoptării și autoritatea care va exercita funcția de Coordonator rămân elemente care urmează a fi stabilite. Importanța acestui proiect este greu de supraapreciat, întrucât el reprezintă instrumentul prin care lacunele cele mai sensibile identificate mai sus, și anume cele privind responsabilizarea platformelor, designul serviciilor și supravegherea, ar urma să fie acoperite.

Celelalte **două inițiative privesc inteligența artificială** și se află într-un stadiu mult mai incipient. Prima este anunțul privind inițierea elaborării unui proiect de lege privind inteligența artificială²⁶, lansat în consultare la finalul lunii mai 2026. Potrivit anunțului, scopul viitoarei legi este instituirea unui cadru normativ național pentru dezvoltarea, utilizarea și supravegherea sistemelor de inteligență artificială, cu asigurarea utilizării lor sigure, etice și responsabile, a protecției drepturilor fundamentale și a alinierii la standardele UE. La data prezentei analize este vorba despre un anunț de inițiere, fără un text de proiect publicat, ceea ce înseamnă că forma concretă a viitoarei reglementări nu este încă cunoscută.

A doua inițiativă în materie de inteligență artificială este proiectul de hotărâre de Guvern pentru aprobarea Programului Național privind Inteligența Artificială și Guvernanța Datelor pentru anii 2026-2030²⁷, aflat de asemenea în stadiul de inițiere a elaborării, cu un concept supus consultării publice. Spre deosebire de anunțul privind proiectul de lege privind inteligența artificială, conceptul Programului oferă deja o imagine asupra direcției asumate. El pornește de la Cartea Albă privind Guvernanța Datelor și Inteligența Artificială²⁸, primul document cadru de politici în domeniu, și identifică explicit, printre problemele de rezolvat, absența unei autorități naționale competente în materie de inteligență artificială și lipsa unui cadru normativ național specific, comparabil cu AI Act.

²⁵ Ministerul Dezvoltării Economice și Digitalizării, proiectul de lege privind serviciile digitale, număr unic 309/MDED/2025, disponibil online: <https://particip.gov.md/ro/document/stages/proiect/14352>.

²⁶ Ministerul Dezvoltării Economice și Digitalizării, anunț privind inițierea elaborării proiectului de lege privind inteligența artificială, ID Particip (16726), mai 2026, disponibil online: <https://particip.gov.md/ro/document/stages/anunt-privind-initierea-elaborarii-proiectului-de-lege-privind-inteligena-artificiala/16726>.

²⁷ Ministerul Dezvoltării Economice și Digitalizării, anunț privind inițierea elaborării proiectului hotărârii pentru aprobarea Programului Național privind Inteligența Artificială și Guvernanța Datelor pentru anii 2026-2030, ID Particip: 16590, aprilie 2026, disponibil online: <https://particip.gov.md/index.php/ro/document/stages/anunt-privind-initierea-elaborarii-proiectului-hotararii-pentru-aprobarea-programului-national-privind-inteligena-artificiala-si-guvernanta-datelor-pentru-anii-2026-2030/16590>.

²⁸ Ministerul Dezvoltării Economice și Digitalizării, Sub-consiliul pentru Inteligență Artificială și Cercetare Aplicată (SCIA), *Cartea Albă privind Inteligența Artificială și Guvernanța Datelor*, 2024, disponibil online: <https://mded.gov.md/carte-alba-privind-inteligena-artificiala-si-guvernanta-datelor-primul-document-cadru-de-politici-al-mded/>.

Primul dintre cele cinci obiective ale Programului vizează tocmai elaborarea, adoptarea și implementarea unui asemenea cadru de reglementare, iar documentul invocă alinierea la Regulamentul privind inteligența artificială și la Regulamentul privind guvernanta datelor. Pentru coordonarea procesului a fost constituit Sub-consiliu pentru Inteligență Artificială și Cercetare Aplicată²⁹, cu participarea mai multor autorități relevante: Ministerul Justiției, Ministerul Educației și Cercetării, Agenția pentru Securitate Cibernetică, CNPDCP, etc. Două observații se impun în legătură cu aceste inițiative. Prima ține de stadiul lor: dintre cele trei, doar proiectul privind serviciile digitale este avansat, în timp ce inițiativele în materie de inteligență artificială se află la nivelul anunțului de inițiere, fără texte normative consolidate, ceea ce înseamnă că rezultatul lor concret și calendarul rămân incerte. Această observație este coerentă cu poziția exprimată public de decidenți, potrivit căreia reglementarea inteligenței artificiale este abia la început.

A doua observație, relevantă analizei, este că niciuna dintre cele două inițiative privind inteligența artificială nu vizează în mod special protecția minorilor. Ambele privesc inteligența artificială preponderent dintr-o perspectivă de dezvoltare economică, inovare și guvernanta a datelor, iar dimensiunea protecției copilului, deși implicită în trimiterea la drepturile fundamentale și la legislația UE, nu constituie un obiect distinct al acestor documente. Prin urmare, chiar și după adoptarea lor, va rămâne necesară verificarea măsurii acoperii riscurilor specifice pentru utilizatori, în special minori, precum sistemele de recomandare care exploatează vulnerabilitățile legate de vârstă, profilarea sau conținutul adictiv.

Cadrul instituțional și capacitatea de aplicare

Orice lege, cât de bună n-ar fi, rămâne inutilă fără instituții capabile să o aplice. De aceea, diagnosticul nu se poate opri doar la analiza legislației, ci trebuie să examineze și arhitectura instituțională și capacitatea reală de implementare. Iar aici se observă o particularitate definitorie a situației moldovenești: nu numai că lipsește o lege integrată privind platformele, dar competențele relevante sunt distribuite între numeroase autorități, fără un centru de coordonare dedicat siguranței digitale, cu precădere a minorilor.

Parlamentul Republicii Moldova are rolul de a adopta cadrul legislativ și de a-l armoniza cu acquis-ul UE, fiind, prin urmare, actorul-cheie pentru acoperirea lacunelor identificate. Ministerul Dezvoltării Economice și Digitalizării este autoritatea de politici în domeniul digital și inițiatorul proiectului de lege privind serviciile digitale, ceea ce îl plasează în centrul reformei viitoare. Ministerul Justiției coordonează politica în materie de drepturi ale copilului și de drept penal, relevant pentru combaterea infracțiunilor digitale. Ministerul Educației și Cercetării are un rol esențial în alfabetizarea digitală, componentă indispensabilă a oricărei abordări care nu se reduce doar la interdicție generală. Ministerul Muncii și Protecției Sociale coordonează politica de protecție a copilului și pe cea de prevenire a violenței în familie.

Pe planul autorităților specializate, CNPDCP este autoritatea de supraveghere în materie de date personale și va deveni, odată cu intrarea în vigoare a noii Legi privind protecția datelor cu caracter personal, autoritatea competentă să asigure respectarea noului regim al consimțământului copiilor. Consiliul Audiovizualului supraveghează protecția minorilor în serviciile media audiovizuale, în temeiul Codului serviciilor media audiovizuale. Agenția pentru Securitate Cibernetică, recent constituită și aflată în proces de operaționalizare, exercită atribuții în domeniul securității rețelelor și sistemelor informatice. În materie de violență, inclusiv digitală, Agenția Națională de Prevenire și Combatere a Violenței împotriva Femeilor și a Violenței în Familie

²⁹Ministerul Dezvoltării Economice și Digitalizării, Comunicat de presă "Lansarea Sub-consiliului pentru Inteligență Artificială și Cercetare Aplicată și prima ședință de lucru interinstituțională", Chișinău, 30.04.2026, disponibil online: <https://mded.gov.md/lansarea-sub-consiliului-pentru-inteligena-artificiala-si-cercetare-aplicata-si-prima-sedinta-de-lucru-interinstitutionala/>.

are un rol central, alături de Poliție și de Procuratură, care asigură constatarea și urmărirea penală a infracțiunilor. Avocatul Poporului pentru drepturile copilului asigură o funcție de garantare și monitorizare a drepturilor copilului, iar Consiliul pentru egalitate supraveghează respectarea principiului nediscriminării. Această cartografiere relevă problema instituțională centrală. Niciuna dintre autoritățile enumerate nu deține, în prezent, un mandat de supraveghere a platformelor digitale comparabil cu cel al unui Coordonator al serviciilor digitale din Uniunea Europeană, prevăzut de DSA. Competențele sunt sectoriale și parțial suprapuse: protecția datelor revine unei autorități, conținutul audiovizual alteia, infracțiunile digitale altora, iar protecția consumatorului încă altora. Riscurile generate de designul platformelor, de algoritmii de recomandare sau de profilarea minorilor cad, în bună măsură, între aceste mandate, fără a fi acoperite pe deplin de niciunul. De asemenea, nu este clar ce instituție ar putea solicita și evalua informații tehnice complexe privind algoritmii sau mecanismele de moderare ale platformelor.

Proiectul de lege privind serviciile digitale, propus de către MDED, desemnează Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI), care în prezent a devenit Agenția Națională pentru Reglementare în Comunicații (ARCOM), în calitate de Coordonator al serviciilor digitale. Instituirea Coordonatorului serviciilor digitale ar oferi punctul de convergență important care lipsește astăzi, dar eficacitatea sa va depinde de resursele umane și financiare alocate și de claritatea delimitării competențelor față de autoritățile existente, pentru a evita atât vidul de responsabilitate, cât și suprapunerile. Dincolo de resurse și de delimitarea competențelor, alegerea autorității care va exercita funcția de Coordonator este ea însăși o chestiune de fond. Rolul Coordonatorului este, în esență, unul de supraveghere a platformelor și a conținutului, evaluarea riscurilor sistemice, a sistemelor de recomandare și a mecanismelor de moderare, mai apropiat de profilul unei autorități de reglementare a mass-mediei decât de cel al unei autorități de comunicații electronice. În Republica Moldova, competențele cele mai apropiate de acest mandat sunt deținute de Consiliul Audiovizualului, care supraveghează deja platformele de partajare video. Această observație nu tranșează, la nivel de diagnostic, identitatea viitorului Coordonator, dar arată că opțiunea instituțională trebuie analizată în funcție de compatibilitatea mandatului.

Sinteza lacunelor sistemice și concluzie de diagnostic intern

Analiza cadrului normativ național efectuată mai sus facilitează o privire de ansamblu. Tabloul normativ al Republicii Moldova aferent protecției minorilor în spațiul digital poate fi descris prin următoarea metaforă:

țara dispune de cărămizi, dar nu de o construcție. Analiza a identificat șapte lacune sistemice:

- 1) *Prima lacună privește temelia sistemului:* Legea nr. 370/2023 privind drepturile copilului oferă un cadru general al drepturilor copilului, dar nu îl extinde explicit asupra mediului digital.
- 2) *A doua lacună ține de paradigma reglementării conținutului:* Legea nr. 30/2013 privind protecția copiilor împotriva impactului negativ al informației operează cu logica filtrării conținutului dăunător, depășită în raport cu abordarea DSA, axată pe responsabilizarea platformelor.
- 3) *A treia lacună este una de domeniu de aplicare:* Codul serviciilor media audiovizuale protejează minorii în audiovizual, dar nu acoperă rețelele sociale ca atare.
- 4) *A patra lacună privește protecția datelor și verificarea vârstei:* regimul datelor reglementează consimțământul minorului, dar nu și verificarea proporțională a vârstei sau accesul la platforme.
- 5) *A cincea lacună (cea mai importantă) este lipsa unui regim modern al serviciilor digitale:* Legea nr. 284/2004 serviciile societății informaționale (comerțul electronic) rămânând ancorată în logica clasică a comerțului electronic, fără a prelua logica DSA de responsabilizare a furnizorilor.

6) *A șasea lacună privește protecția consumatorului-minor*: acest segment este acoperit generic de Legea nr. 105/2003 privind protecția consumatorilor, care, deși a fost aliniată standardelor UE din domeniu, nu abordează separat protecția consumatorilor-minori.

7) *A șaptea lacună ține de funcția preventivă în materie penală*: Codul penal consolidat sancționează abuzul după producerea sa, dar practic nu acoperă partea preventivă.

La aceste șapte lacune se adaugă o carență transversală, de natură diferită, fiindcă privește o tehnologie care străbate toate palierele de mai sus – inteligența artificială. Sistemele de inteligență artificială nu reprezintă un sector separat, ci stratul care alimentează astăzi cele mai multe dintre mecanismele analizate, de la sistemele de recomandare care decid ce conținut ajunge la un minor, până la moderarea automată, publicitatea comportamentală și generarea de conținut sintetic, inclusiv materialele sexualizate de tip deepfake, care pot afecta semnificativ bună-starea minorilor vizați prin astfel de conținut malițios.

Dreptul european a adoptat în această privință un instrument dedicat – AI Act, care interzice, printre altele, sistemele ce exploatează vulnerabilitățile legate de vârstă pentru a distorsiona comportamentul unei persoane într-un mod care îi poate cauza un prejudiciu, protecție direct relevantă pentru copii. Dreptul moldovenesc nu dispune încă de un cadru echivalent, ci doar de semnarea, în septembrie 2024, a Convenției-cadru a Consiliului Europei privind inteligența artificială, care stabilește principii generale, dar nu echivalează cu regimul detaliat de interdicții și obligații al Regulamentului UE.

Privite împreună, aceste lacune conduc la o concluzie certă. Problema reală a Republicii Moldova nu este absența oricărei reglementări, ci caracterul fragmentat, incomplet și parțial depășit al celei existente. Normele actuale acoperă anumite riscuri reale, dar o fac dispersat, prin acte și autorități diferite, și operează preponderent cu o logică anterioară erei AI, axată pe conținut și pe răspunderea intermediarilor, nu pe responsabilizarea proactivă a furnizorilor pentru modul în care își proiectează serviciile. Aici se află distanța față de modelul european: nu în lipsa unor obiective de protecție, ci în absența mecanismelor moderne care, în Uniune, transformă aceste obiective în obligații concrete și verificabile pentru platforme.

Reforma aflată în curs răspunde, în bună parte, tocmai acestor lacune, ceea ce îi conferă o importanță deosebită pentru orice politică publică în domeniu. Proiectul de lege privind serviciile digitale ar acoperi nucleul lacunelor legate de responsabilizarea platformelor, de design și de supraveghere, inclusiv prin instituirea Coordonatorului serviciilor digitale, autoritatea care lipsește astăzi din arhitectura instituțională. Inițiativele în materie de inteligență artificială ar urma să acopere, la rândul lor, carența transversală privind lipsa reglementării sistemelor bazate pe inteligență artificială. Cu alte cuvinte, statul a identificat deja, în linii mari, direcția de remediere, iar aceasta se apropie de modelul european. Două precizări rămân însă necesare pentru o evaluare realistă. Pe de o parte, cu excepția proiectului privind serviciile digitale, aceste inițiative se află într-un stadiu incipient, astfel încât efectele lor concrete și momentul producerii lor rămân incerte. Pe de altă parte, niciuna dintre ele nu este construită specific în jurul protecției minorilor, ceea ce înseamnă că adoptarea lor, deși necesară, nu garantează prin ea însăși acoperirea tuturor riscurilor analizate în prezentul studiu. Rămâne de analizat în ce măsură nevoile specifice ale minorilor vor fi integrate în aceste viitoare act normativ sau document de politici publice.

Privite din perspectiva de gen, cele șapte lacune relevă și o problemă transversală de coerență a răspunsului public. Cadrul existent nu permite încă identificarea sistematică, prin date dezagregate, a diferențelor de expunere, victimizare și impact asupra fetelor și băieților, iar mecanismele de raportare și intervenție nu sunt articulate în mod clar între sistemul de protecție a copilului și cel de prevenire și combatere a violenței împotriva femeilor și fetelor. Această disociere este relevantă în special în cazul adolescentelor, întrucât unele forme de abuz digital se află simultan la intersecția protecției copilului, a prevenirii violenței bazate pe

gen și a obligațiilor platformelor. Perspectiva de gen nu constituie, prin urmare, o lacună distinctă, ci un criteriu transversal de evaluare și remediere a celor șapte lacune deja identificate.

Constatările prenotate au o consecință directă, deși nu predetermină soluția. Întrucât lacunele identificate privesc modul în care platformele funcționează, iar nu simpla prezență a copilului în mediul online, ele orientează atenția către măsuri care acționează asupra designului, transparenței și responsabilității furnizorilor, mai degrabă decât asupra excluderii copilului din spațiul digital. Diagnosticul nu indică, prin el însuși, care dintre direcțiile de reglementare este preferabilă. Această alegere urmează a se face după evaluarea echidistantă a celor trei scenarii și în lumina experienței altor state, analizată în secțiunea ce urmează. Ceea ce diagnosticul arată cu claritate este natura problemei pe care o reglementare eficientă trebuie să o rezolve: nu prezența copiilor în mediul digital, ci modul în care platformele sunt proiectate, supravegheate și responsabilizate, precum și nevoia ca soluția aleasă să fie însoțită de capacitatea instituțională efectivă de a o aplica, inclusiv în privința sistemelor bazate pe inteligență artificială.

Aspecte conceptuale: minorul - subiect vulnerabil, dar activ digital

Orice dezbateră privind reglementarea accesului minorilor la platformele digitale trebuie să pornească de la realitatea contemporană: **minorii se află deja masiv și permanent în spațiul digital**. Nu este vorba despre un fenomen emergent, ci este tabloul actual al practic oricărei societăți contemporane. Această realitate condiționează întreaga arhitectură normativă care urmează, în sensul că reglementarea nu vine să prevină un acces care încă nu există, ci vine să structureze, să protejeze și să responsabilizeze un mediu în care copiii sunt deja actori activi.

Cine este „minorul”? O definiție în evoluție

Punctul de plecare al oricărei analize juridice în acest domeniu îl constituie definirea noțiunii de minor. Convenția ONU privind drepturile copilului din 1989³⁰, în vigoare pentru Republica Moldova din 1993, oferă definiția de referință la nivel internațional, specificând la articolul 1 că, copil este orice ființă umană sub vârsta de 18 ani, cu excepția cazurilor în care legea aplicabilă stabilește majoratul la o vârstă mai mică. Această definiție generală este preluată practic de toate instrumentele europene relevante.

În mediul digital, însă, noțiunea de minor nu poate fi tratată rigid. Legislația europeană analizată mai sus abordează noțiunea de minor în mod diferit, în funcție de scopul specific al fiecărui act. DSA utilizează termenul „minor” în mod consistent, fără a fixa o vârstă-prag, lăsând statelor membre sarcina de a determina, prin trimitere la dreptul intern, granița dintre minor și major. AI Act practic nu utilizează termenul „minor” explicit (cu excepția de la considerentul (9)), ci se referă la „vulnerabilitățile legate de vârstă” ca temei al interdicțiilor privind sistemele de inteligență artificială manipulative. Aceasta este o abordare mai flexibilă, care nu ancorează protecția la o vârstă fixă, ci la o caracteristică de vulnerabilitate demonstrabilă. GDPR introduce, prin articolul 8, o vârstă specifică pentru consimțământul digital, specificând că prelucrarea datelor unui copil în relație cu serviciile societății informaționale este licită doar dacă acesta are cel puțin 16 ani, fiind posibilă coborârea acestei limite până la 13 ani.

Această abordare diferențiată nu este o incoerență legislativă, ci o reflecție principiului că copilul nu este o categorie uniformă și rigidă, ci un subiect de drept aflat în evoluție, ale cărui capacități cognitive, emoționale și de discernământ se construiesc în timp. Un copil de 7 ani, un adolescent de 13 ani și un tânăr de 16 ani nu

³⁰ Organizația Națiunilor Unite, *Convenția cu privire la drepturile copilului*, adoptată de Adunarea Generală a ONU la 20 noiembrie 1989, intrată în vigoare la 2 septembrie 1990, disponibil online:

<https://www.unicef.org/moldova/media/1401/file/Conventia-cu-privire-la-drepturile-copilului.pdf>.

au același nivel de maturitate și nevoi digitale, deci confruntă riscuri diferite. Aceasta înseamnă că o politică publică serioasă trebuie să distingă între vârste, tipuri de servicii digitale, niveluri de risc și măsuri de protecție. Minorul trebuie privit din două perspective. Pe de o parte, este un subiect vulnerabil, care necesită protecție specială, pe motivul experienței de viață, din cauza vârstei mici. Pe de altă parte, este un titular de drepturi, capabil să participe pe deplin la viața socială, educațională și civică, inclusiv prin mijloace digitale. Ba mai mult, această participare este încurajată și bine-venită pentru edificarea unei societăți reziliente și prospere. Această dublă perspectivă este esențială. Dacă accentul cade exclusiv pe vulnerabilitate, soluția tinde spre interdicții și control excesiv. Dacă accentul cade exclusiv pe autonomie, se poate ajunge la subestimarea riscurilor reale. Reglementarea trebuie să păstreze echilibrul între protecție și participare.

Tabloul statistic privind prezența minorilor în spațiul digital

Datele disponibile la nivelul UE confirmă că prezența tinerilor în mediul online este universală și în continuă creștere. Conform datelor Eurostat pentru 2025³¹, 98% dintre tinerii cu vârste cuprinse între 16 și 29 de ani din Uniunea Europeană utilizau internetul zilnic, față de 90% din totalul populației. Rețelele sociale reprezentau, în același an, spațiul digital preferat pentru 89% dintre acești tineri, un nivel stabil menținut timp de aproape un deceniu. 60% dintre tinerii europeni au utilizat instrumente de inteligență artificială generativă în trimestrul anterior sondajului, dublu față de totalul populației. Această diferență majoră de folosire a sistemelor bazată pe inteligență artificială arată că tinerii sunt mult mai deschiși la adoptarea noilor tehnologii informaționale. Datele pentru categoriile de vârstă mai mici sunt și mai relevante. Cercetarea EU Kids Online³², desfășurată de o rețea de cercetători europeni cu sprijinul Comisiei Europene și care a cuprins 25.101 de copii cu vârste între 9 și 16 ani din 19 țări, documentează că majoritatea copiilor chestionați raportau folosirea smartphone-ului „zilnic” sau „aproape tot timpul”, iar timpul petrecut online s-a dublat față de studiul precedent din 2010, ajungând între două și trei ore și jumătate pe zi, în funcție de țară. Practica de a accesa platformele social media înainte de vârsta minimă admisă este sistematică. Studiile arată că o proporție semnificativă din copii sub 13 ani dețin deja profiluri pe platforme al căror prag minim de acces este tocmai 13 ani, ocolind restricțiile prin declararea unor date de naștere false. Aceasta este exact vulnerabilitatea identificată de Comisia Europeană în procedura împotriva Meta din 29 aprilie 2026, menționată mai sus.

Pentru Republica Moldova cifrele sunt similare. Potrivit unui sondaj din 2024³³, prezența minorilor în mediul digital nu este marginală, ci masivă, indicând că 97% dintre copiii din clasele V–XI sunt online zilnic, iar doar 3% au acces restricționat la internet în zilele de școală. Studiul mai constată că aproape toți copiii au acces la internet și dispozitive mobile, indiferent de mediul familial sau de nivelul de vulnerabilitate socială. Aceeași cercetare arată că 93% dintre copii au cel puțin un cont sau profil pe rețele sociale. Copiii din clasele V–IX preferă într-o măsură mai mare TikTok, cei din clasele X–XI folosesc mai mult Instagram, iar copiii din categorii vulnerabile aleg preponderent TikTok. Rețelele sociale sunt folosite în special pentru comunicare,

³¹ Eurostat, *Young people - digital world*, date extrase martie 2026, disponibil online: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Young_people_-_digital_world.

³² Smahel, David, MacHackova, Hana, Mascheroni, Giovanna, Dedkova, Lenka, Staksrud, Elisabeth, Olafsson, Kjartan, Livingstone, Sonia, Hasebrink, Uwe (2020), *EU Kids Online 2020: survey results from 19 countries*. Technical Report. EU Kids Online, The London School of Economics and Political Science, London, UK, disponibil online: <https://researchonline.lse.ac.uk/id/eprint/103294/>.

³³ Data for Impact (D4I), *Children's Safety in the Digital Environment: Republic of Moldova*, Report No. TR-24-588, 2024, 2024, University of North Carolina at Chapel Hill, disponibil online: https://www.data4impactproject.org/wp-content/uploads/2024/10/D4I-Report-Childrens-Safety-in-the-Digital-Environment_TR-24-588_508c.pdf.

socializare și petrecerea timpului liber: 64% pentru comunicare, 59% pentru socializare și 46% pentru timp liber, în timp ce doar 27% le folosesc pentru dezvoltare personală, inclusiv pregătirea temelor.

Timpul petrecut online este, la rândul său, semnificativ. În zilele de școală, doar 14% din copii folosesc internetul mai puțin de o oră, 51% dintre elevii din clasele V–XI folosesc internetul între 1 și 3 ore, iar 32% mai mult de 3 ore. În zilele libere sau în vacanță, 41% dintre copii petrec online mai mult de 4 ore. Copiii din categorii vulnerabile sau care dispun de comunicare și suport părintesc mai puțin tind să petreacă mai mult timp online decât copiii fără vulnerabilitate socială.

Aceste date sunt foarte importante și trebuie citite cu prudență. Studiul menționat nu acoperă regiunea transnistreană și exclude copiii de 15–17 ani care nu continuă studiile după absolvirea clasei a IX-a. Prin urmare, datele sunt utile pentru înțelegerea tendințelor și elaborarea politicilor.

Datele naționale privind minorii nu sunt însă dezagregate pe sexe, ceea ce constituie o limitare suplimentară, cu efect direct asupra politicilor publice. Acolo unde dezagregarea există, ea privește populația adultă și indică o distribuție puternic inegală a riscului. Studiul național „Violența digitală împotriva femeilor în Republica Moldova”, realizat sub coordonarea Centrului Internațional „La Strada” cu sprijinul UNFPA pe un eșantion reprezentativ de 1.016 respondenți, constată că femeile sunt afectate în mod disproporționat, cele mai ridicate niveluri de victimizare fiind înregistrate în segmentul de vârstă 18–29 de ani, iar circa 70% dintre incidente producându-se pe rețelele de socializare. Cercetarea regională UN Women „The Dark Side of Digitalization” arată, la rândul ei, că tinerele de 18–24 de ani sunt de patru ori mai expuse decât femeile de peste 65 de ani, prevalența pe parcursul vieții în Republica Moldova fiind de 65,4%. Întrucât aceste cercetări nu includ minorii, ele nu pot fi citite ca date despre copii. Concentrarea victimizării în cea mai tânără grupă de vârstă măsurată susține însă concluzia că expunerea nu începe la 18 ani, ci în adolescență. La nivel european, raportul Child Safety Online, elaborat în iulie 2026 de copreședinții Special Panel on Child Safety Online, sintetizează cercetări potrivit cărora fetele petrec, în general, mai mult timp pe rețelele sociale și folosesc mai frecvent funcțiile de conversație online, în timp ce băieții petrec mai mult timp în jocurile online. Același raport citează un studiu potrivit căruia până la 63% dintre fete în Europa au raportat o formă de hărțuire online pe rețelele sociale. Aceste constatări nu pot fi extrapolate automat asupra minorilor din Republica Moldova, dar evidențiază necesitatea colectării periodice a datelor naționale dezagregate pe sexe, vârstă, tip de platformă și formă de victimizare.

În completarea acestui studiu, un mini-chestionarul consultativ realizat în cadrul proiectului confirmă aceeași tendință: minorii și tinerii consultați folosesc intens rețelele sociale, iar interdicțiile formale sunt percepute ca ușor de ocolit. Din cele 71 de răspunsuri colectate, 91,5% dintre respondenți au indicat că, în cazul unei interdicții totale, tinerii ar găsi căi de ocolire, iar 73,2% au declarat că, la crearea primului cont, au indicat o vârstă mai mare decât cea reală. Totodată, 66,2% au menționat că părinții nu le limitează sau controlează deloc folosirea rețelelor sociale ori a telefonului.

Aceste rezultate nu au valoarea unui sondaj reprezentativ la nivel național, dar oferă un indiciu empiric relevant pentru analiza de politici publice: protecția minorilor în mediul digital nu poate fi bazată doar restricționarea accesului, or, așa cum declară aproape toți tinerii chestionați, aceștia vor găsi cu certitudine soluții de eludare a restricțiilor. Fezabilitatea tehnică a limitării accesului minorilor la platforme evident obstructive (pornografie, promovarea vădită a violenței, sinuciderii, sau altor fenomene nocive) nu poate fi construită exclusiv pe interdicții de acces sau pe control parental, ci trebuie să includă obligații efective

pentru platforme, mecanisme proporționale de verificare a vârstei, educație digitală și instrumente accesibile de raportare.

Vulnerabilitatea digitală: un risc sporit pentru minori

Având în vedere datele enunțate, întrebarea de politici publice nu este dacă minorii se află sau nu în spațiul digital. Ei sunt deja acolo în mod masiv și constant. Întrebarea reală este cum poate fi făcut acest spațiu mai sigur, mai transparent și mai adecvat vârstei, fără a elimina disproporționat accesul copiilor la comunicare, informare, educație și participare civică.

Vulnerabilitatea minorului în mediul digital nu se reduce la lipsa de experiență. Ea este amplificată de modul în care sunt proiectate serviciile digitale. Platformele folosesc tehnici complexe ce pot crea chiar dependență de utilizarea serviciilor prestate. Aceste mecanisme pot influența comportamentul tuturor utilizatorilor, dar îi afectează mai intens pe copii, deoarece aceștia sunt încă în proces de dezvoltare cognitivă, emoțională și socială. Reglementările europene recunosc explicit această specificitate, iar GDPR subliniază în considerentul (38) că minorii pot fi mai puțin conștienți de riscurile, consecințele și garanțiile legate de prelucrarea datelor lor, în special în scopuri de marketing și profilare, și că această caracteristică justifică o protecție sporită. Dar doctrina de specialitate merge mai departe și arată că vulnerabilitatea copilului în mediul online nu derivă exclusiv din caracteristicile individuale ale copilului, cum ar fi vârsta, experiența redusă, capacitatea cognitivă în formare, ci este în bună măsură generată de structura mediului digital însuși³⁴. Arhitectura interfețelor, mecanismele de captare și reținere a atenției, personalizarea algoritmică a conținutului și opțiunilor sunt proiectate pentru a maximiza angajamentul utilizatorului, indiferent de vârstă. Aplicat unui minor, același mecanism produce efecte cu o intensitate sporită, tocmai pentru că rezistența cognitivă și evaluarea critică sunt mai reduse.

Această perspectivă are o consecință directă pentru elaborarea politicilor publice în domeniu, deoarece protecția minorilor în mediul digital nu se mai poate construi exclusiv pe cunoașterea, de către copil, a riscurilor la care se expune. Ea trebuie să se adreseze mediului digital însuși, prin influențarea designului platformelor, algoritmilor de recomandare, modelelor comerciale care exploatează datele utilizatorilor, etc. Riscurile concrete la care sunt expuși copiii pe internet pot fi sistematizate în cinci categorii, pe care Orientările Comisiei Europene din 14 iulie 2025 în privința DSA le preiau și le extind față de clasificarea inițială a cercetătorilor europeni Sonia Livingstone și Mariya Stoilova³⁵:

- 1. Riscuri de conținut:** expunerea la materiale dăunătoare, violente, sexuale, de dezinformare sau care promovează auto-vătămarea.
- 2. Riscuri de contact:** abordarea minorului de persoane rău-intenționate, grooming, urmărire, hărțuire, manipulare sau exploatare.
- 3. Riscuri de conduită:** comportamente dăunătoare în care minorul poate fi implicat ca martor, participant sau victimă, inclusiv bullying-ul online, partajarea de conținut inadecvat.

³⁴ Helberger Natali, Sax Marijn, Strycharz Joanna, Micklitz Hans-W., „Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability”, *Journal of Consumer Policy*, vol. 45, nr. 2, 2022, disponibil online: https://pure.uva.nl/ws/files/72200873/Helberger2022_Article_ChoiceArchitecturesInTheDigita.pdf.

³⁵ Livingstone Sonia, Stoilova Mariya, *The 4Cs: Classifying Online Risk to Children*, Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut, 2021, disponibil online: https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf.

- 4. Riscuri de consumator:** abonamente cu costuri ascunse, publicitate comportamentală, profilare comercială, publicitate țintită, practici neloiale etc.
- 5. Riscuri transversale:** care privesc confidențialitatea, sănătatea mentală și tratamentul echitabil, indiferent de categoria principală de risc.

Aceste categorii de risc nu afectează însă fetele și băieții în mod identic. Raportul Child Safety Online, elaborat în 2026 de copreședinții Special Panel on Child Safety Online, sintetizează cercetări care sugerează că fetele sunt mai expuse hărțuirii sexiste și misogine, distribuirii neconsensuale a imaginilor intime și materialelor sexualizate de tip deepfake. Formele de victimizare pot varia și în funcție de vârstă: în cazul fetelor de 13–15 ani sunt semnalate mai frecvent excluderea din conversațiile de grup, umilirea publică, comentariile privind aspectul fizic și afectarea reputației, iar în intervalul 11–18 ani pot apărea forme sexualizate sau de control, inclusiv constrângerea, groomingul și utilizarea abuzivă a imaginilor. Raportul indică, de asemenea, o expunere mai mare a fetelor la comparația socială, presiunea privind imaginea corporală și conținutul care poate favoriza tulburările de alimentație, cu posibile efecte asupra anxietății, depresiei și stimei de sine.

În cazul băieților, utilizarea mai frecventă a jocurilor online poate concentra riscuri asociate folosirii problematice, contactelor periculoase și sănătății mintale. Practica penală națională indică vulnerabilitatea acestora față de racolarea prin platformele online și aplicațiile de mesagerie pentru activități infracționale, în special pentru distribuirea de droguri în calitate de curieri. Raportul Child Safety Online semnalează că vulnerabilitatea băieților față de riscurile cu caracter sexual online poate fi subestimată și că, în situații de cyberbullying, aceștia pot recurge mai frecvent la evitare și la gestionarea individuală a problemei, în loc să solicite ajutor. Diferențele descrise nu justifică măsuri stereotipe, ci impun ca evaluarea riscurilor, setările implicite de siguranță, mecanismele de raportare și serviciile de sprijin să țină cont simultan de vârstă, sex și circumstanțele individuale ale copilului. Formele și implicațiile violenței digitale care afectează disproporționat femeile și fetele, precum și lacunele cadrului național, sunt analizate distinct în raportul Centrului Parteneriat pentru Dezvoltare „Combaterea violenței digitale în bază de gen în Republica Moldova în procesul de aderare la Uniunea Europeană”.

Drepturile copilului ca fundament transversal

Vulnerabilitatea sporită a copiilor nu poate, totuși, să fie apreciată separat de drepturile copiilor și avantajele participării în mediul online. Prevederile DSA, GDPR și AI Act trebuie privite și interpretate în lumina drepturilor fundamentale ale copilului.

Prevederile internaționale

Convenția ONU privind drepturile copilului din 1989, menționată anterior, prevede expres la articolul 13 alineatul (1) că orice copil are dreptul la libertatea de exprimare. Acest drept include libertatea de a căuta, de a primi și de a transmite informații și idei de orice natură, indiferent de frontiere, oral, în scris, tipărit, sub formă artistică sau prin orice alte mijloace alese de copil. În această categorie de mijloace se încadrează, în mod evident, și platformele digitale, rețelele sociale, aplicațiile de comunicare și alte servicii online disponibile. Convenția admite posibilitatea restrângerii acestui drept, însă numai în condiții stricte. Potrivit articolului 13 alineatul (2), orice restricție trebuie să fie prevăzută de lege și necesară pentru respectarea drepturilor sau reputației altor persoane ori pentru protecția securității naționale, ordinii publice, sănătății publice sau moralei publice. În interpretarea standardelor internaționale privind drepturile omului, această limitare trebuie să respecte și cerința proporționalității.

În era digitală, păstrarea echilibrului dintre libertatea și protecția copiilor în spațiul virtual a fost clarificată și consolidată prin adoptarea Comentariului general nr. 25 (2021)³⁶ al Comitetului ONU pentru Drepturile Copilului. Acest document strategic clarifică modul în care Convenția cu privire la drepturile copilului trebuie implementată în epoca internetului, a rețelelor sociale și a inteligenței artificiale. Documentul recunoaște oficial că drepturile prevăzute de Convenție se aplică pe deplin și în mod egal în mediul digital, oferind statelor piloni necesari pentru a naviga între oportunitățile tehnologice și riscurile specifice internetului. Comentariul general aduce trei contribuții fundamentale la interpretarea modernă a Convenției:

□ *Libertatea de exprimare întărită*: Documentul subliniază că platformele digitale au devenit spații vitale pentru exercitarea drepturilor prevăzute la articolul 13. Statele au obligația nu doar de a **nu restricționa abuziv** accesul copiilor la internet, ci și de a le asigura o conectivitate sigură, echitabilă și accesibilă ca preț pentru a-și face auzită vocea.

□ *Proiectarea siguranței din start (Safety by Design)*: În privința restrângerii drepturilor din motive de protecție (conform articolului 13 alin. 2 al Convenției), Comentariul mută o mare parte din responsabilitate de pe umerii copilului sau ai părintelui către furnizorii de tehnologie. Companiile și rețelele sociale sunt obligate să aplice setări de confidențialitate stricte în mod implicit și să elimine din designul algoritmilor elementele care creează dependență sau expun copiii la conținut dăunător și profilare comercială.

□ *Echilibrul proporționalității*: Comitetul subliniază că măsurile de protecție luate de state sau platforme nu trebuie să devină o formă de cenzură generalizată. Orice limitare a accesului la informație sau a libertății de exprimare online trebuie să fie strict proporțională, fundamentată juridic și axată exclusiv pe interesul superior al copilului.

Astfel, Comentariul general nr.25 din 2021 transformă textul Convenției din 1989 într-un instrument viu, asigurându-se că transformarea digitală servește dezvoltării reziliente și participării civile a copiilor, fără a le compromite siguranța, datele personale, sănătatea mintală și fizică.

Prevederile europene

Legea comunitară include și ea prevederi care vin să întărească protecția drepturilor fundamentale ale minorilor. Articolul 24 din Carta drepturilor fundamentale a Uniunii Europene³⁷ prevede că fiecare copil are dreptul la protecția și îngrijirea necesare pentru bunăstarea sa, că își poate exprima liber opinia, iar interesul superior al copilului trebuie să fie o considerație primordială în toate acțiunile care îl privesc. Regula menționată mai sus are două consecințe majore:

- I. Statul are obligația de a proteja copilul împotriva riscurilor reale din mediul digital.
- II. Protecția nu trebuie să anuleze participarea copilului la viața socială, educațională și civică.

Minorii nu sunt doar beneficiari pasivi ai protecției statului. Ei sunt titulari de drepturi, inclusiv dreptul la exprimare liberă, informare, asociere, educație și participare, inclusiv în demiul digital.

³⁶ Comitetul ONU pentru Drepturile Copilului, *Comentariul general nr. 25 (2021) privind drepturile copiilor în legătură cu mediul digital*, Doc. ONU CRC/C/GC/25, disponibil online:

<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=3wwrH9vtD%2BoythbnJGI1Dqn5y4fFzaSP11aNXvcuXv5C3K2aqoc2AKAhAk6WnfcPIfKx15lvKF0lmmtkhxb4eA%3D%3D>.

³⁷ Parlamentul European, Consiliul și Comisia, *Carta drepturilor fundamentale a Uniunii Europene*, JO C 202/389, 07.06.2016, pp. 389-405, disponibil online: https://eur-lex.europa.eu/eli/treaty/char_2016/oj#.

Strategia UE privind drepturile copilului³⁸ și Strategia *Better Internet for Kids Plus* (BIK+)³⁹ consolidează această abordare. BIK+ promovează o viziune bazată pe trei direcții:

- i. protecția copiilor în mediul online;
- ii. împuternicirea lor prin competențe digitale;
- iii. participarea lor la modelarea mediului digital.

Strategia subliniază că minorii trebuie să fie protejați, respectați și împuterniciți online, nu excluși automat din spațiul digital. Această perspectivă este importantă pentru studiul de față. O politică publică privind accesul minorilor la platforme nu trebuie să pornească doar de la riscuri, ci și de la **beneficiile participării digitale**. Rețelele sociale, aplicațiile de mesagerie, platformele educaționale și spațiile digitale de participare pot avea roluri importante în informare, socializare, educație, exprimare și mobilizare civică. Prin urmare, soluțiile normative trebuie să fie proporționale și să evite tratamentul minorului ca simplu obiect al protecției prin prohibiție.

Aceste prevederi arată că accesul minorilor la spațiul digital nu poate fi tratat exclusiv ca o problemă de control sau interdicție. Platformele digitale sunt și mijloace prin care copiii își exercită libertatea de exprimare, accesul la informație, participarea socială și dezvoltarea competențelor digitale. O interdicție generală, aplicată uniform tuturor minorilor indiferent de vârstă, de natura platformei sau de tipul de conținut, ridică prin însuși caracterul său absolut probleme serioase de compatibilitate cu cadrul normativ internațional și european. Același standard s-ar impune și atunci când verificarea vârstei sau consimțământul parental sunt instituite ca mecanism de acces. Dacă modalitățile concrete de implementare conduc la excluderea practică a minorilor din spațiul digital, efectul normei ar putea echivala, chiar fără intenție, cu o restricție disproporționată.

Prin urmare, orice măsură de limitare a accesului minorilor la rețele sociale sau la alte servicii digitale trebuie să fie clar prevăzută de lege, să urmărească un scop legitim, să fie necesară într-o societate democratică și să fie proporțională cu riscul real urmărit. O interdicție generală sau excesiv de largă, nefundamentată pe dovezi și neînsoțită de garanții adecvate, ar putea ridica probleme serioase de compatibilitate cu drepturile fundamentale ale copilului. Aceste considerente nu exclud total reglementarea modului de utilizare a platformelor digitale de către minori. Totuși, este mai rezonabil și conform principiilor internaționale ca protecția minorilor în mediul digital să fie construită în jurul riscurilor generate de comportamentul platformelor, nu în jurul prezenței în sine a copilului în spațiul digital.

Cadrul european include și instrumente relevante pentru prevenirea infracțiunilor și formelor grave de prejudiciere a minorilor în mediul digital. Directiva 2011/93/UE privind combaterea abuzului sexual asupra

³⁸Comisia Europeană, Comunicare către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, *Strategia UE privind drepturile copilului*, COM(2021) 142 final, Bruxelles, 24.03.2021, disponibil online: <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52021DC0142&from=EN>.

³⁹Comisia Europeană, Comunicare către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, *Un deceniu digital pentru copii și tineri: noua strategie europeană pentru un internet mai bun pentru copii (Better Internet for Kids, BIK+)*, COM(2022) 212 final, Bruxelles, 11.05.2022, disponibil online: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=COM%3A2022%3A212%3AFIN>.

copiilor⁴⁰, Convenția de la Lanzarote⁴¹ și Convenția de la Budapesta⁴² oferă repere importante pentru combaterea exploatării sexuale, groomingului, distribuției materialelor de abuz sexual asupra copiilor și altor forme de criminalitate digitală. Aceste instrumente sunt relevante deoarece o parte dintre riscurile analizate în prezentul studiu se află la intersecția dintre protecția copilului, securitatea cibernetică și dreptul penal. Platformele digitale pot facilita contactul cu persoane rău-intenționate, distribuirea imaginilor intime, hărțuirea, șantajul, generarea de conținut sexualizat prin inteligență artificială sau groomingul.

În astfel de cazuri, reglementarea platformelor are și o funcție preventivă. Mecanisme eficiente de raportare, moderarea conținutului, limitarea recomandărilor nocive, verificarea proporțională a vârstei și cooperarea cu autoritățile – pot reduce riscul ca minorii să devină victime digitale. Din perspectivă conceptuală, „protecția” nu trebuie confundată cu „restricția”. Protecția urmărește reducerea riscurilor reale pentru copil, cu păstrarea posibilității de participare. Restricția limitează accesul sau anumite funcționalități, inclusiv și cele benefice și chiar necesare. Împuternicirea digitală reprezintă o componentă esențială. Copilul trebuie să fie ajutat să înțeleagă mediul online, să recunoască riscurile, să știe unde poate cere ajutor și să poată folosi tehnologia în mod responsabil. Totuși, această componentă este inutilă fără responsabilizarea furnizorilor. Această distincție este importantă pentru evaluarea celor trei scenarii de reglementare. Scenariul restrictiv pornește de la protecție prin interdicție. Scenariul moderat pornește de la acces condiționat. Scenariul progresiv pornește de la responsabilizarea platformelor și capacitate digitală a utilizatorilor, cu precădere minorii. Analiza acestor scenarii trebuie să țină cont de faptul că minorul este, simultan, vulnerabil și activ digital. El are nevoie de protecție, dar și de acces la informație, comunicare, educație, socializare, participare. În concluzie, minorul nu poate fi tratat nici ca adult digital, nici ca subiect complet pasiv. El este o persoană în dezvoltare, cu drepturi proprii, cu vulnerabilități specifice și cu o prezență reală în spațiul online. O reglementare adecvată trebuie să pornească de la această realitate. Scopul nu trebuie să fie eliminarea copilului din mediul digital, ci transformarea acestui mediu într-un spațiu mai sigur, mai transparent, mai responsabil și mai adecvat vârstei.

Analiza comparativă a situației din alte țări

Analiza comparativă nu urmărește identificarea unui model străin care ar putea fi transpus mecanic în Republica Moldova. Sistemele examinate funcționează în contexte instituționale, tehnice și politice diferite, iar utilitatea lor constă în lecțiile pe care le oferă, scopul final fiind de a aduce claritate cu privire la următoarele aspecte: ce tip de intervenție a fost ales, asupra cui stă obligația principală, cum este tratată verificarea vârstei utilizatorului, ce rol revine părinților și ce riscuri apar la aplicare. Pentru a evita efectuarea unei analize comparative haotice, modelele analizate au fost grupate în patru categorii de reglementare:

⁴⁰ Parlamentul European și Consiliul, Directiva 2011/93/UE din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului, JO L 335, 17.12.2011, disponibil online: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32011L0093>.

⁴¹ Consiliul Europei, *Convenția pentru protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale (Convenția de la Lanzarote)*, CETS nr. 201, deschisă spre semnare la Lanzarote la 25 octombrie 2007, ratificată de Republica Moldova prin Legea nr. 263 din 19 decembrie 2011, disponibil online: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=201>.

⁴² Consiliul Europei, *Convenția privind criminalitatea informatică (Convenția de la Budapesta)*, CETS nr. 185, deschisă spre semnare la 23 noiembrie 2001, ratificată de Republica Moldova prin Legea nr. 6 din 2 februarie 2009, disponibil online: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

- i. limitarea accesului prin praguri de vârstă și consimțământ parental – pentru acest model au fost selectate țările **Franța și Danemarca**;
- ii. responsabilizarea furnizorilor și supravegherea instituțională, fără interdicție generală – **Germania și Irlanda** fiind considerate țările cele mai potrivite pentru analiză;
- iii. modelul în tranziție, construit pe obligația de diligență a platformelor („*duty of care*”) și orientat recent spre restricții de acces – țara cea mai reprezentativă fiind **Regatul Unit**;
- iv. modelul restrictiv, bazat pe interdicția funcțională de acces – prima țară din lume care a adoptat acest model fiind **Australia**.

Această structură permite legarea exemplelor de cele trei scenarii analizate ulterior: restrictiv, moderat și progresiv; fără a prejudeca recomandările finale.

În acest domeniu, distincția dintre legislație adoptată, proiect de lege, acord politic și orientare administrativă este esențială, deoarece dezbaterea publică evoluează rapid, iar unele state au anunțat măsuri restrictive fără ca acestea să fi devenit încă regimuri juridice în vigoare. Pentru Republica Moldova, aflată în proces de aderare la UE, precizia contează dublu: orice soluție națională trebuie raportată nu doar la oportunitatea politică internă, ci și la compatibilitatea cu DSA, GDPR, AI Act, cu drepturile fundamentale ale copilului protejate la nivel european și cu principiul proporționalității.

Un reper rămâne constant pe parcursul acestei analize: la data analizei, **niciun stat membru al UE nu a adoptat o interdicție totală și operațională a accesului minorilor la rețelele sociale**. Statele europene folosesc fie praguri de vârstă cu acces condiționat, fie obligații de diligență pentru platforme, în timp interdicția efectivă și intenția anunțată de a interzice accesul provin din afara Uniunii.

Franța și Danemarca: modelul hibrid, bazat pe praguri de vârstă, consimțământ parental și restricționare parțială

Franța și Danemarca pornesc de la ideea că accesul autonom al minorilor la rețele sociale poate fi condiționat până la o anumită vârstă, ceea ce le face relevante pentru scenariul moderat.

Franța este, dintre statele membre, cea care a împins cel mai departe ambiția de a limita prin lege accesul minorilor la rețelele sociale, iar tocmai traiectoria ei oferă Republicii Moldova lecția cea mai instructivă despre constrângerile dreptului Uniunii. O legea din iulie 2023⁴³ a stabilit un „majorat digital” la 15 ani, stipulând că, furnizorii de rețele sociale care își desfășoară activitatea în Franța ar urma să refuze înscrierea minorilor sub 15 ani în absența autorizării unui titular al autorității părintești, să permită părintelui să ceară suspendarea contului și să activeze, la înscrierea unui minor, un dispozitiv de control al timpului de utilizare. Totodată, erau prevăzute sancțiuni financiare pentru furnizori.

Această dispoziție nu a fost însă aplicată, din cauza unor conflicte cu dreptul Uniunii Europene.⁴⁴ Aceste conflicte au fost evidențiate într-o scrisoare a Comisiei Europene din 14 august 2023, care indica:⁴⁵

⁴³ Republica Franceză, Legea nr. 2023-566 din 7 iulie 2023 privind instituirea unui majorat digital și combaterea urii online (art. 4, care inserează art. 6-7 în Legea nr. 2004-575 din 21 iunie 2004), JORF nr. 0157 din 8 iulie 2023, disponibil online: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>.

⁴⁴ Adunarea Națională a Franței, Întrebarea scrisă nr. 5149, Legislatura a XVII-a, Răspuns oficial al Ministrului delegat pe lângă Prim-ministru, însărcinat cu relațiile cu Parlamentul, publicat în JORF nr.0106 din 6 mai 2025, p. 3291, disponibil online: <https://questions.assemblee-nationale.fr/q17/17-5149QE.htm>.

⁴⁵ Comisia Europeană, Sistemul de Informare privind Reglementările Tehnice, Dosarul de notificare TRIS nr. 2023/0362/FR (Franța) – Dispoziții legislative pentru stabilirea unei vârste digitale a majoratului și combaterea incitării

i. încălcarea DSA, care realizează o armonizare maximă (un nivel unic de reglementare la scara întregii Uniuni), ceea ce împiedică un stat membru să impună unilateral platformelor obligații tehnice sau procedurale suplimentare, precum un sistem propriu de măsurare a timpului petrecut online ori o procedură specifică de validare a acordului parental;

ii. nerespectarea principiul țării de origine din legislația europeană, care prevede că o platformă cu sediul european în alt stat membru se supune, în principiu, reglementărilor statului în care este stabilită, astfel încât Franța nu putea impune unilateral sancțiuni unor furnizori stabiliți în altă parte;

iii. vicii de procedură, legea fiind promulgată în 2023 fără a aștepta finalizarea procedurii obligatorii de notificare prealabilă către Comisie.

Aceste aspecte sunt esențial pentru Republica Moldova. Chiar și o soluție moderată, bazată pe consimțământ parental, poate deveni inaplicabilă dacă impune unilateral obligații tehnice suplimentare platformelor stabilite în alte state sau dacă nu respectă arhitectura europeană de reglementare.

Confruntată cu acest blocaj, Franța a reluat demersul în noiembrie 2025 printr-o nouă propunere de lege, care viza protejarea minorilor de riscurile la care îi expune utilizarea rețelelor sociale.⁴⁶ Pentru a evita eroarea din 2023, textul a fost reconstruit, în urma avizului Consiliului de Stat din 8 ianuarie 2026⁴⁷, astfel încât interdicția să nu mai apese exclusiv pe platforme. Conturile deținute de copiii sub 15 ani urmează să devine ilicite în dreptul francez, ceea ce constrânge platformele să se conformeze pe canalul DSA.

În prima jumătate a anului 2026, Parlamentul francez a examinat noua propunere legislativă. În procesul parlamentar au fost discutate mai multe formule. Adunarea Națională a adoptat textul în primă lectură, la 26 ianuarie 2026, optând pentru o interdicție generală a accesului sub 15 ani, cu câteva excepții (enciclopediile colaborative, repertoriile educative sau științifice, platformele de software liber), mesageriile private de tipul WhatsApp fiind sub interdicție.

Senatul a adoptat însă, tot în primă lectură, la 31 martie 2026, o versiune diferită. Raportul Senatului a atras atenția că o interdicție generală și absolută poate ridica probleme de proporționalitate, libertate de exprimare și exercitare a autorității părintești.⁴⁸ Astfel, Senatul a respins interdicția generală în numele libertăților fundamentale și a optat pentru un sistem pe două niveluri, în care platformele calificate drept periculoase ar fi interzise tuturor minorilor sub 15 ani, cu verificarea vârstei, iar celelalte ar fi accesibile cu acordul parental. Întrucât cele două camere au adoptat versiuni diferite, textul nu era, la data analizei, o lege în vigoare, ci continua procedura parlamentară, prin urmare, aceste evoluții trebuie tratate ca inițiative legislative în curs, nu ca regim definitiv aplicabil. Mai mult, Guvernul francez însuși consideră această inițiativă legislativă expusă riscului de neconformitate cu dreptul Uniunii și a notificat, la 9 aprilie 2026, Comisia Europeană în acest

la ură din mediul online, observațiile Comisiei emise la 14 august 2023), disponibil online: <https://technical-regulation-information-system.ec.europa.eu/ro/notification/23884>.

⁴⁶ Adunarea Națională și Senatul Franței, Proiect de lege privind protecția minorilor împotriva riscurilor legate de utilizarea rețelelor sociale, disponibil online: https://www.assemblee-nationale.fr/dyn/17/dossiers/proteger_mineurs_reseaux_sociaux_17e.

⁴⁷ Consiliul de Stat (Franța), Aviz asupra proiectului de lege privind protecția minorilor împotriva riscurilor legate de utilizarea rețelelor sociale, 8 ianuarie 2026, disponibil online: https://www.assemblee-nationale.fr/dyn/17/textes/l17b2107_avis-conseil-etat.pdf.

⁴⁸ Senatul Franței, Raportul nr. 468 (2025-2026) întocmit în numele Comisiei pentru cultură, educație, comunicare și sport asupra propunerii de lege privind protecția minorilor împotriva riscurilor legate de utilizarea rețelelor sociale, Paris, 25 martie 2026, disponibil online: https://www.senat.fr/rap/l25-468/l25-468_mono.html.

sens.⁴⁹ Prin acest mecanism de notificare prealabilă, Executivul de la Paris a recunoscut vulnerabilitățile juridice în raport cu legislația UE, în special riscul repetat de neconformitate cu DSA.

În paralel, Franța a adoptat măsuri funcționale în domenii unde marja națională de acțiune este mai clară. Cea mai avansată reglementare vizează accesul minorilor la conținut pornografic online. Legea din 2024 privind securizarea și reglementarea spațiului digital, cunoscută ca Legea SREN,⁵⁰ a consolidat competențele Autorității de Reglementare a Comunicării Audiovizuale și Digitale din Franța (ARCOM) și a impus furnizorilor de servicii care difuzează conținut pornografic obligația de a implementa sisteme de verificare a vârstei conforme unui referențial (orientări) tehnic⁵¹. Acest referențial, publicat în octombrie 2024, cere protecția minorilor înainte de accesarea conținutului, soluții eficiente împotriva eludării și garanții de protecție a vieții private, inclusiv prin prestatori independenți și mecanisme de tip „dublu anonimat” – în loc să oblige platformele din alte state membre să folosească sisteme proprii franceze de colectare a datelor (fapt ce încălca GDPR și DSA), noile reglementări franceze se bazează pe utilizarea EU Digital Identity Wallet (Portofelul de Identitate Digitală al UE). Acest fapt asigură o „dublă anonimitate”: **furnizorul de identitate confirmă vârsta fără a ști ce site vizitează utilizatorul, iar platforma află doar că utilizatorul are peste 15 ani, fără a-i colecta datele personale**. O lecție relevantă pentru Moldova.

Practica relevantă a CJUE. Această direcție franceză a fost consolidată recent de către jurisprudența Curții de Justiție a Uniunii Europene (CJUE). Prin hotărârea sa din 16 iunie 2026, în cauzele conexe C-188/24 și C-190/24⁵², Curtea a confirmat că un stat membru poate, în anumite condiții, să impună furnizorilor stabiliți în alte state membre obligații de verificare a vârstei pentru site-uri pornografice. În speță, operatorii unor platforme pornografice stabiliți în Republica Cehă au contestat Legea franceză nr. 2024-449 din 21 mai 2024 privind securizarea și reglementarea spațiului digital, care le impunea măsuri stricte de verificare a vârstei pentru a împiedica accesul minorilor. Companiile au invocat că regulile încalcă Directiva 2000/31/CE privind comerțul electronic, deoarece serviciile lor ar trebui reglementate exclusiv de statul de stabilire – Cehia („principiul țării de origine”). Curtea a decis că statele membre nu pot impune o obligație generală și abstractă de verificare a vârstei tuturor platformelor stabilite în alte state membre prin reguli generale. Totuși, legislația UE permite autorităților dintr-un stat membru (ex. Franța) să oblige un furnizor concret cu sediul în alt stat membru (ex. Cehia) să implementeze aceste sisteme, dacă măsura este necesară pentru protecția minorilor și respectă condițiile de proporționalitate din Directiva privind comerțul electronic. Hotărârea este relevantă, dar nu trebuie extrapolată automat la toate rețelele sociale. Ea privește un domeniu cu risc ridicat și conținut evident inadecvat minorilor, cum ar fi pornografia.

Măsuri suplimentare. Pe lângă eforturile de reglementare a rețelelor sociale, Franța a implementat cu succes măsuri concrete în zone unde dreptul european îi permite să acționeze. O legea franceză din 2022 privind

⁴⁹ Guvernul Franței, Notificarea nr. 2026/0143/F cu privire la proiectului de lege privind protecția minorilor împotriva riscurilor legate de utilizarea rețelelor sociale, 9 aprilie 2026, disponibil online: <https://technical-regulation-information-system.ec.europa.eu/en/notification/27828>.

⁵⁰ Republica Franceză, Legea nr. 2024-449 din 21 mai 2024 privind securizarea și reglementarea spațiului digital, JORF nr. 0117 din 22 mai 2024, disponibil online: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049563368/2026-06-21>.

⁵¹ ARCOM (Franța), Orientări tehnice privind verificarea vârstei pentru protecția minorilor împotriva pornografiei online, 11 octombrie 2024, disponibil online: <https://www.arcom.fr/se-documenter/espace-juridique/textes-juridiques/referentiel-technique-sur-la-verification-de-lage-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne>.

⁵² CJUE, Cauzele conexe C-188/24 (*WebGroup Czech Republic și NKL Associates*) și C-190/24 (*Coyote System*), hotărârea din 16 iunie 2026, disponibil online: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62024CJ0188>.

consolidarea controlului parental, cunoscută ca Legea Studer,⁵³ obligă ca dispozitivele conectate la internet (smartphones, tablete, laptopuri) vândute în Franța să includă un sistem de control parental ușor accesibil, a cărui activare să fie propusă gratuit la prima punere în funcțiune. Acest sistem trebuie să fie capabil să blocheze descărcarea aplicațiilor cu conținut dăunător. O altă lege franceză din 2020 reglementează activitatea minorilor influenceri,⁵⁴ inclusiv prin mecanisme de autorizare, protecție a remunerației și drepturi specifice legate de imaginea copilului. Există un cadru legal strict care protejează copiii care generează venituri pe platformele video (YouTube, TikTok), limitându-le orele de muncă online și obligând părinții să depună câștigurile într-un cont bancar blocat până la majorat. Potrivit legii franceze, dispozitivele electronice destinate minorilor trebuie să afișeze mesaje clare de avertizare pe ambalajul exterior cu privire la riscurile pe care utilizarea excesivă a ecranelor le are asupra dezvoltării copiilor.

Aceste soluții arată că Franța nu acționează doar prin limitarea accesului, ci și prin reguli privind dispozitivele, conținutul, monetizarea imaginii copilului și responsabilitatea adulților. Pentru Republica Moldova, lecția principală a modelului francez este una de prudență. Pragul de 15 ani și consimțământul parental pot inspira scenariul moderat, dar numai dacă sunt însoțite de mecanisme proporționale de verificare a vârstei, compatibile cu protecția datelor și cu standardele europene. Verificarea vârstei nu trebuie să devină o obligație generală de colectare a actelor de identitate, imaginilor faciale sau datelor biometrice ale minorilor. În aceeași direcție merge și soluția europeană de verificare a vârstei, care urmărește dovada vârstei fără transmiterea identității, datei nașterii sau istoricului de navigare către platforme – principiul dublului anonim. Prin urmare, Franța este relevantă pentru Republica Moldova nu ca model de copiat integral, ci ca avertisment metodologic. Ea arată că protecția minorilor online poate justifica reguli ferme, dar aceste reguli trebuie calibrate atent. O reglementare națională care vizează rețelele sociale trebuie să fie compatibilă cu DSA, GDPR, AI Act și principiul țării de origine (având în vedere excepțiile recente consacrate prin practica CJUE), să evite colectarea excesivă de date și să păstreze un echilibru între protecție, participarea tinerilor, libertatea de exprimare și rolul părinților.

Danemarca merge într-o direcție apropiată de modelul francez, dar mai puțin consolidată juridic. În noiembrie 2025, Guvernul danez și partidele semnatare au încheiat un acord politic privind protecția digitală a copiilor,⁵⁵ prin care s-a convenit introducerea, prin lege, a unei limite naționale de 15 ani pentru accesul la anumite rețele sociale. Regula propusă pornește de la premisa că minorii sub 15 ani nu ar trebui, ca principiu, să aibă acces la platformele care îi pot expune la conținut sau funcționalități dăunătoare, dar admite o excepție: părinții pot permite accesul de la vârsta de 13 ani. Acordul nu vizează toate serviciile digitale, ci platformele mari care permit crearea de profiluri publice și sunt asociate cu riscuri documentate pentru copii și adolescenți, inclusiv design adictiv, conținut ilegal sau conținut dăunător.

Aplicarea practică a acestui model este concepută în legătură cu verificarea vârstei și cu DSA. Acordul danez precizează că limita de vârstă urmărește să activeze obligații de verificare a vârstei în logica orientărilor europene privind protecția minorilor în temeiul DSA. Între timp, Danemarca a făcut un pas tehnic important,

⁵³ Republica Franceză, Legea nr. 2022-300 din 2 martie 2022 privind consolidarea controlului parental asupra mijloacelor de acces la internet, JORF nr. 0052 din 3 martie 2022, disponibil online: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT0000045287677>.

⁵⁴ Republica Franceză, Legea nr. 2020-1266 din 19 octombrie 2020 privind reglementarea exploatarei comerciale a imaginii copiilor sub 16 ani pe platformele online, JORF nr. 0255 din 20 octombrie 2020, disponibil online: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT0000042439054>.

⁵⁵ Ministerul digitalizării (Danemarca), Acord politic privind protecția digitală a copilului, 7 noiembrie 2025, disponibil online: <https://www.digmin.dk/digitalisering/nyheder/nyhedsarkiv/2025/nov/ny-politisk-aftale>.

adoptând în februarie 2026 legea privind portofelul național de identitate digitală, iar în iunie 2026 a lansat aplicația AltID, care permite cetățenilor să își verifice vârsta sau să se identifice într-un mod mai ușor și mai sigur. Aceasta este disponibilă persoanelor de peste 13 ani și include un certificat de vârstă ce poate fi utilizat pentru verificare anonimă a vârstei de către servicii online, inclusiv rețele sociale.

Totuși, existența acestui instrument tehnic nu echivalează cu intrarea în vigoare a unei interdicții legale generale pentru minorii sub 15 ani. Prin urmare, Danemarca nu trebuie prezentată ca stat care a adoptat deja o interdicție aplicabilă de acces al minorilor la rețele sociale. Ea trebuie tratată, la fel ca Franța, ca exemple de orientare politică europeană spre stabilirea ”majoratului digital” și spre combinarea unui prag de vârstă cu consimțământ parental, verificare proporțională a vârstei, stabilirea unei infrastructuri sigure de identitate digitală și aplicarea acestor măsuri în logica DSA. Lecția comună oferită de Franța și Danemarca este că scenariul moderat poate îmbrăca mai multe forme: prag de acces autonom, consimțământ parental sub acest prag, verificare proporțională a vârstei, limitarea unor funcționalități de risc și informare adaptată minorilor. Totuși, aceste măsuri nu funcționează izolat.

Germania și Irlanda: modelul non-prohibiționist, bazat pe responsabilizarea furnizorilor și supravegherea instituțională

Germania și Irlanda ilustrează o abordare diferită de modelele bazate pe interdicție sau pe praguri generale de acces. Accentul nu cade pe excluderea minorilor de pe rețelele sociale, ci pe responsabilizarea furnizorilor, clasificarea riscurilor, protecția față de conținutul dăunător, mecanismele de raportare, controlul parental, verificarea proporțională a vârstei și supravegherea instituțională.

Germania are o tradiție îndelungată de protecție a minorilor în media, construită nu în jurul unei vârste minime generale pentru accesul la rețele sociale, ci în jurul protecției copiilor și adolescenților față de conținuturile, serviciile și funcționalitățile care le pot afecta dezvoltarea. Cadrul german se sprijină pe Legea privind protecția tinerilor (*Jugendschutzgesetz*)⁵⁶ și pe Tratatul interstatal privind protecția minorilor în media (*Jugendmedienschutz-Staatsvertrag – JMStV*)⁵⁷, a cărui versiune revizuită este în vigoare de la 1 decembrie 2025. Noul cadru menține protecția față de conținuturile dăunătoare, dar include mai clar și riscurile care nu provin doar din conținut, ci din modul de utilizare a serviciului: funcții de comunicare și contact, funcții de cumpărare, mecanisme asemănătoare jocurilor de noroc, stimularea utilizării excesive, transmiterea datelor către terți fără consimțământ și apeluri comerciale neadecvate vârstei.

Particularitatea modelului german constă în combinarea reglementării publice cu mecanisme de co-reglementare și auto-reglementare supravegheată. Statul stabilește standardele, iar organismele recunoscute ale furnizorilor pot participa la clasificarea conținutului, evaluarea mijloacelor tehnice și aplicarea regulilor, sub controlul autorităților publice. Furnizorii pot recurge, în funcție de natura serviciului, la clasificări pe categorii de vârstă, programe de protecție a minorilor, sisteme de verificare a vârstei pentru conținuturi sensibile, control parental sau alte mijloace tehnice. Autoritatea centrală în domeniu este Comisia

⁵⁶ Germania, Legea privind protecția tinerilor din 23 iulie 2002 (*Jugendschutzgesetz – JuSchG*), publicată în Monitorul Oficial Federal (*Bundesgesetzblatt I*, p. 2730), cu modificările ulterioare, disponibil online: <https://www.gesetze-im-internet.de/juschg/BJNR273000002.html>.

⁵⁷ Germania. Tratatul interstatal privind protecția minorilor în mass-media din 25 ianuarie 2002 (*Jugendmedienschutz-Staatsvertrag – JMStV*), aprobat prin legile de ratificare ale landurilor federale, cu modificările ulterioare, disponibil online: https://www.kjm-online.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/JMStV/JMStV_english_version.pdf.

pentru protecția minorilor în media (KJM),⁵⁸ care supraveghează aplicarea JMStV, recunoaște organismele de auto-reglementare, evaluează sistemele tehnice și examinează încălcările.

Irlanda este relevantă din două perspective: (i) poziția sa în ecosistemul european al platformelor și (ii) arhitectura sa de siguranță online. Modelul irlandez se întemeiază pe Legea privind siguranța online și reglementarea mass-media din 2022 (*Online Safety and Media Regulation Act 2022*),⁵⁹ care a creat Comisia pentru mass-media (*Coimisiún na Meán*) și a extins cadrul de reglementare media asupra siguranței online, inclusiv prin posibilitatea adoptării unor coduri de siguranță online.

Pe baza acestei legi, Comisia pentru mass-media a adoptat Codul privind siguranța online (*Online Safety Code*), primul cod obligatoriu de siguranță online al Irlandei.⁶⁰ Codul transpune logica articolului 28b din Directiva serviciilor media audiovizuale⁶¹ și se aplică nu tuturor rețelelor sociale, ci serviciilor de platformă de partajare video aflate sub jurisdicția irlandeză sau desemnate ca atare. Această delimitare este importantă: Irlanda nu a instituit o interdicție generală de acces la rețele sociale și nu a creat un regim aplicabil tuturor serviciilor digitale folosite de minori. Reglementarea vizează, în principal, conținutul video, conținutul generat de utilizatori, comunicările comerciale audiovizuale și mecanismele de protecție împotriva conținutului dăunător.

Codul a fost adoptat în octombrie 2024. Obligațiile generale au început să se aplice din noiembrie 2024, iar obligațiile detaliate, inclusiv cele care implicau adaptări tehnice, din 21 iulie 2025.⁶² Codul impune platformelor să protejeze copiii față de conținut video care le poate afecta dezvoltarea fizică, mentală sau morală, precum și față de conținut destinat exclusiv adulților. Măsurile pot include clasificarea conținutului, verificarea sau asigurarea vârstei, control parental, mecanisme de raportare și semnalare, instrumente de educație media și reguli privind comunicările comerciale care se adresează copiilor.

Această delimitare trebuie păstrată pentru a nu transforma modelul irlandez într-un regim general al rețelelor sociale. În același timp, rolul Irlandei depășește domeniul strict al serviciilor de partajare video. Comisia pentru mass-media este și Coordonatorul serviciilor digitale pentru Irlanda în sensul DSA. Aceasta supraveghează platformele online stabilite în Irlanda, iar pentru platformele online foarte mari și motoarele de căutare foarte mari responsabilitatea este partajată cu Comisia Europeană.⁶³ Din acest motiv, Irlanda are o relevanță practică specială: multe platforme importante sunt stabilite în Irlanda, iar modul în care autoritatea irlandeză aplică DSA are efecte asupra întregului ecosistem european.

⁵⁸ Despre Comisia pentru protecția minorilor în media (KJM): <https://www.kjm-online.de/en/about-us/>.

⁵⁹ Republica Irlanda, Online Safety and Media Regulation Act 2022 (No. 41 of 2022), disponibil online: <https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/html>.

⁶⁰ Comisia pentru mass-media (Irlanda), *Online Safety Code*, adoptat la 21 octombrie 2024, disponibil online: <https://www.cnam.ie/industry-and-professionals/online-safety-framework/online-safety-code/>.

⁶¹ Parlamentul European și Consiliul, Directiva 2010/13/UE (Directiva serviciilor mass-media audiovizuale), astfel cum a fost modificată prin Directiva (UE) 2018/1808 - art. 28b privind protecția minorilor pe platformele de partajare video, disponibil online: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02010L0013-20181218>.

⁶² Comunicare oficială a Comisiei pentru mass-media (Irlanda), 21 octombrie 2024, disponibil online: <https://www.cnam.ie/coimisiun-na-mean-adopts-final-online-safety-code/>.

⁶³ Comunicare oficială a Comisiei pentru mass-media (Irlanda), disponibil online: <https://www.cnam.ie/industry-and-professionals/broadcasting-on-demand-digital/online-platforms/>.

Merită de subliniat că, în elaborarea *Online Safety Code*, Comisia a desfășurat consultări publice ample și a consultat propriul Comitet consultativ pentru tineret.⁶⁴ Această practică este direct relevantă pentru Republica Moldova, or, o reformă care privește accesul minorilor la platforme digitale trebuie să includă consultarea reală a adolescenților, nu doar consultarea instituțiilor și a adulților. În 2026, această abordare a fost continuată printr-un Forum pentru tineret privind siguranța online, organizat pentru copii și tineri cu vârste între 10 și 17 ani, inclusiv pe tema verificării vârstei și a unei posibile vârste minime legale pentru accesul la social media.⁶⁵

Actualitatea modelului irlandez trebuie formulată prudent. Irlanda nu a adoptat, la acest moment, o interdicție generală de acces la social media pentru persoanele sub 16 ani. Totuși, Guvernul irlandez explorează, în coordonare cu alte state membre și la nivelul UE, opțiuni privind restricțiile de vârstă pentru utilizarea rețelelor sociale, cu accent pe minorii sub 16 ani. În paralel, Irlanda dezvoltă un "Portofel digital guvernamental" care ar putea susține verificarea vârstei într-un mod mai sigur și mai puțin intruziv. Aceste evoluții arată o posibilă apropiere politică de dezbaterile europene privind „majoratul digital”, dar nu schimbă încă natura juridică a modelului irlandez.⁶⁶

Germania și Irlanda arată că protecția poate fi construită fără excludere generală, dar cu obligații ferme pentru furnizori și cu supraveghere reală. Această orientare răspunde direct uneia dintre cele mai importante lacune naționale – absența unui regim modern al serviciilor digitale, construit după logica DSA. Un asemenea regim ar trebui să includă cel puțin interzicerea publicității bazate pe profilare adresate minorilor, transparența sistemelor de recomandare, reguli împotriva designului manipulator, mecanisme accesibile de raportare și un sistem de evaluare și atenuare a riscurilor sistemice.

Regatul Unit și Australia: modelul restrictiv, bazat pe interdicție generală

Regatul Unit și Australia indică direcția mai restrictivă a dezbaterii internaționale privind reglementarea accesului minorilor la rețele sociale, dar nu trebuie confundate. Regatul Unit este mai degrabă un model de tranziție, care pornește de la obligații sistemice ale platformelor și se orientează abia recent spre restricții de acces. Australia este modelul restrictiv propriu-zis, cu o interdicție funcțională deja în vigoare. Deși ambele state nu sunt membre UE, analiza acestora este benefică, deoarece va permite aprecierea fezabilității și oportunității preluării modelului mai restrictiv.

Regatul Unit a adoptat Legea privind siguranța online din 2023 (*Online Safety Act 2023*),⁶⁷ care impune furnizorilor de servicii online obligația de a evalua riscurile pentru copii și de a-i proteja, sub supravegherea autorității de reglementare – Ofcom. Logica legii nu este interzicerea accesului, ci obligația de diligență. Un

⁶⁴ Comitet consultativ pentru tineret (Irlanda), Raport privind consultarea privind proiectul de Cod privind siguranța online, disponibil online: <https://www.cnam.ie/app/uploads/2024/11/Youth-Advisory-Committee-Report.pdf>.

⁶⁵ Comunicatul oficial de presă a Ministerului pentru Cultură, Comunicații și Sport (Irlanda), Youth Forum on Online Safety, Dublin, 2 iunie 2026, disponibil online: <https://www.gov.ie/en/department-of-culture-communications-and-sport/press-releases/minister-odonovan-updates-government-on-online-safety-progress-keeping-young-people-safe-online-a-priority/>.

⁶⁶ Comunicatul oficial de presă a Ministerului pentru Cultură, Comunicații și Sport (Irlanda), Keeping Young People Safe Online a Priority, Dublin, 10 decembrie 2025, disponibil online: <https://www.gov.ie/en/department-of-culture-communications-and-sport/press-releases/minister-odonovan-updates-government-on-online-safety-progress-keeping-young-people-safe-online-a-priority/>.

⁶⁷ Parlamentul Regatului Unit, *Online Safety Act 2023* (c.50), sancțiune regală 26 octombrie 2023, disponibil online (prezentare): <https://www.gov.uk/government/collections/online-safety-act>.

serviciu susceptibil să fie accesat de copii trebuie să realizeze o evaluare a riscurilor și să aplice măsuri de protecție, inclusiv verificarea vârstei acolo unde este necesar, în special pentru a limita accesul la pornografie și la conținut care promovează sinuciderea, autovătămarea sau tulburările de alimentație.

De la 25 iulie 2025, platformele au obligația legală de a aplica metode robuste de verificare a vârstei pentru astfel de conținuturi. Modelul britanic mută astfel sarcina de la copil și părinte către furnizor. O platformă nu poate invoca formal că nu se adresează copiilor dacă, în practică, aceștia o pot accesa.

Asupra acestui cadru s-a suprapus, în 2026, o evoluție importantă. Prin Legea privind bunăstarea copiilor și școlile din 2026 (*Children's Wellbeing and Schools Act 2026*),⁶⁸ care a primit sancțiunea regală la 29 aprilie 2026, Guvernul a obținut competența de a impune, prin legislație secundară, restricții de acces sau de funcționalitate pentru minorii sub 16 ani, printr-o modificare adusă Legii privind siguranța online. Respectiv, în iunie 2026, Guvernul Regatului Unit a anunțat intenția de a folosi această competență pentru a interzice accesul minorilor sub 16 ani la anumite servicii de social media,⁶⁹ cu reglementări preconizate a fi prezentate Parlamentului până la finele anului 2026 și o intrare în vigoare estimată în primăvara anului 2027. Această măsură a fost precedată de o amplă consultare publică, „Growing up in the online world”⁷⁰, care a strâns peste 116.000 de răspunsuri.

Particularitatea britanică este că restricția anunțată nu înlocuiește modelul „*duty of care*”, ci se adaugă peste el. De aceea, Regatul Unit trebuie tratat ca model de tranziție, iar posibila restricție de acces sub 16 ani trebuie privită strict ca dezvoltare în curs de operaționalizare, nu ca regim deja aplicabil. Conex, ține de subliniat că, supravegherea britanică acordă o atenție specifică riscurilor diferențiate pe criterii de gen, autoritatea Ofcom desfășurând o linie de lucru separată siguranței online a femeilor și fetelor. Aceasta este o dimensiune relevantă, dată fiind expunerea mai accentuată a fetelor la conținut potențial dăunător.

Australia reprezintă reperul-limită al scenariului restrictiv. Prin Legea de modificare privind vârsta minimă pe rețelele sociale (*Online Safety Amendment (Social Media Minimum Age) Act 2024*),⁷¹ care a modificat Legea privind siguranța online din 2021, Australia a introdus o vârstă minimă de 16 ani pentru anumite platforme sociale. Regimul este aplicabil din 10 decembrie 2025 și obligă platformele vizate să ia „măsuri rezonabile” pentru a împiedica crearea sau menținerea conturilor de către utilizatorii sub 16 ani aflați în Australia. Responsabilitatea de bază revine platformelor, iar copiii și părinții nu sunt sancționați, și, spre deosebire de modelul franco-danez, nu există o excepție întemeiată pe consimțământul parental.

Modelul australian este important tocmai pentru că testează limitele scenariului restrictiv. Primele date privind aplicarea ridică însă întrebări serioase: autoritatea australiană de siguranță online (eSafety) a constatat, într-un raport din martie 2026, că o proporție substanțială a minorilor sub 16 ani și-au păstrat

⁶⁸ Parlamentul Regatului Unit, *Children's Wellbeing and Schools Act 2026* (c. 21), Partea 3 (modificarea Online Safety Act 2023), sancțiune regală 29 aprilie 2026, disponibil online: <https://www.legislation.gov.uk/ukpga/2026/21/part/3/enacted>.

⁶⁹ Departamentul pentru Știință, Inovație și Tehnologie (Regatul Unit), *Fact sheet: New rules to protect children online*, 19 iunie 2026, disponibil online: <https://www.gov.uk/government/publications/fact-sheet-new-rules-to-protect-children-online/fact-sheet-new-rules-to-protect-children-online>.

⁷⁰ Departamentul pentru Știință, Inovație și Tehnologie (Regatul Unit), *Growing up in the online world: a national consultation* (2 martie – 26 mai 2026), disponibil online: <https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation>.

⁷¹ Parlamentul Australiei, *Online Safety Amendment (Social Media Minimum Age) Act 2024* (nr. C2024A00127, care modifică Online Safety Act 2021), sancțiune regală 10 decembrie 2024, disponibil online: <https://www.legislation.gov.au/C2024A00127/asmade/text>.

conturile ori și-au creat altele noi,⁷² iar un sondaj realizat de Molly Rose Foundation împreună cu panelul de tineret YouthInsight, pe 1.050 de copii de 12–15 ani, a arătat că 61% dintre cei care aveau conturi pe platforme restricționate înainte de interdicție păstrau accesul la cel puțin un cont, iar dintre cei care continuau să le folosească, 70% au considerat că eludarea interdicției a fost „ușoară”.⁷³

Pentru Republica Moldova, Australia este utilă pentru a testa proporționalitatea și fezabilitatea unei interdicții, nu ca model de transpunere directă: ea arată că o interdicție sub 16 ani poate fi formulată juridic și plasată în sarcina platformelor, dar că, în lipsa unor mecanisme tehnice robuste, a cooperării reale cu furnizorii și a unei capacități administrative pe măsură, riscă să creeze o aparență de protecție fără a reduce substanțial riscurile. În plus, fiind un stat din afara Uniunii, Australia nu este ținută în aceeași măsură de DSA, GDPR, AI Act și de jurisprudența europeană privind proporționalitatea, ceea ce limitează transferabilitatea modelului.

Concluzii comparative și relevanța pentru Republica Moldova

Analiza comparativă confirmă că nu există un model unic. Franța și Danemarca alimentează scenariul moderat, prin folosirea pragurilor de vârstă și a consimțământului parental. Germania și Irlanda alimentează scenariul progresiv, prin accentul pus pe obligațiile furnizorilor și pe supraveghere. Regatul Unit arată tranziția de la obligații sistemice spre restricții de acces, iar Australia alimentează scenariul restrictiv.

Trei lecții se desprind cu putere pentru Republica Moldova:

- 1) orice soluție întemeiată pe vârstă depinde de verificarea vârstei, iar aceasta trebuie să fie proporțională, sigură și conformă cu protecția datelor. Altfel, măsura poate genera riscuri mai mari decât cele pe care încearcă să le reducă.
- 2) responsabilitatea nu poate fi transferată exclusiv părinților sau copiilor, deoarece platformele controlează arhitectura serviciilor, sistemele de recomandare, publicitatea, interfețele și mecanismele de captură a atenției. Siguranța prin proiectare (integrarea protecției încă din faza de concepție a serviciului) este, de aceea, indispensabilă.
- 3) instituțiile contează la fel ca regulile, întrucât, fără o autoritate competentă, expertiză tehnică, proceduri de raportare și capacitate de aplicare, orice reglementare riscă să rămână formală.

Pentru Republica Moldova, o interdicție generală a accesului sub 16 ani ar fi cea mai ușor de comunicat politic, dar și cea mai dificil de justificat juridic, de aplicat tehnic și de aliniat cu drepturile minorilor la exprimare, informare, educație și participare. Un model de acces condiționat, inspirat parțial de Franța și de orientarea daneză, poate fi analizat ca soluție intermediară, însă numai dacă mecanismele de verificare a vârstei și a consimțământului parental nu conduc la colectarea excesivă de date. Un model progresiv, inspirat de Germania, Irlanda și de logica DSA, ar așeza accentul pe obligațiile platformelor, protecția datelor, siguranța prin design, limitarea profilării și consolidarea autorităților. Concluzia de etapă este că nicio soluție nu este suficientă dacă este aplicată izolat: întrebarea reală nu este doar dacă minorii sub o anumită vârstă

⁷²Safety Commissioner (Australia), *Social media age restrictions* (cadru aplicabil de la 10 decembrie 2025; raport de implementare, martie 2026), disponibil online: <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>.

⁷³ Molly Rose Foundation și YouthInsight, *More than 60% of Australian children still using social media despite ban for under-16s* (sondaj pe 1.050 de copii de 12–15 ani, teren 12–31 martie 2026), aprilie 2026, disponibil online: <https://mollyrosefoundation.org/more-than-60-of-australian-children-still-using-social-media-despite-ban-for-under-16s-research-shows/>.

trebuie să aibă acces la rețele sociale, ci ce combinație de reguli, garanții și instituții poate reduce riscurile fără a limita disproporționat participarea lor la viața digitală.

Evaluarea scenariilor de reglementare

Pentru a fundamenta o decizie de politici publice echilibrată și compatibilă cu standardele europene, este necesară examinarea comparativă a principalelor opțiuni de intervenție a statului în spațiul digital. Dezbateră privind siguranța minorilor în mediul online nu se poate rezuma la o alegere binară între inacțiune și interdicție absolută. În acest sens, analiza se structurează în jurul a trei scenarii distincte de reglementare, fiecare propunând o paradigmă diferită privind echilibrul dintre protecție, drepturile fundamentale ale copilului și obligațiile furnizorilor de servicii digitale.

Cele trei scenarii sunt evaluate echidistant, având la bază criterii precum: impactul asupra siguranței, compatibilitatea cu cadrul legal european fezabilitatea tehnică și riscurile de securitate cibernetică.

Scenariul 1 – Model restrictiv: interdicția generală de acces sub 16 ani

Scenariul restrictiv presupune instituirea unei interdicții generale de acces la rețelele sociale pentru persoanele sub 16 ani. În sensul prezentului studiu, interdicția nu ar trebui înțeleasă ca blocare a accesului minorilor la internet sau la toate serviciile digitale. Ea ar viza doar rețelele sociale și platformele online cu funcții sociale relevante: crearea de profiluri, distribuirea de conținut generat de utilizatori, interacțiunea între utilizatori, sisteme de recomandare algoritmică și mecanisme de captare a atenției. Serviciile educaționale, platformele școlare, instrumentele de comunicare familială, serviciile publice digitale și alte servicii cu risc redus nu ar trebuie să cadă sub interdicție.

Argumentul principal în favoarea acestui scenariu este caracterul său preventiv. O interdicție sub 16 ani ar transmite un mesaj politic clar: protecția copiilor prevalează asupra interesului comercial al platformelor. Ea ar putea reduce formal expunerea copiilor mai mici la conținut dăunător, contact abuziv, grooming, cyberbullying, publicitate comportamentală, design adictiv și recomandări algoritmice intruzive. În același timp, ar oferi părinților un reper normativ simplu, mai ușor de aplicat în viața de familie.

În varianta sa juridic mai corectă, acest scenariu nu ar trebui să sancționeze copiii sau părinții. Obligația principală trebuie plasată asupra platformelor, deoarece acestea controlează arhitectura serviciului, sistemele de recomandare, verificarea conturilor, publicitatea, interfețele și mecanismele de raportare. Aceasta este și logica modelului australian: minorii și părinții nu sunt sancționați, iar furnizorii de platforme trebuie să ia măsuri rezonabile pentru a preveni menținerea conturilor de către utilizatori sub 16 ani.

Reperul comparativ principal este Australia, prima jurisdicție care a adoptat un model restrictiv general pentru rețelele sociale. Online Safety Amendment (Social Media Minimum Age) Act 2024 impune platformelor obligația de a lua măsuri rezonabile pentru a împiedica utilizatorii sub 16 ani să dețină conturi pe platforme restricționate (nota de subsol 72). Acest model este util pentru Republica Moldova ca reper-limită, nu ca soluție iminentă. De subliniat că, Australia nu este legată de obligativitate transpunerii sau alinierii cadrului normativ național la standardele UE. Modelul australian arată că o interdicție poate fi formulată juridic, doar că eficiența sa depinde de verificarea veritabilă a vârstei, cooperarea reală a platformelor și capacitatea instituțională de aplicare a interdicției, control și, eventual, sancționare.

Datele inițiale din Australia confirmă că punerea în aplicare a modelului restrictiv este destul de complicată. Pe de o parte, eSafety Commissioner a comunicat că platformele mari au restricționat accesul la aproximativ 4,7 milioane de conturi identificate ca aparținând copiilor sub 16 ani (nota de subsol 73). Pe de altă parte,

primele sondaje ridică întrebări serioase privind eficiența reală a interdicției. Potrivit unui sondaj realizat pe un eșantion de 1.050 de copii australieni de 12–15 ani, 61% dintre copiii care aveau conturi pe platforme restricționate înainte de intrarea în vigoare a interdicției continuau să aibă acces la cel puțin un cont (nota de subsol 74). Mai mult, majoritatea copiilor care continuau să utilizeze platformele au declarat că platformele nu au întreprins nicio acțiune pentru eliminarea conturilor existente. Datele Qustodio, citate de Reuters, indică, la rândul lor, că o parte semnificativă a adolescenților de 13–15 ani continuau să utilizeze TikTok și Snapchat la câteva luni după intrarea în vigoare a interdicției.⁷⁴ Aceste date nu demonstrează inutilitatea totală a interdicției, dar arată că efectul este parțial și dependent de aplicare.

Cazul Franței este la fel de important, dar din alt unghi. Franța a adoptat Legea nr. 2023-566 din 7 iulie 2023 privind instituirea unui majorat digital și combaterea urii online, care prevedea că furnizorii de rețele sociale trebuie să refuze înscrierea minorilor sub 15 ani, cu excepția cazului în care există autorizare parentală (nota de subsol 44). Legea nu a intrat însă efectiv în aplicare, acest fapt fiind condiționat de primirea aprobării Comisiei Europene care să permită considerarea mecanismului ca fiind compatibil cu dreptul UE. Ulterior, Guvernul francez a recunoscut oficial că legea „nu a putut prospera” din cauza fricțiunilor cu dreptul Uniunii Europene. Comisia Europeană a semnalat, în special, probleme privind incompatibilități de fond cu DSA și cu principiul țării de origine, potrivit căruia entitatea se subordonează exigențelor normative din țara unde este înregistrată (nota de subsol 46). Pentru Republica Moldova, această lecție este directă: o reglementare națională privind accesul la rețele sociale, chiar dacă urmărește un scop legitim, poate deveni inaplicabilă sau vulnerabilă dacă nu este construită în logica DSA.

Din perspectiva cadrului european analizat anterior, scenariul restrictiv se îndepărtează de logica dominantă a UE. DSA nu interzice accesul minorilor la platforme, ci obligă platformele accesibile minorilor să asigure un nivel ridicat de confidențialitate, siguranță și securitate, să nu prezinte publicitate bazată pe profilare minorilor, să explice condițiile de utilizare într-un limbaj accesibil și să evalueze riscurile sistemice pentru copii. GDPR nu instituie un prag general de acces la rețele sociale, ci reglementează consimțământul copilului pentru prelucrarea datelor în contextul serviciilor societății informaționale și impune garanții sporite pentru copii. AI Act nu exclude minorii din mediul digital, ci interzice sistemele de inteligență artificială care exploatează vulnerabilitățile legate de vârstă și afectează autonomia comportamentală a persoanei. Prin urmare, o interdicție generală sub un anumit prag nu este automat imposibilă, dar ar trebui justificată printr-un test strict și complicat de necesitate și proporționalitate.

Această problemă devine și mai sensibilă prin prisma drepturilor fundamentale ale copilului. În secțiunile anterioare ale studiului s-a arătat că minorul este vulnerabil, dar nu este un subiect pasiv. El are dreptul la protecție, dar și la exprimare, informare, educație, socializare și participare. Legea nr. 370/2023 privind drepturile copilului garantează copilului dreptul de a-și exprima opinia, dreptul la libera exprimare și dreptul de a căuta, primi și difuza informații prin orice mijloace alese. În aceeași logică, Strategia europeană BIK+ promovează nu doar protecția copiilor online, ci și împuternicirea lor digitală și participarea la modelarea mediului digital. O interdicție generală ar limita direct aceste drepturi și ar trebui demonstrat că obiectivul protecției nu poate fi atins prin măsuri mai puțin intruzive: conturi adaptate vârstei, dezactivarea profilării, restricții de funcționalități, control parental, mecanisme de raportare, design sigur și supraveghere efectivă. Cea mai dificilă componentă rămâne una tehnică – verificarea veritabilă a vârstei. Fără verificare reală, interdicția rămâne declarativă. Cu verificare generalizată, apar riscuri serioase de protecție a datelor și

⁷⁴ REUTERS, *One-fifth of Australian teens still use TikTok, Snapchat after social media ban* (O cincime dintre adolescenții australieni folosesc în continuare TikTok și Snapchat după interzicerea rețelelor sociale), 13 martie 2026, disponibil online: <https://www.reuters.com/business/media-telecom/one-fifth-australian-teens-still-use-tiktok-snapchat-after-social-media-ban-2026-03-13/>.

securitate cibernetică. O platformă nu poate ști cine are sub 16 ani fără a evalua vârsta tuturor utilizatorilor. Mecanismele posibile – documente de identitate, verificare biometrică, estimare facială, furnizori terți de identitate digitală sau declarații pe propria răspundere – au limite evidente. Declarațiile pot fi ușor ocolite. Documentele și datele biometrice sunt intruzive. Estimarea facială poate produce erori. Furnizorii terți pot crea dependențe tehnice și riscuri suplimentare.

Comitetul European pentru Protecția Datelor avertizează expres că verificarea vârstei trebuie realizată într-un mod proporțional, bazat pe risc, cu respectarea minimizării datelor și fără a crea mijloace suplimentare de identificare, localizare, profilare sau urmărire a persoanelor (nota de subsol 4). Această cerință este esențială pentru Republica Moldova. Dacă interdicția sub 16 ani ar fi aplicată prin colectarea generalizată a actelor de identitate, a imaginilor faciale sau a datelor biometrice ale minorilor și părinților, riscul de incompatibilitate cu standardele europene privind protecția datelor ar fi ridicat. Într-un asemenea caz, soluția juridică ar putea genera riscuri mai mari decât cele pe care încearcă să le reducă.

Fezabilitatea tehnică este, de asemenea, limitată. Minorii pot ocoli interdicția prin conturi create cu datele adulților, conturi partajate, rețele private virtuale (VPN), platforme alternative, servicii nereglementate sau declararea falsă a vârstei. O interdicție dură poate produce și efecte nedorite: migrarea spre spații digitale mai opace, reducerea raportării abuzurilor, slăbirea comunicării dintre copii și părinți, precum și falsa impresie că problema siguranței online a fost rezolvată printr-un simplu prag de vârstă.

Particularități tehnice:

În practică, eludarea nu se limitează doar la declararea falsă a vârstei. În cazul mecanismelor bazate pe estimare facială sau verificare biometrică instantanee, minorii pot recurge la metode simple de ocolire, cum ar fi folosirea unui frate mai mare sau a unui părinte în momentul verificării, utilizarea machiajului sau a accesoriilor pentru alterarea estimării faciale, folosirea VPN-urilor ori migrarea către conturi și servicii mai greu de supravegheat. Aceste limite arată că o interdicție generală, fără arhitectură tehnică proporțională și fără obligații reale de reducere a riscurilor la nivelul platformei, poate produce mai curând o aparență de control decât o protecție efectivă.

Pentru Republica Moldova, aplicarea acestui model ar cere o infrastructură instituțională pe care statul nu o are încă pe deplin: un coordonator al serviciilor digitale, competențe clare de control, proceduri de audit tehnic, capacitate de cooperare cu platforme globale, mecanisme de sancționare și expertiză avansată în protecția datelor și securitate cibernetică. În lipsa acestor condiții, interdicția riscă să rămână o normă cu valoare simbolică ridicată, dar cu eficiență practică limitată.

Matricea de evaluare tehnică și juridică

Criteriu de evaluare	Scenariul 1 – Model restrictiv (Interdicție totală sub 16 ani)
Cine verifică vârsta?	Platformele digitale sau furnizorii terți de soluții de identificare. În practică, pentru a bloca minorii, platformele sunt obligate să verifice identitatea și vârsta tuturor utilizatorilor , inclusiv a adulților.
Ce date se colectează?	Date sensibile și puternic intruzive: documente de identitate guvernamentale (buletin, pașaport), date biometrice (scanări faciale, estimare facială prin IA) sau date ale cardurilor bancare.

Unde se stochează?	Cel puțin temporar pe serverele platformelor sau în bazele de date ale companiilor intermediare, existând riscul documentat al reținerii nejustificate a acestora.
Cât de ușor se poate ocoli mecanismul?	Extrem de ușor. Minorii folosesc instrumente precum VPN-urile, acte false, scanări tip „proxy” (folosind un frate mai mare sau părinte) ori machiaj pentru a păcăli sistemele IA. De exemplu, sondajul privind interdicția din Australia a demonstrat că 70% dintre copiii afectați au considerat eludarea restricțiilor drept o sarcină „ușoară”.
Ce riscuri de securitate și protecție a datelor apar?	Risc sistemic de furt de identitate și breșe de date din cauza bazelor de date centralizate. Totodată, abordarea distruge anonimatul online și exclude complet cetățenii vulnerabili care nu posedă acte de identitate guvernamentale.
Ce capacitate instituțională cere?	O capacitate administrativă și tehnică de auditare colosală. Statul ar trebui să aibă capabilitatea să monitorizeze și să sancționeze constant mii de platforme globale, lucru ineficient fără o cooperare internațională.
Cât de compatibil este cu DSA, GDPR și AI Act?	Incompatibil. Colectarea masivă de documente încalcă direct principiul minimizării datelor din GDPR și ignoră recomandările din Declarația EDPB 1/2025 care respinge soluțiile disproporționate. DSA impune un mediu safety-by-design, nu o interdicție generală.
Ce efect are asupra participării minorilor la viața digitală?	Are un efect nociv de segregare și suprimare. Lezează dreptul minorilor la liberă exprimare și informare. Mai grav, restricția împinge tinerii spre zone nereglementate (<i>dark net</i>) sau rețele ascunse, unde expunerea la abuzatori și conținut nociv este și mai mare, lipsind moderarea.

Scenariul 1 (restrictiv) se dovedește a fi cea mai intruzivă și ineficientă abordare. Sub promisiunea politică a creării unui mediu sigur, acest model mută povara protecției de pe reglementarea ecosistemului digital pe o formă de supraveghere generalizată a tuturor utilizatorilor. Interdicția totală nu rezolvă problemele de fond generate de platforme (precum designul manipulator), ci doar exclude minorii, în timp ce adolescenții vor ocoli tehnic aceste bariere cu ușurință. Scenariul restrictiv răspunde ferm unei preocupări sociale reale. El poate fi justificat politic prin nevoia de protecție a copiilor și prin eșecul platformelor de a reduce voluntar riscurile pentru minori. Totuși, analiza comparativă și cadrul european indică limite serioase. Franța arată că o soluție națională bazată pe praguri de vârstă poate deveni inaplicabilă dacă nu respectă DSA și principiul țării de origine. Australia arată că o interdicție poate fi adoptată și plasată în sarcina platformelor, dar aplicarea ei rămâne dificilă, iar o parte importantă a minorilor continuă să acceseze platformele.

Pentru Republica Moldova, interdicția generală de acces sub 16 ani nu ar trebui tratată ca opțiune imposibilă din punct de vedere juridic, dar nici ca soluție preferabilă în forma sa generală. În lipsa unei autorități digitale

consolidate, a unui mecanism proporțional de verificare a vârstei și a unei evaluări riguroase a impactului asupra drepturilor copilului, acest scenariu ar produce un risc ridicat de reglementare simbolică, greu aplicabilă și vulnerabilă față de standardele europene. Elementele utile ale scenariului restrictiv pot fi păstrate doar punctual: obligația platformelor de a preveni accesul copiilor la funcționalități cu risc evident și ridicat (ex. pornografia), lipsa sancționării copiilor și părinților, verificare a vârstei proporțională și măsuri ferme împotriva profilării, designului adictiv și contactului abuziv cu minorii.

Scenariul 2 – Model moderat: acces condiționat

Scenariul moderat pornește de la premisa că accesul autonom al minorilor la rețelele sociale poate fi condiționat până la o anumită vârstă, fără a fi interzis. Minorii nu sunt excluși de pe rețelele sociale, dar accesul lor autonom este condiționat până la o anumită vârstă. Modelul combină trei elemente: prag de vârstă, consimțământ parental pentru minorii aflați sub prag și limitarea unor funcționalități cu risc ridicat. Dintre cele trei opțiuni, scenariul moderat este cel mai apropiat de cadrul intern existent. Legea nr. 195/2024 privind protecția datelor cu caracter personal stabilește, la articolul 8, pragul de 14 ani pentru consimțământul la prelucrarea datelor minorului (în vigoare la 23 august 2026) (nota de subsol 16). Distincția esențială, semnalată deja în diagnostic, este că acesta este un prag de consimțământ la prelucrarea datelor, nu un prag de acces. El stabilește cine poate consimți la prelucrare, dar nu reglementează accesul la platformă și nu instituie un mecanism de verificare a vârstei.

Pe planul *acquis-ului comunitar*, scenariul se ancorează în articolul 8 din GDPR (consimțământul parental sub prag) coroborat cu principiul minimizării datelor (articolul 5), în articolul 28 din DSA (măsuri proporționale pentru minori) și, în mod critic, în articolul 28 alineatul (3), potrivit căruia conformarea nu obligă platformele să prelucreze date suplimentare pentru a stabili dacă utilizatorul este minor, aceasta fiind o limită directă pentru orice mecanism de verificare a vârstei. Reiterăm că, Declarația EDPB 1/2025 (nota de subsol 4) avertizează în același sens că necesitatea stabilirii vârstei nu trebuie să devină pretext pentru colectarea excesivă de date. Proiectul de orientări EDPB 3/2025 privind interacțiunea DSA-GDPR (versiune de consultare) confirmă că o verificare a vârstei trebuie să rămână o soluție care protejează viața privată, minimizează datele și nu presupune stocarea vârstei exacte.⁷⁵

Într-o formă prudentă, scenariul ar putea funcționa astfel: minorii peste prag accesează platformele autonom, dar în regim de protecție sporită. Minorii sub prag pot accesa anumite platforme sau funcționalități doar cu acordul părintelui. Totuși, toate conturile minorilor sunt configurate implicit cu nivel ridicat de confidențialitate și siguranță. Platformele ar trebui să dezactiveze pentru conturile minorilor publicitatea bazată pe profilare, să limiteze recomandările algoritmice intrusive, să ofere mecanisme simple de raportare, să limiteze contactul nesolicitat din partea adulților necunoscuți și să evite funcțiile care stimulează utilizarea excesivă a serviciilor.

Această abordare este mai apropiată de logica DSA decât interdicția generală. DSA cere platformelor accesibile minorilor să adopte măsuri adecvate și proporționale pentru a asigura un nivel ridicat de confidențialitate, siguranță și securitate. DSA interzice publicitatea bazată pe profilare atunci când platforma știe cu o certitudine rezonabilă că utilizatorul este minor. Orientările Comisiei Europene din 14 iulie 2025

⁷⁵ Comitetul European pentru Protecția Datelor (EDPB), *Orientări 3/2025 privind interacțiunea dintre Regulamentul privind serviciile digitale (DSA) și Regulamentul general privind protecția datelor (GDPR)*, versiune adoptată pentru consultare publică la 12 septembrie 2025 (consultare închisă la 31 octombrie 2025; versiunea finală în curs de adoptare), disponibil online: https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf.

privind protecția minorilor dezvoltă aceeași logică: conturi private implicit, reducerea expunerii la conținut dăunător, raportare accesibilă, limitarea funcțiilor adictive și design adecvat vârstei.

Punctul sensibil al scenariului rămâne verificarea vârstei. Dacă se bazează doar pe autodeclarare, mecanismul este slab. Dacă se bazează pe acte de identitate, imagini faciale sau date biometrice, devine intruziv. Soluția acceptabilă este verificarea proporțională sau "dublu anonim". Consimțământul parental este util, dar nu rezolvă singur problema. El poate deveni o simplă formalitate dacă platforma rămâne proiectată pentru captarea atenției, profilare și recomandări agresive. De asemenea, verificarea relației părinte-copil poate presupune prelucrarea unor date suplimentare despre familie.

Lecția franceză trebuie însușită. Franța a încercat printr-o lege din 2023 să instituie un prag de 15 ani ("majoratul digital") și consimțământul parental, însă aceasta a rămas neoperaționalizată, din cauza conflictului cu dreptul UE ([nota de subsol 44](#)). Eroarea necesară de evitat este impunerea unilaterală de obligații tehnice platformelor stabilite în alte state, ceea ce e contrar principiului țării de origine. Soluția mai robustă juridic, sugerată de abordarea daneză, constă în ancorarea verificării într-o infrastructură națională de identitate, nu în obligații tehnice impuse direct platformelor. Orice obligație de verificare opozabilă platformelor străine ar trebui să treacă, și aici, prin calea individuală a derogării, nu printr-o obligație generală; or, pragul „riscului grav și serios” nu este automat îndeplinit pentru rețelele sociale generaliste.

Particularități tehnice:

O soluție tehnică intermediară este folosirea indicatorilor de vârstă și a setărilor de siguranță la nivel de cont, dispozitiv sau ecosistem digital, nu doar la nivelul fiecărei platforme. În practică, acest lucru poate include conturi de copil configurate în sistemele de operare majore (ex. iOS, Android sau Windows), limite de timp pentru aplicații, aprobarea instalării unor aplicații de către părinte, filtrarea conținutului, blocarea cumpărăturilor sau restricționarea mesajelor de la persoane necunoscute. Pot exista și aplicații dedicate care filtrează conținutul sau blochează anumite tipuri de materiale pe dispozitivul copilului. Aceste instrumente pot reduce nevoia ca fiecare platformă să colecteze documente de identitate sau date biometrice, dar nu pot fi tratate ca soluție completă. Ele depind de configurarea corectă de către adult, de faptul că minorul folosește propriul dispozitiv, de posibilitatea de a accesa serviciul de pe alt telefon și de capacitatea minorilor de a dezactiva, ocoli sau evita aceste controale.

Matricea de evaluare tehnică și juridică

Criteriu de evaluare	Scenariul 2 – Model moderat (acces condiționat)
Cine verifică vârsta?	Verificarea are loc la momentul accesului sau al creării contului, printr-o combinație: platforma aplică pragul, iar un furnizor de verificare (idealmente o infrastructură națională de identitate digitală) confirmă atributul de vârstă fără a dezvălui identitatea. Sub prag, se adaugă verificarea consimțământului parental.
Ce date se colectează?	În varianta proporțională, doar un atribut „peste/sub prag”, emis criptografic (dublu anonim), fără ca platforma să rețină documente de identitate. Punctul sensibil rămâne verificarea relației părinte-copil pentru consimțământ, care poate atrage prelucrarea unor date suplimentare.

Unde se stochează?	Idealmente, dovada vârstei nu se stochează de platformă, ci este validată tranzitoriu prin furnizorul de identitate. Riscul de stocare reapare dacă verificarea recurge la documente sau imagini faciale.
Cât de ușor se poate ocoli mecanismul?	Mai dificil decât simpla autodeclarare, dar nu impenetrabil: conturi parentale, dispozitive partajate, rețele VPN. Eficacitatea depinde de robustețea verificării și de modul concret de aplicare a consimțământului parental.
Ce riscuri de securitate și protecție a datelor apar?	Expunerea datelor este limitată dacă verificarea respectă dublul anonim; crește dacă presupune documente sau biometrie. Infrastructura de identitate și mecanismul de verificare a relației parentale devin ținte de securitate și surse potențiale de date despre minori.
Ce capacitate instituțională cere?	Necesită o infrastructură națională de identitate digitală funcțională și o autoritate care să acrediteze și să supravegheze furnizorii de verificare. Sarcină semnificativă, construită însă pe o infrastructură de identitate existentă sau în dezvoltare.
Cât de compatibil este cu DSA, GDPR și AI Act?	Compatibil în principiu dacă respectă minimizarea datelor (GDPR art. 8 și 5), limita din articolul 28(3) DSA (fără date suplimentare pentru a stabili calitatea de minor) și principiile EDPB privind verificarea vârstei; tensiunea apare dacă verificarea devine generalizată sau biometrică. Opozabilitatea față de platformele stabilite în alte state rămâne condiționată de calea individuală a derogării (cauza CJUE C-188/24).
Ce efect are asupra participării minorilor la viața digitală?	Condiționează accesul, fără a-l exclude: minorii peste prag accesează autonom, cei sub prag cu acordul părinților. Există un risc de excludere pentru copiii fără sprijin parental sau fără acces la o identitate digitală.

În concluzie, Scenariul 2 (moderat) este mai echilibrat decât interdicția generală. El are avantajul de a se sprijini pe pragul deja existent din Legea nr. 195/2024 privind protecția datelor cu caracter personal și pe o orientare europeană recunoscută (prag, consimțământ parental, verificare proporțională), oferind o soluție intermediară între inacțiune și interdicție.

Evaluarea pe criteriile de mai sus relevă însă două tensiuni: distincția dintre pragul de consimțământ și pragul de acces cere o construcție normativă nouă, iar verificarea proporțională a vârstei și a consimțământului parental, dacă nu este ancorată în dublul anonim, poate aluneca spre o colectare excesivă de date, incompatibilă cu GDPR și principiile EDPB. Adicional, opozabilitatea față de platformele stabilite în alte state rămâne condiționată de calea individuală a derogării, conform practicii CJUE.

Pentru Republica Moldova, acest scenariu poate fi o opțiune de compromis, mai ales ca etapă tranzitorie. El este mai compatibil cu drepturile copilului decât scenariul restrictiv, dar cere o arhitectură instituțională și tehnică solidă. Fără aceste garanții, riscă să devină fie declarativ, fie intruziv.

Scenariul 3 – Model progresiv: responsabilizarea platformelor, fără interdicții pentru minori



Scenariul progresiv mută accentul de pe controlul accesului minorului pe controlul riscurilor create de platforme. El nu interzice accesul minorilor la rețelele sociale și nu condiționează accesul general de acord parental. Logica sa este diferită: dacă principalele riscuri provin din designul platformelor, din profilare, din sistemele de recomandare sau monetizare a atenției, atunci obligațiile trebuie impuse platformelor.

Acest scenariu se inspiră direct din logica DSA. Elementele sale centrale sunt: interzicerea publicității bazate pe profilare pentru minori, setări implicite de confidențialitate ridicată, condiții de utilizare redactate pe înțelesul copiilor, mecanisme simple de raportare, proiectarea sigură a serviciului (*safety-by-design*), transparența sistemelor de recomandare, opțiune de recomandare fără profilare, evaluarea periodică a riscurilor sistemice pentru minori precum și instituirea unui Coordonator al serviciilor digitale care supraveghează respectarea acestor obligații ([nota de subsol 1](#)). Spre deosebire de scenariile 1 și 2, verificarea vârstei nu este poarta principală de acces, ci un instrument auxiliar, folosit doar acolo unde este strict necesar pentru protecția minorilor. Modelul progresiv este preluat de către Germania și Irlanda.

Scenariul răspunde direct lacunelor identificate în diagnosticul intern. Republica Moldova are norme generale privind drepturile copilului, protecția datelor, audiovizualul, comerțul electronic, protecția consumatorilor și răspunderea penală, dar nu are încă un regim modern aplicabil platformelor sociale. Legea nr. 284/2004 privind serviciile societății informaționale rămâne construită pe logica veche a comerțului electronic și a răspunderii limitate a intermediarilor, nefiind aliniată la DSA. Ea nu reglementează profilarea minorilor, sistemele de recomandare, designul adictiv, evaluarea riscurilor sistemice sau obligațiile speciale ale platformelor accesibile copiilor ([nota de subsol 17](#)).

În acest sens, pentru preluarea scenariului progresiv, Republica Moldova nu pornește de la zero. Proiectul de lege privind serviciile digitale (număr unic 309/MDED/2025) urmărește deja transpunerea parțială a DSA și instituirea unui Coordonator al serviciilor digitale ([nota de subsol 25](#)). Pentru prezentul scenariu, direcția corectă nu este adoptarea unei legi separate de interdicție, ci completarea și operaționalizarea transpunerii DSA pe dimensiunea minorilor. Aceasta ar permite Republicii Moldova să avanseze pe o cale compatibilă cu procesul de aderare la UE, fără a crea obligații naționale izolate, greu de aplicat platformelor globale. Modelul european confirmă această abordare. DSA nu tratează protecția minorilor ca simplă obligație de avertizare, ci ca obligație de proiectare și prevenire. Articolul 28 cere platformelor accesibile minorilor să asigure un nivel ridicat de confidențialitate, siguranță și securitate. Articolul 25 interzice interfețele manipulatorii. Articolul 27 impune transparența sistemelor de recomandare, iar articolul 38 obligă platformele foarte mari să ofere cel puțin o opțiune de recomandare care nu se bazează pe profilare. Articolele 34 și 35 cer evaluarea și atenuarea riscurilor sistemice, inclusiv a efectelor negative asupra drepturilor copilului, sănătății, dezvoltării și bunăstării minorilor.

AI Act completează această logică. Articolul 5 interzice sistemele de inteligență artificială care exploatează vulnerabilitățile legate de vârstă sau folosesc tehnici manipulative capabile să producă prejudicii semnificative ([nota de subsol 5](#)). Aplicat platformelor sociale, acest standard este relevant pentru sistemele de recomandare, designul adictiv și mecanismele algoritmice care împing minorii spre conținut nociv sau spre utilizare excesivă. Astfel, scenariul progresiv nu se limitează la „mai multă informare”, ci cere schimbarea modului în care platformele digitale și serviciile sale sunt proiectate și oferite.

Practica recentă a Comisiei Europene arată că acest model nu este doar teoretic. Procedurile împotriva TikTok privind designul care creează dependență și împotriva Meta privind protecția minorilor confirmă că DSA este deja folosit pentru a verifica dacă platformele identifică, evaluează și reduc riscurile pentru copii ([notele de subsol 8, 9 și 10](#)). Pentru Republica Moldova, lecția este importantă: o reglementare modernă trebuie să permită supravegherea efectivă a platformelor, nu doar declararea unor principii generale.

Analiza comparativă a altor modele europene susține aceeași direcție. Germania este relevantă prin modelul său non-prohibiționist, construit pe protecția minorilor în media și online, clasificare, co-reglementare și supraveghere. Cadrul german nu pornește de la o interdicție generală de acces la rețele sociale, ci de la protecția copilului față de conținuturi și funcționalități care îi pot afecta dezvoltarea: comunicare și contact, cumpărături, mecanisme asemănătoare jocurilor de noroc, stimularea utilizării excesive, transmiterea datelor către terți și apeluri comerciale neadecvate vârstei. Acest model este util deoarece arată cum pot fi combinate standardele publice cu responsabilizarea furnizorilor.

Irlanda oferă un al doilea reper. Regimul irlandez impune obligații privind protecția copiilor față de conținut nociv, asigurarea vârstei acolo unde este necesar, control parental, mecanisme de raportare și educație media. Chiar dacă Guvernul irlandez a anunțat intenția de a examina restricții privind accesul copiilor sub 16 ani la social media, preferabil printr-o soluție coordonată la nivelul UE, această intenție rămâne o direcție politică, nu un regim juridic definitiv adoptat. Prin urmare, modelul irlandez rămâne relevant.

Principalul avantaj al scenariului 3 este că nu limitează participarea minorilor la viața digitală. El păstrează accesul la informare, exprimare, educație, socializare și participare civică, dar reduce riscurile structurale ale platformelor. Această abordare este mai apropiată de ideea că minorul este vulnerabil, dar și activ digital. Copilul nu este eliminat din spațiul online. Mediul online este obligat să devină mai sigur.

Limita scenariului este aplicarea. O lege de tip DSA este inutilă dacă autoritatea competentă nu are resurse, competențe tehnice și capacitate de cooperare transfrontalieră. Scenariul cere un Coordonator capabil, proceduri clare de control, capacitate de audit algoritmic, acces la date relevante, cooperare cu autorități europene și sancțiuni efective. Fără aceste elemente, obligațiile platformelor pot rămâne formale.

Matricea de evaluare tehnică și juridică

Criteriu de evaluare	Scenariul 3 – Model progresiv (responsabilizarea platformelor)
Cine verifică vârsta?	Verificarea vârstei nu este poarta de acces, ci un instrument auxiliar. Obligațiile de proiectare se aplică indiferent de verificare; pentru obligațiile specifice minorilor (de ex. interzicerea publicității prin profilare), platforma aplică o evaluare proporțională a vârstei fără a colecta date suplimentare.
Ce date se colectează?	Scenariul reduce stimulentele colectării masive, întrucât nu condiționează accesul de verificarea identității tuturor utilizatorilor. Datele relevante privesc evaluarea agregată a riscurilor și transparența, nu identificarea individuală.
Unde se stochează?	Mai puține date de identitate stocate; obligațiile vizează proiectarea serviciului, nu colectarea. Datele de transparență și audit se păstrează de platforme și de autoritatea de supraveghere.
Cât de ușor se poate ocoli mecanismul?	Nu există o barieră de acces care să fie eludată de minori; obligațiile se aplică platformei. Riscul principal este conformarea formală sau superficială a platformelor, nu eludarea de către utilizatori.

Ce riscuri de securitate și protecție a datelor apar?	Scenariul nu impune verificarea identității tuturor utilizatorilor, ceea ce limitează expunerea datelor personale. Riscul se deplasează spre eficacitatea supravegherii și a auditului algoritmic.
Ce capacitate instituțională cere?	Necesită un Coordonator al serviciilor digitale funcțional, cu competențe de audit algoritmic și de cooperare transfrontalieră. Sarcina cea mai exigentă instituțional, prefigurată însă de proiectul de transpunere a DSA.
Cât de compatibil este cu DSA, GDPR și AI Act?	Aliniere prin construcție: scenariul transpune logica DSA (art. 25, 27/38, 28, 33-35), interdicția din AI Act art. 5 și standardele GDPR. Respectă armonizarea maximă, întrucât nu adaugă obligații necoordonate; proiectul de orientări EDPB 3/2025 ghidează aplicarea coerentă DSA-GDPR.
Ce efect are asupra participării minorilor la viața digitală?	Nu exclude minorii, ci modelează mediul în care aceștia participă. Riscul este ca, în lipsa unei aplicări efective, protecția să rămână formală, fără efect practic.

În concluzie, Scenariul 3 (progresiv) prezintă o compatibilitate ridicată cu acquis-ul comunitar, prin însăși construcția sa, fiind deja parțial inițiat prin proiectul de transpunere a DSA. Acesta oferă cea mai coerentă cale de aliniere la standardele europene. El nu promite o soluție rapidă, dar atacă sursa principală a riscurilor: modul în care platformele sunt proiectate, monetizează atenția, recomandă conținut și gestionează interacțiunile cu minorii. Spre deosebire de interdicția generală sau de accesul condiționat de consimțământul părinților, acest model nu mută povara asupra copilului sau părinților.

Pentru Republica Moldova, scenariul progresiv ar presupune finalizarea transunerii DSA, completarea proiectului de lege privind serviciile digitale cu obligații clare pentru protecția minorilor, integrarea standardelor AI Act privind interzicerea manipulării și exploatarei vulnerabilităților, consolidarea Coordonatorului serviciilor digitale și dezvoltarea capacității de supraveghere tehnică. Riscul principal nu este incompatibilitatea juridică, ci insuficiența aplicării. Din acest motiv, scenariul poate funcționa doar dacă este însoțit de resurse instituționale reale, competențe tehnice și mecanisme de cooperare externă.

În loc de concluzii: identificarea celui mai potrivit scenariu

Evaluate separat pe aceleași criterii, cele trei scenarii de reglementare a accesului minorilor la rețele sociale pot fi acum evaluate comparativ, pentru a stabili care dintre ele este, în același timp, cel mai opozabil, fezabil și adecvat realităților Republicii Moldova. Comparația nu pornește de la o preferință prestabilită, ci de la rezultatele evaluării pe criterii și de la experiența comparatorilor analizați anterior.

Scenariul restrictiv întâmpină, pentru Republica Moldova, două obstacole de fond.

Primul ține de opozabilitatea juridică. Parcursul european spre care țara se aliniază tratează cu rezervă interdicțiile generale aplicate platformelor stabilite în afara jurisdicției naționale. Experiența franceză este ilustrativă: Legea din 2023, care institua "majoratul digital" la 15 ani și solicita acordul parental pentru crearea unui cont, nu a devenit niciodată operațională din cauza divergențelor cu raționamentul DSA și din cauza conflictului cu principiul țării de origine (regula potrivit căreia un serviciu digital este reglementat de

statul în care este stabilit furnizorul, iar nu de statul în care se află utilizatorii). Această linie a fost confirmată de CJUE, care, în cauzele conexe C-188/24 și C-190/24, prin hotărârea sa din 16 iunie 2026 a statuat că un stat membru nu poate impune furnizorilor stabiliți în alt stat membru o obligație generală și abstractă. Curtea a stabilit însă o derogare specifică, condiționată de o măsură individualizată, proporțională, precedată de solicitarea statului de stabilire și de notificarea Comisiei Europene. Deși această derogare privea conținutul pornografic, domeniu în care verificarea vârstei este deja recunoscută ca măsură adecvată, ea fixează coridorul procedural și de proporționalitate prin care trebuie să treacă orice restricție impusă unor platforme externe. Prin deducție, poziția Republicii Moldova este chiar mai dificilă decât a unui stat membru: nefiind parte a mecanismelor de cooperare și executare ale Uniunii și având o influență jurisdicțională limitată, o interdicție unilaterală ar fi greu de transpus în practică.

Al doilea obstacol ține de eficacitate. Acolo unde a fost adoptată, o interdicție de acces se dovedește ușor de eludat. Australia, care a introdus interdicția pentru minorii sub 16 ani, din decembrie 2025, oferă primele date: un sondaj realizat în martie 2026 pe 1.050 de minori de 12-15 ani, indică faptul că peste 60% dintre cei care dețineau conturi înainte de interdicție păstrau acces la cel puțin o platformă, iar aproximativ două treimi afirmă că platformele nu luaseră nicio măsură elocventă. Eludarea interdicției de acces s-a realizat prin VPN, documente de identitate împrumutate și alte mijloace. Rezultă că o interdicție lipsită de un mecanism proporțional și solid de verificare a vârstei produce mai degrabă o conformare aparentă și un risc de migrare către spații mai puțin reglementate decât o protecție reală. Pentru Republica Moldova, scenariul restrictiv nu este, așadar, nici opozabil, nici eficace.

Scenariile moderat și progresiv, în schimb, operează în interiorul logicii europene și se dovedesc complementare, nu concurente. Scenariul progresiv construiește coloana structurală: un regim modern al serviciilor digitale, de tip DSA, dublat de o autoritate de coordonare cu capacitate reală. Structura dată răspunde celei mai importante lacune identificate în diagnosticul național: absența unui act de transpunere a DSA. Scenariul moderat adaugă, pe acest fundament, garanții calibrate de acces: verificarea proporțională a vârstei, instrumente de control parental și obligații de proiectare în interesul minorului. Cele două abordări acoperă planuri diferite ale aceleiași probleme și pot fi implementate de comun.

Concluzia analizei comparative a scenariilor de reglementare este că opțiunea opozabilă și adecvată pentru Republica Moldova constă într-o simbioză între modelul progresiv și cel moderat.

În concret, prioritatea ar trebui să fie alinierea cadrului normativ și instituțional național la standardele Uniunii Europene: Regulamentul privind serviciile digitale (DSA), Regulamentul general privind protecția datelor (GDPR) și Regulamentul privind inteligența artificială (AI Act); însoțită de o consolidare semnificativă a instituțiilor publice cu atribuții în domeniu. Pe acest nucleu se pot adăuga măsuri moderate, proporționale, de protecție a accesului, în locul unei interdicții generale.

Opțiunea limitării accesului sub un anumit prag de vârstă (de exemplu, 16 ani) poate fi analizată, însă numai cu titlu de ipoteză supusă unor condiții stricte, iar nu ca soluție implicită. O asemenea limitare ar fi admisibilă doar în strictă conformitate cu practica europeană și cu coridorul trasat de jurisprudența recentă a CJUE: respectarea principiilor legalității, necesității și proporționalității, recurgerea la măsuri individualizate (iar nu la o obligație generală și abstractă), cooperarea cu statul de stabilire al platformei și notificarea Comisiei. Experiența franceză arată, în plus, că o astfel de măsură rămâne pur simbolică în absența normelor de aplicare și a fezabilității tehnice. Pragul intern de vârstă reținut deja de legislația moldovenească pentru consimțământul privind prelucrarea datelor: 14 ani, potrivit Legii nr. 195/2024 privind protecția datelor cu caracter personal; oferă, de altfel, un punct de referință.

În fine, această orientare nu este doar una de oportunitate, ci una structurală. În calitate de stat candidat la aderarea la Uniunea Europeană, cu negocierile de aderare formal deschise, Republica Moldova și-a asumat alinierea progresivă la *acquis-ul comunitar*. În materie digitală, aceasta înseamnă că marja reală de manevră a statului nu constă în construirea unor model divergente proprii, ci în adoptarea standardelor și a procedurilor definite de instituțiile europene. Republica Moldova are, prin urmare, un interes deopotrivă juridic și practic de a se alinia la aceste practici, mai degrabă decât de a le anticipa prin soluții care s-au dovedit, în alte jurisdicții, fie neopozabile, fie ineficace.

Recomandări

Analiza cadrului național a arătat că Republica Moldova dispune de cărămizi, dar nu de o construcție. Drepturile copilului sunt protejate la nivel general, datele personale beneficiază de un regim aflat în modernizare, audiovizualul are reguli solide, iar cadrul penal a fost recent consolidat. Totuși, niciuna dintre aceste piese nu acoperă, singură, modul în care platformele digitale funcționează și îi afectează pe minori. Cele șapte lacune sistemice identificate nu indică absența generală a reglementării, ci caracterul fragmentat al acesteia, parțial depășit și neadaptat erei rețelelor sociale imense și a inteligenței artificiale.

Concluzia analizei comparative a celor trei scenarii a fost că soluția potrivită pentru Republica Moldova nu este nici inacțiunea, nici interdicția generală, ci o **simbioză între modelul progresiv și cel moderat**. S-a considerat necesară edificarea unei coloane structurale de tip DSA, care responsabilizează platformele, completată cu garanții proporționale de acces, calibrate în interesul minorului.

Recomandările formulate mai jos derivă din lacunele sistemice identificate în diagnosticul cadrului normativ și instituțional al Republicii Moldova. Ele pornesc de la concluzia că protecția minorilor în spațiul digital nu poate fi realizată eficient printr-o interdicție generală de acces la rețelele sociale, ci printr-un pachet coerent de măsuri legislative și instituționale. Direcția principală trebuie să fie responsabilizarea platformelor, alinierea la DSA, GDPR și AI Act, consolidarea autorităților competente și introducerea unor mecanisme proporționale de verificare a vârstei, control parental, raportare și limitare a funcționalităților cu risc ridicat pentru minori. Recomandările nu urmăresc excluderea copiilor din spațiul digital. Ele urmăresc transformarea acestui spațiu într-un mediu mai sigur, mai transparent și mai adecvat vârstei. Copilul trebuie protejat împotriva riscurilor reale, dar fără a-i fi afectate disproporționat dreptul la informare, exprimare, educație, socializare și participare civică. Acest echilibru impune o intervenție graduală: pe termen scurt – adoptarea cadrului legislativ minim și instituirea mecanismelor de bază; pe termen mediu – consolidarea capacității instituționale, modernizarea legislației conexe și integrarea riscurilor generate de inteligența artificială.

1. Recomandările legislative pe termen scurt (0–12 luni)

1.1. Accelerarea procesului de adoptarea legii privind serviciile digitale.

Prima prioritate legislativă este accelerarea procesului de adoptare a proiectului legii privind serviciile digitale – numărul unic 309/MDED/2025 ([nota de subsol 25](#)). Proiectul transpune parțial DSA și desemnează Coordonatorul național al serviciilor digitale. Prin obiectul său, proiectul răspunde direct celei mai importante lacune identificate în prezentul studiu: absența unui regim modern de responsabilizare a platformelor online. Adoptarea acestui proiect este importantă nu doar pentru armonizarea formală cu *acquis-ul* UE, ci și pentru instituirea unor obligații concrete privind transparența, mecanismele de raportare, sistemele de recomandare, publicitatea online și protecția minorilor. În lipsa acestei legi, cadrul național va continua să trateze riscurile digitale prin norme dispersate, construite pentru domenii conexe, dar insuficiente pentru realitatea platformelor utilizate de minori. Având în vedere că proiectul a fost consultat public în aprilie–mai

2025, dar nu a fost încă, la data prezentei analize, aprobat de Guvern și transmis spre adoptare Parlamentului, este necesară includerea acestuia printre prioritățile legislative imediate ale Guvernului și Parlamentului. Întârzierea adoptării prelungește vidul de responsabilitate în raport cu platformele digitale și limitează capacitatea autorităților de a interveni eficient în protecția minorilor online.

Totuși, armonizarea formală cu DSA nu trebuie confundată cu aplicarea efectivă față de marile platforme globale. În lipsa unui sediu, reprezentant legal sau mecanism operațional de contact și executare în Republica Moldova, obligațiile impuse unor furnizori precum Google, Meta sau TikTok riscă să rămână dificil de aplicat direct. Din acest motiv, viitoarea lege privind serviciile digitale trebuie să distingă între obligațiile aplicabile efectiv furnizorilor stabiliți sau reprezentați în Republica Moldova și obligațiile care pot fi urmărite realist doar prin cooperare externă, aliniere la mecanismele europene și dialog instituțional cu platformele. Implementarea practică și sancționarea companiilor globale depind totuși de alinierea cu autoritățile de reglementare din UE (în special statele de stabilire, precum Irlanda) și de exercitarea presiunii colective a blocului comunitar, Republica Moldova neavând forța de piață necesară pentru a dicta unilateral condiții gigantilor Big Tech. Integrarea în mecanismele de aplicare ale Uniunii Europene este importantă, deoarece doar Comisia Europeană sau țara de stabilire (Irlanda) dețin pârghiile financiare necesare pentru a sancționa corporațiile cu amenzi de până la 6% din cifra de afaceri globală în caz de nerespectare a regulilor DSA (cum este cazul investigațiilor actuale împotriva TikTok sau Meta)

1.2. Accelerarea elaborării și promovării proiectului de lege privind inteligența artificială

A doua prioritate legislativă este accelerarea elaborării proiectului de lege privind inteligența artificială. În prezent, această inițiativă se află doar la etapa anunțului de inițiere, fără un proiect de lege sau un concept publicat ([nota de subsol 26](#)). Această etapă incipientă oferă oportunitatea ca protecția minorilor să fie integrată din start în arhitectura viitoarei reglementări, nu adăugată ulterior, prin completări fragmentare. Viitoarea lege trebuie să transpună nu doar logica generală a AI Act, ci și garanțiile cu relevanță directă pentru copii. În special, actul național trebuie să reflecte expres articolul 5 din AI Act, care interzice sistemele de inteligență artificială ce exploatează vulnerabilitățile legate de vârstă pentru a distorsiona comportamentul unei persoane într-un mod care poate cauza prejudicii. Această interdicție este esențială pentru mediul digital, unde minorii pot fi expuși la sisteme de recomandare intruzive, publicitate personalizată, jocuri neadecvate, conținut generat artificial dăunător sau mecanisme de captare a atenției.

Se recomandă ca proiectul legii privind inteligența artificială să includă expres protecția minorilor printre obiectivele și principiile sale de bază. Legea trebuie să prevadă garanții pentru situațiile în care sistemele AI sunt utilizate în servicii accesibile copiilor, în educație, pe platforme digitale, în publicitate, moderare de conținut sau interacțiuni automatizate. Fără o astfel de abordare, există riscul ca viitorul cadru național să fie construit în jurul inovării și guvernantei datelor, dar neglijent față de vulnerabilitățile specifice minorilor.

1.3. Integrarea protecției minorilor în Programul Național privind Inteligența Artificială și Guvernanța Datelor 2026–2030

O altă prioritate legislativă este finalizarea și aprobarea Programului Național privind Inteligența Artificială și Guvernanța Datelor pentru anii 2026–2030 ([nota de subsol 27](#)), cu includerea expresă a protecției minorilor în spațiul digital. Conceptul Programului stabilește direcții importante: dezvoltarea unui cadru național de reglementare a AI, consolidarea capitalului uman, infrastructura de date, stimularea inovării și utilizarea AI în administrația publică. Totuși, protecția copiilor nu apare ca direcție distinctă, deși minorii sunt una dintre categoriile cele mai expuse la riscurile generate de sistemele AI.

Se recomandă ca Programul să prevadă o componentă dedicată siguranței minorilor în raport cu AI. Aceasta ar trebui să includă măsuri privind alfabetizarea AI pentru copii, părinți și profesori, evaluarea riscurilor sistemelor AI utilizate în educație, prevenirea deepfake-urilor (în special cele sexualizate), limitarea manipulării comportamentale, protecția datelor copiilor și cooperarea dintre autoritățile competente. De asemenea, Programul trebuie să stabilească responsabilități clare pentru Ministerul Dezvoltării Economice și Digitalizării, Ministerul Educației și Cercetării, CNPDCP, Agenția pentru Securitate Cibernetică, autoritățile de protecție a copilului, organizațiile de tineret.

Integrarea acestei dimensiuni este necesară pentru ca Programul să nu rămână un document axat doar pe competitivitate, inovare și infrastructură. AI poate sprijini educația, serviciile publice și incluziunea, dar poate amplifica și riscurile existente: profilare, manipulare, conținut sintetic, exploatarea vulnerabilităților de vârstă și expunerea copiilor la sisteme pe care nu le pot înțelege sau controla. Programul trebuie să trateze aceste riscuri ca parte a guvernantei responsabile a AI, nu ca temă secundară.

1.4. Integrarea orientărilor Comisiei Europene privind protecția minorilor în aplicarea legii naționale privind serviciile digitale

Adoptarea legii privind serviciile digitale nu trebuie să fie urmată de o etapă lungă de incertitudine privind aplicarea obligațiilor față de minori. Proiectul de lege preia standardele DSA, inclusiv obligația platformelor accesibile minorilor de a asigura un nivel ridicat de confidențialitate, siguranță și securitate, prevăzute în articolul 28. Totuși, această obligație are nevoie de clarificări practice pentru a produce efecte reale.

Se recomandă ca, încă din etapa de promovare a proiectului, autoritățile să țină cont de Orientările Comisiei Europene din 14 iulie 2025 privind aplicarea articolului 28 alin. (1) al DSA ([nota de subsol 3](#)). Aceste orientări oferă repere concrete privind setările implicite de siguranță, protecția datelor, verificarea proporțională a vârstei, controlul parental, raportarea ușor de utilizat de către copii, limitarea designului adictiv, sistemele de recomandare și protecția împotriva practicilor manipulative. Elementele esențiale ale orientărilor ar trebui reflectate fie direct în proiectul de lege, fie în actele subsecvente și ghidurile Coordonatorului serviciilor digitale, adoptate imediat după intrarea în vigoare a legii. Riscul inacțiunii este adoptarea unui cadru corect formal, dar insuficient de clar pentru platforme, autorități, copii și părinți.

1.5. Integrarea orientărilor Comisiei Europene privind practicile AI interzise în viitorul cadru național privind inteligența artificială

Viitorul cadru național privind inteligența artificială trebuie să includă de la început protecția minorilor, nu să o trateze ulterior ca element secundar. Această abordare este necesară deoarece AI poate amplifica riscurile deja identificate în studiu: profilare, manipulare comportamentală, conținut sintetic, deepfake-uri, recomandări nocive și captarea abuzivă a atenției copiilor.

Se recomandă ca Ministerul Dezvoltării Economice și Digitalizării să țină cont de Orientările Comisiei Europene din 4 februarie 2025 privind practicile AI interzise ([nota de subsol 6](#)), în special de interpretarea articolului 5 din AI Act. Acest articol interzice sistemele AI care exploatează vulnerabilitățile legate de vârstă, atunci când acestea pot distorsiona comportamentul unei persoane și pot cauza prejudicii. Viitoarea lege privind AI și Programul Național privind Inteligența Artificială și Guvernanța Datelor 2026–2030 ar trebui să prevadă expres măsuri pentru identificarea și prevenirea sistemelor AI care exploatează minorii. Riscul inacțiunii este adoptarea unui cadru AI orientat spre inovare și guvernanța datelor, dar insuficient pregătit pentru riscurile specifice copiilor în mediul digital.

1.6. Completarea Legii nr. 370/2023 privind drepturile copilului cu dimensiunea digitală

Legea nr. 370/2023 oferă temelia națională a protecției copilului, dar nu dezvoltă suficient aplicarea drepturilor copilului în mediul digital. În prezent, protecția copilului online poate fi dedusă din principiile generale ale legii, însă nu este formulată ca obligație clară pentru stat și pentru actorii relevanți.

Se recomandă completarea legii cu referiri explicite la drepturile copilului în mediul digital, în acord cu Comentariul general nr. 25 (2021) al Comitetului ONU pentru Drepturile Copilului ([nota de subsol 37](#)). Modificările ar trebui să vizeze: protecția copilului online, participarea digitală, informarea adecvată vârstei, siguranța prin design, consultarea copiilor în politicile ce-i vizează. Această completare ar ancora politicile privind siguranța digitală în drepturile copilului, nu doar în logica de control sau restricție. Riscul inacțiunii este menținerea unui cadru general bun, dar insuficient adaptat riscurilor digitale.

1.7. Transpunerea principiilor EDPB privind verificarea proporțională a vârstei

Legea nr. 195/2024 privind protecția datelor cu caracter personal (în vigoare din 23 august 2026), stabilește că un copil poate consimți singur la prelucrarea datelor sale începând cu vârsta de 14 ani. Acesta este însă un prag pentru consimțământ, nu un prag de acces, și nu spune cum ar trebui verificată vârsta fără a colecta date excesive. Nici proiectul privind serviciile digitale nu rezolvă această chestiune. Articolul 28, preluat din DSA, prevede că protecția minorilor nu trebuie să permită colectarea datelor în exces. Rămâne, așadar, de stabilit cum confirmă o platformă vârsta unui copil fără a se transforma într-un instrument de supraveghere. Se recomandă în acest sens adoptarea, imediat după intrarea în vigoare a legii privind protecția datelor, a cadrului subsecvent care să consacre verificarea proporțională a vârstei pe principiul „dublului anonim”: un furnizor de identitate confirmă doar că utilizatorul are vârsta necesară, fără să afle ce platformă vizitează, iar platforma află doar că utilizatorul îndeplinește condiția, fără să-i colecteze datele. Aceasta este soluția recomandată și de Declarației EDPB 1/2025 privind asigurarea vârstei ([nota de subsol 4](#)) și, în spațiul european, este construită pe infrastructura portofelului de identitate digitală.

Cadrul subsecvent ar trebui să includă un **set minim de cerințe tehnice** pentru mecanismele de asigurare a vârstei. Aceste cerințe trebuie să fie clare: platforma nu ar trebui să păstreze copii ale actelor de identitate dacă este suficientă confirmarea că utilizatorul are peste un anumit prag de vârstă; verificarea printr-un terț ar trebui să transmită doar rezultatul necesar, de exemplu „peste 16 ani”, nu numele, adresa sau numărul actului; datele biometrice, cum ar fi selfie-ul sau scanarea facială, nu ar trebui folosite atunci când există o metodă mai puțin intruzivă; iar jurnalele de audit ar trebui să păstreze doar informațiile necesare pentru verificare și control. Soluțiile tehnice trebuie să fie proporționale cu riscul serviciului. De exemplu, accesul la o funcție de comentarii nu justifică același nivel de verificare ca accesul la conținut destinat adulților sau la funcții care permit contact direct cu persoane necunoscute.

Pentru minorii sub 14 ani, unde legea impune obligativitatea obținerii consimțământului reprezentantului legal, cadrul de reglementare trebuie să includă rezolvarea tehnică a consimțământului parental verificabil. Acest mecanism se va realiza prin utilizarea modulului guvernamental EVOSign și a serviciului de identificare la distanță (eKYC). Părinții vor putea autoriza legal accesul minorului prin aplicarea unei semnături electronice avansate direct de pe dispozitivul mobil. Această arhitectură decuplează complet platformele sociale de obligația și riscul major de a procesa acte de stare civilă (ex. certificate de naștere) pentru a demonstra relația de rudenie.

Cerințele tehnice trebuie să impună direct compatibilitatea cu standardul internațional de referință BS ISO/IEC 27566-1:2025 (Sisteme de asigurare a vârstei – Cadru), vizând caracteristicile de reziliență algoritmică și securitate. Suplimentar, dezvoltatorii platformelor trebuie să se alinieze la nivelurile de încredere (assurance levels) din standardul IEEE 2089.1-2024, asigurând o defensivă tehnică riguroasă împotriva

atacurilor de tip spoofing, injectare de date false și prezentare de credențiale alterate (Presentation Attack Detection).

În contextul Republicii Moldova, actele normative subsecvente trebuie să desemneze Portofelul de identitate digitală EVO 2.0 (dezvoltat conform standardelor europene EUDI Wallet) drept infrastructură de bază pentru acest mecanism. Din perspectivă tehnică, asigurarea dublului anonim va fi implementată prin intermediul tehnologiei dovezilor cu cunoaștere zero (Zero-Knowledge Proofs - ZKP). Astfel, platforma comercială va interoga sistemul EVO și va primi exclusiv o atestare binară a vârstei (ex. „utilizatorul are peste 14 ani”), fiind blocată tehnic posibilitatea de a colecta date personale, data nașterii sau documente de identitate brute ale minorilor.

2. Recomandări instituționale pe termen scurt (0–12 luni)

2.1. Analiza oportunității reexaminării autorității desemnate în calitate de Coordonator al serviciilor digitale⁷⁶

Desemnarea Coordonatorului serviciilor digitale nu este o simplă alegere administrativă, ci o decizie structurală de care depinde eficacitatea întregului regim. Funcția Coordonatorului ține mai mult de supravegherea platformelor și a conținutului, evaluarea riscurilor sistemice, examinarea sistemelor de recomandare și a mecanismelor de moderare, aplicarea obligațiilor de siguranță prin proiectare și, acolo unde este necesar, limitarea accesului la anumite conținuturi sau funcționalități. Acest profil este mai apropiat de cel al unei autorități de reglementare a mass-mediei și a conținutului decât de cel al unei autorități de reglementare a comunicațiilor electronice și a accesului consumatorilor la servicii. Experiența comparativă confirmă această logică. În Irlanda, rolul de Coordonator al serviciilor digitale a fost atribuit autorității de reglementare a mass-mediei – Comisia pentru mass-media (*Coimisiún na Meán*), care supraveghea deja platformele de partajare video și siguranța online, în temeiul transpunerii articolului 28b din Directiva serviciilor media audiovizuale și al Codului privind siguranța online.

În Republica Moldova, competențele cele mai apropiate de mandatul unui Coordonator sunt deținute astăzi de Consiliul Audiovizualului, care, potrivit articolului 61¹ din Codul serviciilor media audiovizuale, supraveghează deja furnizorii de platforme de partajare a materialelor video, inclusiv sub aspectul verificării vârstei, al controlului parental și al mecanismelor de raportare. Astfel, se recomandă ca decidenții să reexamineze oportunitatea desemnării ARCOM în calitate de Coordonator al serviciilor digitale și să evalueze, ca alternativă, atribuirea acestei funcții Consiliului Audiovizualului, autoritate al cărei mandat de supraveghere a conținutului și de protecție a minorilor este mai compatibil cu logica DSA.

O asemenea opțiune ar fi viabilă numai cu îndeplinirea cumulativă a două condiții: consolidarea semnificativă a capacităților tehnice ale Consiliului Audiovizualului și instituirea unui parteneriat solid cu Agenția pentru Securitate Cibernetică, care să asigure expertiza tehnică necesară (verificarea vârstei, auditul soluțiilor tehnice, securitatea datelor). Indiferent de autoritatea reținută în final, criteriile decisive rămân compatibilitatea mandatului, capacitatea tehnică reală și claritatea delimitării competențelor. Riscul

⁷⁶ Această recomandare a fost (re)formulată în urma dezbaterilor din cadrul evenimentului public de lansare a studiului (Chișinău, 29 iunie 2026). În cadrul discuțiilor, reprezentanta ARCOM a exprimat rezerve față de intenția de a desemna autoritatea în calitate de Coordonator al serviciilor digitale, invocând absența competențelor și a capacităților umane și tehnice necesare, lipsa unor atribuții de verificare a conținutului, precum și tensiunea dintre misiunea centrală a instituției de a asigura accesul tuturor consumatorilor la servicii și rolul Coordonatorului, care presupune, dimpotrivă, posibilitatea limitării accesului la anumite servicii.

inacțiunii este consolidarea unui Coordonator lipsit de afinitate funcțională cu supravegherea conținutului digital, cu o aplicare formală a legii și o fragmentare a supravegherii între mai multe autorități.

2.2. Instituirea unui mecanism de cooperare interinstituțională pentru siguranța digitală a minorilor

Riscurile digitale pentru minori nu se pot încadra într-un singur mandat instituțional. Ele pot viza protecția datelor, securitatea cibernetică, conținutul ilegal, violența digitală, publicitatea bazată pe profilare, protecția consumatorilor, siguranța audiovizualului, educația, etc. Fără cooperare, cazurile pot fi tratate fragmentat sau pot rămâne între competențe, adică ignorate.

Se recomandă instituirea unui mecanism permanent de cooperare între viitorul Coordonator al serviciilor digitale și alte autorități publice relevante. Mecanismul ar trebui să stabilească reguli clare pentru sesizări, schimb de informații, reacție rapidă, trimiterea cazurilor și cooperarea cu platformele. Riscul inacțiunii este menținerea unei protecții dispersate, în care minorii, părinții și profesorii nu știu unde să se adreseze, iar autoritățile intervin necoordonat.

2.3. Implicarea Agenției pentru Securitate Cibernetică în evaluarea soluțiilor tehnice cu impact asupra minorilor

Protecția minorilor online nu poate fi separată de securitatea tehnică a soluțiilor propuse. Mecanisme de verificare a vârstei, raportare, control parental sau protecție a conturilor pot crea riscuri suplimentare dacă presupun colectarea excesivă de date, identificare inutilă sau vulnerabilități de securitate.

Se recomandă ca Agenția pentru Securitate Cibernetică să fie implicată sistematic în evaluarea soluțiilor tehnice care privesc minorii, în special în procesul de asigurare a vârstei, protecția conturilor, raportarea abuzurilor, securitatea datelor și riscurile asociate platformelor. Rolul Agenției nu trebuie să înlocuiască atribuțiile Coordonatorului, ci să asigure expertiza tehnică necesară aplicării responsabile a viitorului cadru privind serviciile digitale. Riscul inacțiunii este adoptarea unor soluții juridic atractive, dar tehnic vulnerabile, care pot expune copiii la riscuri noi de securitate și protecție generală a datelor personale.

Implicarea autorității competente ar trebui să includă o listă minimă de verificare tehnică pentru soluțiile propuse platformelor. Aceasta ar trebui să analizeze ce date sunt colectate, unde sunt stocate, cât timp sunt păstrate, cine are acces la ele, dacă sunt criptate, dacă pot fi reutilizate în alte scopuri și ce se întâmplă în cazul unei breșe de securitate. De exemplu, o soluție care cere încărcarea actului de identitate și păstrează copia în sistemul platformei prezintă un risc mai mare decât o soluție care primește de la un furnizor de identitate doar confirmarea că utilizatorul a depășit vârsta necesară.

Lista ar trebui să verifice și reziliența la eludare: folosirea VPN, declararea unei vârste false, utilizarea contului unui adult, scanarea feței unui frate mai mare sau crearea repetată de conturi noi. Această evaluare ar permite diferențierea între soluțiile care reduc efectiv riscul pentru copii și soluțiile care doar mută riscul către securitatea datelor personale.

2.4. Consultarea structurată și continuă a minorilor și organizațiilor de tineret

Politicile privind siguranța digitală a minorilor trebuie elaborate cu participarea reală a celor vizați. Adolescenții cunosc direct modul în care sunt utilizate platformele, cum sunt ocolite restricțiile, ce riscuri apar și ce instrumente de protecție sunt realmente utile.

Se recomandă instituirea unui mecanism de consultare cu adolescenți, elevi, organizații de tineret, părinți, profesori și organizații specializate în protecția copilului, după modelul irlandez ([nota de subsol 65](#)). Consultarea ar trebui aplicată înainte de adoptarea măsurilor privind accesul la platforme, verificarea vârstei,

controlul parental, raportarea conținutului și educația digitală. Riscul inacțiunii este adoptarea unor măsuri paternaliste, greu de aplicat și insuficient conectate la realitatea digitală a copiilor.

3. Recomandări legislative pe termen mediu (12 –24 luni)

3.1. Modernizarea legislație privind protecția copiilor împotriva impactului negativ al informației

Legea nr. 30/2013 cu privire la protecția copiilor împotriva impactului negativ al informației rămâne relevantă, dar reflectă o paradigmă depășită, centrată în principal pe filtrarea conținutului. Riscurile actuale pentru minori nu țin doar de existența conținutului dăunător, ci și de modul în care platformele îl recomandă, îl amplifică și îl monetizează.

Se recomandă revizuirea legii pentru a include riscurile generate de platforme: sisteme de recomandare, profilare, design manipulator, mecanisme de captare a atenției, control parental, raportare accesibilă copiilor și setări implicite de siguranță. Revizuirea trebuie corelată cu viitoarea lege privind serviciile digitale, pentru a evita dublările și contradicțiile. Riscul inacțiunii este menținerea unei legi utile pentru un internet mai vechi, dar insuficientă pentru rețelele sociale și platformele utilizate efectiv de minori.

3.2. Clarificarea raportului dintre audiovizual, platforme video și rețele sociale

Codul serviciilor media audiovizuale oferă garanții importante pentru protecția minorilor, inclusiv în raport cu serviciile media și platformele de partajare video. Totuși, multe riscuri actuale apar pe rețele sociale și platforme cu conținut generat de utilizatori, care nu se suprapun integral cu regimul audiovizual.

Se recomandă clarificarea delimitării dintre serviciile media audiovizuale, platformele de partajare video și platformele online reglementate prin legea privind serviciile digitale. Scopul nu este extinderea mecanică a Codului audiovizualului asupra tuturor rețelelor sociale, ci evitarea zonelor gri și stabilirea clară a competențelor autorităților. Riscul inacțiunii este menținerea unor suprapuneri sau goluri de reglementare, în care anumite riscuri pentru minori rămân insuficient acoperite.

3.3. Consolidarea protecției consumatorului-minor în mediul digital

Minorii sunt expuși tot mai des la practici comerciale digitale: abonamente greu de înțeles sau greu de întrerupt, rețineri de plăți netransparente, conținut sponsorizat camuflat, practici comerciale înșelătoare, publicitate agresivă și interfețe care favorizează decizii impulsive. Cadrul actual de protecție a consumatorilor oferă instrumente utile, dar tratează minorul în mare parte ca pe un consumator generic.

Se recomandă completarea legislației privind protecția consumatorilor cu garanții specifice pentru minorii care utilizează servicii digitale. Acestea ar trebui să vizeze transparența costurilor, interzicerea practicilor comerciale manipulative și agresive, marcarea clară a conținutului publicitar, limitarea presiunii comerciale și protecția față de mecanismele care exploatează vulnerabilitățile legate de vârstă. Riscul inacțiunii este ca minorii să rămână protejați doar prin reguli generale, insuficient adaptate economiei digitale.

3.4. Corelarea cadrului penal cu mecanismele preventive din legislația digitală

Cadrul penal a fost consolidat în raport cu anumite forme de violență digitală, inclusiv hărțuire, urmărirea (*stalking*), manipularea în scopuri sexuale (*grooming*) sau alte forme de abuzuri facilitate online. Totuși, dreptul penal intervine, de regulă, după producerea prejudiciului și nu are scop preventiv.

Se recomandă corelarea legislației penale și procesual-penale cu mecanismele preventive care urmează a fi prevăzute de viitorul cadru privind serviciile digitale: raportare accesibilă, reacție rapidă, cooperare cu platformele, protecția victimei minore și trimiterea eficientă a cazurilor între autorități. Această corelare trebuie realizată fără a transforma platformele în organe de urmărire penală, dar asigurând că ele cooperează

efectiv cu organele de drept și/sau coordonatorul național, în cazurile care afectează minorii. Riscul inacțiunii este menținerea unei protecții predominant reactive, în care minorul primește sprijin instituțional abia după ce prejudiciul s-a produs.

4. Recomandări instituționale pe termen mediu (12 –24 luni)

4.1. Dezvoltarea capacității tehnice a autorităților responsabile

Aplicarea regulilor privind platformele digitale nu poate fi realizată doar prin competențe juridice generale. Autoritățile vor avea nevoie de expertiză privind sisteme de recomandare, publicitate digitală, verificarea vârstei, protecția datelor, moderarea conținutului, securitate cibernetică și inteligență artificială.

Se recomandă dezvoltarea capacității tehnice în special a ARCOM, CNPDCP, Agenției pentru Securitate Cibernetică, Consiliului Audiovizualului, ISSNPC și organelor de drept. Aceasta ar trebui să includă formări specializate, proceduri comune, acces la expertiză tehnică și informațională externă și capacitatea de a analiza informațiile furnizate de platforme. Riscul inacțiunii este o aplicare formală a noilor reguli, în care autoritățile pot constata încălcări, dar nu pot evalua riscurile reale generate de arhitectura platformelor.

4.2. Dezvoltarea mecanismelor de raportare și reacție rapidă pentru cazurile care afectează minorii

Minorii, părinții și profesorii trebuie să aibă canale clare pentru raportarea sigură și promptă a abuzurilor digitale. În prezent, riscurile precum hărțuirea online, urmărirea digitală, ademenirea sexuală prin manipulare online, distribuirea imaginilor intime, amenințările sau deepfake-urile sexualizate, etc. pot implica mai multe autorități, fără un traseu instituțional ușor de urmat.

Se recomandă dezvoltarea unor mecanisme de raportare accesibile copiilor și adulților care îi protejează, conectate cu proceduri clare de reacție rapidă. Aceste mecanisme trebuie să permită trimiterea eficientă a cazurilor între autorități, cooperarea cu platformele și protecția victimei minore. Riscul inacțiunii este menținerea unei protecții reactive și fragmentate, în care copilul primește sprijin abia după ce prejudiciul s-a produs sau după ce cazul a circulat între mai multe instituții.

4.3. Integrarea educației digitale în politicile de protecție a copilului

Educația digitală este necesară și necesită a fi efectuată în paralel cu responsabilizarea platformelor sau instituirea restricțiilor țintite și justificate. Ea trebuie să completeze reglementarea, oferind copiilor, părinților și profesorilor instrumente reale pentru înțelegerea riscurilor online.

Se recomandă integrarea educației digitale în programele școlare, activitățile extracurriculare și politicile de protecție a copilului. Temele prioritare ar trebui să includă: cunoașterea drepturilor digitale, protecția datelor, recunoașterea publicității înșelătoare, urmărirea, hărțuirea sau manipularea sexuală online, raportarea abuzurilor, deepfake-urile, securitatea conturilor, drepturile consumatorului de servicii digitale și utilizarea responsabilă a AI. Riscul inacțiunii este ca protecția minorilor să rămână dependentă de reacția părinților sau profesorilor, fără competențe suficiente pentru a înțelege și gestiona riscurile digitale.

4.4. Integrarea dimensiunii de gen în monitorizarea riscurilor digitale

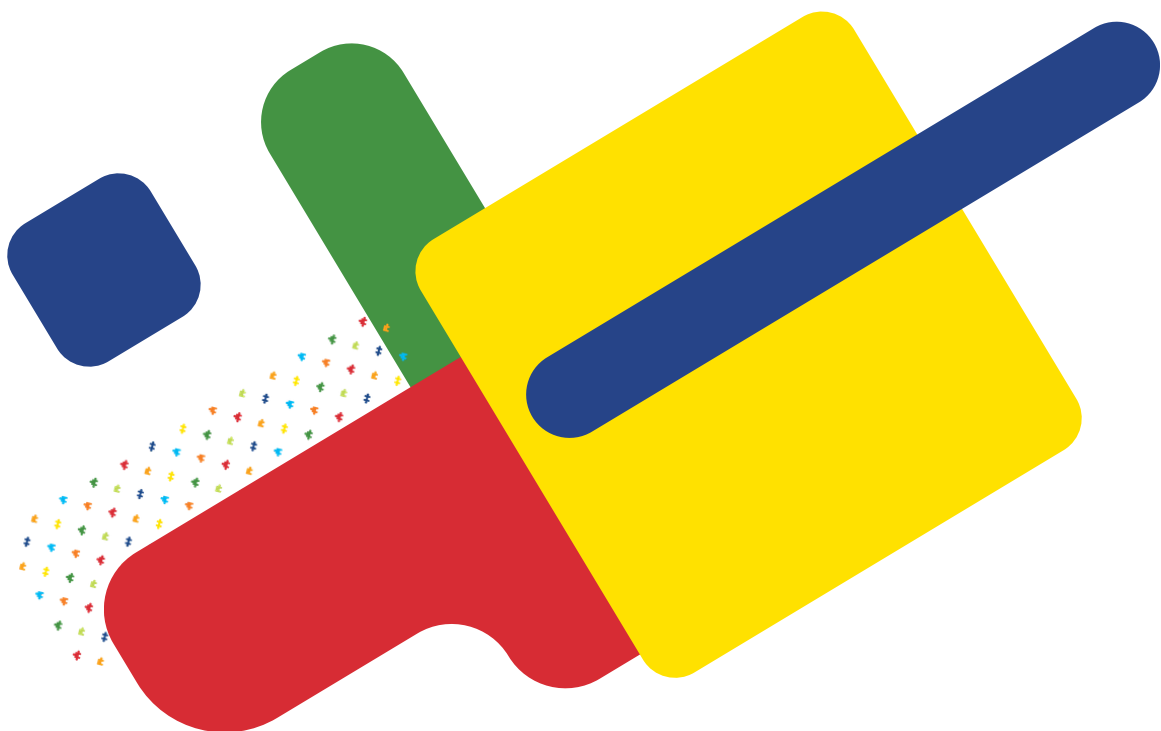
Riscurile digitale nu afectează toți copiii la fel. Fetele și tinerele sunt expuse mai mult hărțuirii online, urmăririi digitale, șantajului sexual, distribuirii neconsensuale a imaginilor intime sau deepfake-urilor.

În contrapartidă, practica penală națională demonstrează că băieții reprezintă o categorie extrem de vulnerabilă în fața tacticilor de racolare pentru activități infracționale. Aceștia sunt sistematic vizați de grupările criminale care utilizează platformele online și rețelele de mesagerie pentru a-i atrage în scheme de

distribuire și trafic de droguri (în calitate de curieri), exploatând promisiunile de câștiguri rapide și lipsa discernământului deplin al consecințelor juridice.

Se recomandă ca autoritățile responsabile să integreze dimensiunea de gen în colectarea datelor, mecanismele de raportare, formarea specialiștilor și evaluarea riscurilor pentru minori. Această abordare trebuie realizată în cooperare cu instituțiile și organizațiile specializate în prevenirea violenței împotriva femeilor și fetelor. Riscul inacțiunii este tratarea riscurilor digitale ca fenomen uniform, cu ignorarea unor forme grave de violență online care afectează în mod special fetele și tinerele.

Această concluzie este susținută și de interviul de feedback inclus în anexă, care arată că riscurile grave pentru copii apar de regulă prin acumularea mai multor factori: contactul cu persoane necunoscute, manipularea treptată a minorului, lipsa unei reacții rapide din partea platformei, dificultatea de a raporta abuzul și lipsa sprijinului pentru copilul victimă. Exemplele relevante nu țin doar de accesul la platformă, ci și de modul în care platforma funcționează după crearea contului: mesaje private de la adulți, distribuirea imaginilor fără acord, presiuni pentru trimiterea de fotografii, recomandarea repetată a unor materiale nocive sau imposibilitatea copilului de a bloca și raporta rapid un utilizator abuziv. Prin urmare, protecția minorilor nu trebuie redusă la verificarea vârstei. Ea trebuie să includă educație digitală, raportare simplă, reacție instituțională rapidă și obligații clare pentru platforme de a reduce riscurile generate de propriile funcționalități.



Anexa 1 – Foaie de parcurs

Recomandări legislative pe termen scurt (0–12 luni)		
Acțiunea necesară	Instituția responsabilă Guvernul și Parlamentul; inițiator – MDED	Termen orientativ
1.1 Accelerarea adoptării proiectului de lege privind serviciile digitale (nr. unic 309/MDED/2025) și includerea lui printre prioritățile legislative imediate		0–12 luni
1.2 Accelerarea elaborării și promovării proiectului de lege privind inteligența artificială, cu integrarea protecției minorilor din start (transpunerea expresă a art. 5 din AI Act)	MDED (elaborare); Guvernul și Parlamentul (promovare)	0–12 luni
1.3 Finalizarea și aprobarea Programului Național privind Inteligența Artificială și Guvernanța Datelor 2026–2030, cu o componentă dedicată siguranței minorilor	MDED (coordonare), cu MEC, CNPDCP, Agenția pentru Securitate Cibernetică, autoritățile de protecție a copilului	0–12 luni
1.4 Reflectarea Orientărilor Comisiei Europene din 14 iulie 2025 (art. 28 DSA) în proiectul de lege și în actele subsecvente/ghidurile Coordonatorului serviciilor digitale	MDED și Coordonatorul serviciilor digitale	0–12 luni; actele subsecvente – imediat după intrarea în vigoare a legii
1.5 Reflectarea Orientărilor Comisiei Europene din 4 februarie 2025 privind practicile AI interzise (art. 5 AI Act) în viitorul cadru privind IA și în Programul Național 2026–2030	MDED	0–12 luni
1.6 Completarea Legii nr. 370/2023 privind drepturile copilului cu dimensiunea digitală, în acord cu Comentariul general nr. 25 (2021)	MMPS / MJ (inițiere); Parlamentul (adoptare)	0–12 luni
1.7 Adoptarea cadrului subsecvent privind verificarea proporțională a vârstei pe principiul „dublului anonim”	CNPDCP și MDED (cadru subsecvent)	După intrarea în vigoare a Legii nr. 195/2024 (23.08.2026); 0–12 luni

Recomandări instituționale pe termen scurt (0–12 luni)

Acțiunea necesară	Instituția responsabilă	Termen orientativ
2.1 Reexaminarea autorității desemnate în calitate de Coordonator al serviciilor digitale	Guvernul, MDED	0–12 luni (primul an de aplicare)
2.2 Instituirea unui mecanism permanent de cooperare interinstituțională pentru siguranța digitală a minorilor	Coordonatorul viitor, ARCOM, CNPDCP, Agenția pentru Securitate Cibernetică, Consiliul Audiovizualului, ISSPNPC, Poliția, Procuratura, MEC, MMPS, Avocatul Poporului pentru drepturile copilului	0–12 luni
2.3 Implicarea sistematică a Agenției pentru Securitate Cibernetică în evaluarea soluțiilor tehnice cu impact asupra minorilor (verificarea vârstei, control parental, protecția conturilor)	Agenția pentru Securitate Cibernetică, în cooperare cu ARCOM și CNPDCP	0–12 luni
2.4 Instituirea unui mecanism de consultare structurată și continuă a minorilor și organizațiilor de tineret (model irlandez)	Coordonatorul viitor / MDED, cu MEC și organizațiile de tineret și de protecție a copilului	0–12 luni

Recomandări legislative pe termen mediu (12–24 luni)

Acțiunea necesară	Instituția responsabilă	Termen orientativ
3.1 Modernizarea Legii nr. 30/2013 privind protecția copiilor împotriva impactului negativ al informației (riscuri de design, profilare, sisteme de recomandare), corelat cu legea privind serviciile digitale	Guvernul (MMPS) / Parlamentul; corelare cu Coordonatorul serviciilor digitale și Consiliul Audiovizualului	12–24 luni
3.2 Clarificarea delimitării dintre serviciile media audiovizuale, platformele de partajare video și platformele online	MDED, Consiliul Audiovizualului și ARCOM	12–24 luni
3.3 Completarea legislației privind protecția consumatorilor cu garanții specifice pentru consumatorul-minor în mediul digital	MDED / ISSPNPC; adoptare – Parlamentul	12–24 luni

3.4 Corelarea cadrului penal și procesual-penal cu mecanismele preventive din legislația digitală	MJ / Parlamentul, cu Procuratura și Poliția	12–24 luni
Recomandări instituționale pe termen mediu (12–24 luni)		
Acțiunea necesară	Instituția responsabilă	Termen orientativ
4.1 Dezvoltarea capacității tehnice a autorităților (formări specializate, proceduri comune, acces la expertiză externă, analiza informațiilor furnizate de platforme)	Coordonatorul viitor, ARCOM, CNPDCP, Agenția pentru Securitate Cibernetică, Consiliul Audiovizualului, ISSPNPC, organele de drept (cu sprijinul Guvernului)	12–24 luni
4.2 Dezvoltarea mecanismelor de raportare și reacție rapidă pentru cazurile care afectează minorii	Coordonatorul viitor, ARCOM, Poliția, Procuratura, CNPDCP, autoritățile de protecție a copilului	12–24 luni
4.3 Integrarea educației digitale în programele școlare, activitățile extracurriculare și politicile de protecție a copilului	MEC, cu MMPS și autoritățile de protecție a copilului	12–24 luni
4.4 Integrarea dimensiunii de gen în colectarea datelor, mecanismele de raportare, formarea specialiștilor și evaluarea riscurilor	Autoritățile responsabile (ARCOM, CNPDCP, organele de drept), în cooperare cu Agenția Națională de Prevenire și Combatere a Violenței Împotriva Femeilor și a Violenței în Familie	12–24 luni

Arina Țurcan-Donțu

Inițiativa privind protecția minorilor în spațiul digital și opțiunile de reglementare pentru Republica Moldova

Durată: 25-30 min	Format: Interviu semi-structurat	Obiectiv: Feedback	Utilizare: Pentru studiu și recomandări
-----------------------------	--	------------------------------	---

Profilul expertizei

Arina Țurcan-Donțu este avocată cu peste 15 ani de experiență în reprezentarea victimelor infracțiunilor, inclusiv în cauze ce vizează violența, abuzul, exploatarea și protecția persoanelor vulnerabile. Perspectiva sa este relevantă pentru prezentul studiu deoarece aduce o înțelegere practică a riscurilor cu care se confruntă minorii în mediul digital, dincolo de analiza juridică și instituțională. Interviuul contribuie la calibrarea recomandărilor prin raportare la experiențe reale privind racolarea online, exploatarea sexuală, hărțuirea digitală, șantajul, vulnerabilitatea copiilor și accesul victimelor la protecție.

Contextul discuției

Consiliul Național al Tineretului din Moldova lucrează la o analiză și la un set de recomandări pentru Republica Moldova privind protecția minorilor în spațiul digital, în special în raport cu rețelele sociale și alte platforme online. În centrul acestui demers se află întrebarea ce tip de intervenție publică ar putea proteja mai bine copiii și adolescenții de riscurile din mediul online, fără a crea măsuri disproporționate, greu de aplicat sau incompatibile cu standardele europene. Documentul evaluează trei scenarii de reglementare:

1. interdicția generală de acces sub un anumit prag de vârstă,
2. accesul condiționat prin verificarea vârstei și implicarea părinților
3. model orientat spre responsabilizarea platformelor.

Discuția cu dvs. este importantă pentru noi deoarece vrem să înțelegem mai bine această problemă din perspectiva protecției victimelor, a drepturilor copilului și a riscurilor care apar în practică. Ne-ar ajuta foarte mult opinia dvs. despre ce forme de protecție ar fi cu adevărat utile, ce lacune există astăzi și ce ar trebui evitat, astfel încât recomandările finale să fie nu doar corecte juridic, ci și relevante și aplicabile în realitate.

Lista de întrebări

Mai jos am creat o lista de întrebări care o să ne ajute să definim mai bine acest raport:

A. Riscuri/vulnerabilități pentru minori în spațiul digital

#	Întrebare	Notițe / idei-cheie
1	Care vi se par cele mai grave riscuri pentru minori în spațiul digital, din perspectiva protecției victimelor? De ce întrebăm: Pentru a ancora inițiativa în riscuri reale, nu în percepții generale. De ex.: Conținut dăunător, grooming, hărțuire, exploatare, presiune socială, design manipulator.	Din perspectiva mea, ca avocat care de peste 15 ani reprezintă victime ale infracțiunilor, unul dintre cele mai grave riscuri pentru minori în spațiul digital este racolarea online în scopul exploatarei și abuzului sexual. Am întâlnit cazuri în care copiii au fost contactați prin rețele sociale sau aplicații de mesagerie, au fost manipulați emoțional, li s-a câștigat încrederea, iar ulterior au devenit victime ale abuzului sexual. De multe ori, acești copii nu conștientizează pericolul până când este prea târziu. Un alt risc major este implicarea minorilor în activități legate de droguri. Tot mai frecvent, grupările infracționale folosesc mediul online pentru a recruta adolescenți în calitate de curieri sau distribuitori de droguri. Copiii sunt atrași prin promisiuni de câștiguri rapide și ajung să fie folosiți pentru activități ilegale fără a înțelege pe deplin consecințele. În activitatea mea profesională am întâlnit atât fete, cât și băieți care au ajuns să fie condamnați pentru infracțiuni legate de traficul de droguri după ce au fost racolați prin intermediul internetului. În spatele acestor dosare se află, de multe ori, copii vulnerabili, manipulați de persoane care profită de lipsa lor de experiență și de nevoia de apartenență sau câștig. De aceea, protecția copiilor în mediul digital nu înseamnă doar securitate cibernetică. Înseamnă prevenirea exploatarei sexuale, a recrutării de către grupări criminale și educarea copiilor pentru a recunoaște pericolele ascunse în spatele unui simplu mesaj primit online.
2	Ce forme de violență sau abuz digital considerați că sunt în prezent subestimate în Republica Moldova? De ce întrebăm: Pentru a identifica zonele în care reglementarea și instituțiile nu văd suficient problema. De ex.: Hărțuire repetată, stalking digital, distribuire de imagini intime, umilire publică, șantaj.	Din perspectiva mea, una dintre cele mai subestimate forme de violență digitală în Republica Moldova este abuzul psihologic exercitat prin intermediul tehnologiilor. Controlul permanent, monitorizarea activității online, mesajele obsesive, amenințările și hărțuirea continuă sunt adesea percepute ca simple conflicte personale, deși pot avea efecte devastatoare asupra sănătății emoționale a victimelor. O altă formă grav subestimată este exploatarea sexuală online a copiilor, inclusiv producerea, distribuirea și deținerea materialelor cu caracter de abuz sexual asupra minorilor. În practică, observăm că mediul online facilitează contactul dintre agresori și copii, iar riscurile sunt mult mai mari decât percepe societatea.

	De asemenea, amenințarea cu divulgarea imaginilor intime – cunoscută și ca „revenge porn” sau șantaj sexual online – reprezintă un fenomen în creștere. Victimele, în special femeile și adolescentele, sunt constrânse, umilite și controlate prin amenințarea că fotografiile sau videoclipurile intime vor fi publicate ori transmise familiei, prietenilor sau colegilor. În activitatea mea de avocat am întâlnit victime care au suferit mai mult din cauza umilinței și fricii generate de aceste amenințări decât din cauza violenței fizice. Din păcate, multe persoane încă nu conștientizează că aceste fapte constituie forme reale de violență și necesită intervenția promptă a autorităților. Este esențial să înțelegem că violența digitală nu este „virtuală” – consecințele ei sunt cât se poate de reale și pot afecta profund siguranța, sănătatea mintală și demnitatea victimelor.
3 Există categorii de minori care ar trebui tratate ca deosebit de vulnerabile în această inițiativă? De ce întrebăm: Pentru calibrarea măsurilor și a protecției diferențiate. De ex.: Fete, copii din medii vulnerabile, minori-victime, copii cu dizabilități, adolescenți fără suport familial.	Consider că toți copiii trebuie să fie incluși în inițiativele de prevenire și educare privind siguranța în mediul digital. Este important ca aceștia să cunoască atât riscurile de a deveni victime ale infracțiunilor online, cât și consecințele implicării în activități ilegale desfășurate prin intermediul internetului. Totuși, există anumite categorii de minori care necesită o atenție sporită. Din experiența mea profesională, copiii cu dizabilități intelectuale sunt printre cei mai vulnerabili, deoarece pot avea dificultăți în identificarea pericolelor, în înțelegerea intențiilor reale ale persoanelor cu care interacționează online și în evaluarea consecințelor propriilor acțiuni. De asemenea, copiii din mediul rural pot fi expuși unor riscuri sporite, în special atunci când accesul la educație digitală, servicii specializate și programe de informare este limitat. În multe cazuri, aceștia sunt mai ușor de manipulat de persoane care urmăresc exploatarea sexuală, recrutarea pentru activități infracționale sau alte forme de abuz. O atenție deosebită ar trebui acordată și copiilor aflați în situații de vulnerabilitate socială, celor lipsiți de supraveghere parentală adecvată sau celor care petrec foarte mult timp online fără ghidare și sprijin din partea adulților. Din această perspectivă, inițiativa ar trebui să combine educația digitală pentru toți copiii cu măsuri și materiale adaptate grupurilor deosebit de vulnerabile, astfel încât prevenirea să ajungă exact la cei care au cea mai mare nevoie de protecție.

B. Fete, discriminare și violență de gen

#	Întrebare	Notițe / idei-cheie
1	În ce măsură fetele și adolescentele sunt expuse unor riscuri diferite față de băieți în mediul online? De ce întrebăm: Pentru integrarea reală a dimensiunii de gen în recomandări. De ex.: Abuz sexualizat, presiune reputațională, control, intimidare, expunere publică.	Da, fetele și băieții se confruntă cu riscuri diferite în mediul online, iar aceste diferențe trebuie luate în considerare atunci când sunt dezvoltate măsuri de prevenire și protecție. Din experiența mea profesională, fetele și adolescentele sunt expuse într-o măsură mai mare riscului de exploatare și abuz sexual online. Acestea sunt mai frecvent vizate de persoane care urmăresc obținerea imaginilor intime, șantajul sexual, hărțuirea online sau divulgarea neconsensuală a fotografiilor și videoclipurilor cu caracter intim. În multe cazuri, agresorii folosesc manipularea emoțională și construiesc relații de încredere înainte de a exploata victima. În cazul băieților, observ mai frecvent riscul de recrutare pentru activități infracționale. Grupările criminale utilizează rețelele sociale, aplicațiile de mesagerie și platformele online pentru a racola minori în scheme ilegale, inclusiv pentru distribuirea drogurilor, transportul bunurilor provenite din infracțiuni sau alte activități ilicite. Adolescenții sunt atrași prin promisiuni de câștiguri rapide și pot ajunge să răspundă penal pentru fapte ale căror consecințe nu le înțeleg pe deplin. Desigur, aceste riscuri nu sunt exclusive. Atât fetele, cât și băieții pot deveni victime ale exploatării sexuale, ale șantajului, ale fraudelor online sau ale recrutării infracționale. Cu toate acestea, datele din practică arată că fetele sunt afectate mai frecvent de formele de violență sexuală online, iar băieții de recrutarea în activități infracționale. Din acest motiv, programele de educație și prevenire trebuie să fie adaptate diferitelor tipuri de riscuri la care sunt expuși copiii, oferindu-le instrumentele necesare pentru a recunoaște pericolele și pentru a solicita ajutor la timp.
2	Ce ar trebui să prevadă o inițiativă serioasă pentru a răspunde mai bine hărțuirii online, abuzului sexualizat, stalking-ului digital sau umilirii publice?	Din perspectiva mea, ca avocat care reprezintă de peste 15 ani victime ale violenței și infracțiunilor, o inițiativă serioasă trebuie să combine prevenirea, protecția victimelor și tragerea la răspundere a agresorilor. În primul rând, este necesară educarea copiilor, părinților și profesorilor cu privire la riscurile din mediul online, la modalitățile de recunoaștere a hărțuirii, stalking-ului digital, șantajului sexual și a altor forme de abuz. Prevenirea este cea mai eficientă formă de protecție.

De ce întrebăm: Pentru a extrage măsuri concrete și nu doar principii. De ex.: Raportare, intervenție rapidă, obligații pentru platforme, suport pentru victimă, educație preventivă.	În al doilea rând, victimele trebuie să aibă acces la mecanisme simple și rapide de raportare și asistență. Multe persoane nu știu unde să se adreseze sau renunță să solicite ajutor deoarece consideră că autoritățile nu vor interveni eficient. Un element esențial îl reprezintă dezvoltarea capacităților profesioniștilor – polițiști, procurori, judecători, avocați, psihologi și asistenți sociali – pentru a identifica, investiga și documenta corect formele de violență digitală și probele electronice. De asemenea, este necesară consolidarea cooperării cu platformele digitale pentru eliminarea rapidă a conținutului abuziv, în special a imaginilor intime distribuite fără consimțământ și a materialelor care implică exploatarea sexuală a copiilor. Nu în ultimul rând, victimele trebuie să beneficieze de sprijin psihologic și juridic specializat. În practică, am întâlnit persoane care au suferit traume severe în urma umilirii publice online, a hărțuirii constante sau a amenințărilor cu divulgarea imaginilor intime. Impactul acestor fapte poate fi la fel de grav ca în cazul unor forme de violență exercitate în lumea reală. O inițiativă eficientă trebuie să transmită un mesaj clar: violența digitală este o formă reală de violență, iar victimele trebuie protejate rapid, eficient și fără a fi revictimizate.
Cum poate fi integrată dimensiunea de gen fără ca textul să rămână doar declarativ? De ce întrebăm: Pentru a transforma perspectiva de gen în cerințe aplicabile. De ex.: Indicatori, obligații, proceduri, rolul instituțiilor, linii de suport.	Dimensiunea de gen nu trebuie să se limiteze la formulări generale privind egalitatea dintre femei și bărbați, ci trebuie reflectată în măsuri concrete, bazate pe riscurile diferite la care sunt expuse fetele și băieții în mediul online. Din experiența mea profesională, fetele și adolescentele sunt afectate într-o măsură mai mare de hărțuirea sexuală online, șantajul sexual, divulgarea imaginilor intime și alte forme de violență bazate pe gen. În schimb, băieții sunt mai frecvent vizați de recrutarea în activități infracționale, inclusiv în scheme de distribuire a drogurilor sau alte forme de criminalitate organizată facilitate prin internet. Pentru ca dimensiunea de gen să fie una reală și nu doar declarativă, inițiativa ar trebui să prevadă colectarea și analiza datelor dezagregate pe sexe, identificarea riscurilor specifice pentru fete și băieți, dezvoltarea unor programe de prevenire adaptate acestor riscuri și instruirea profesioniștilor pentru a recunoaște formele de violență digitală bazate pe gen.

	De asemenea, este important ca mecanismele de raportare și asistență să fie accesibile și sensibile la nevoile victimelor, în special ale fetelor și adolescentelor care sunt expuse fenomenelor de exploatare sexuală online. Integrarea perspectivei de gen înseamnă să recunoaștem că nu toți copiii se confruntă cu aceleași pericole și să construim măsuri de protecție adaptate realităților pe care le trăiesc diferite categorii de copii în mediul digital.
--	---

C. Minori ca victime și acces la protecție

#	Întrebare	Notițe / idei-cheie
1	Dacă un minor devine victimă în mediul online, care sunt cele mai importante lacune de protecție astăzi? De ce întrebăm: Pentru a lega inițiativa de mecanismele de intervenție efectivă. De ex.: Sesizare, consiliere, reacția școlii, poliție, suport juridic, suport psihologic.	Din perspectiva mea, principala problemă nu mai este lipsa reglementărilor legale. Republica Moldova dispune de un cadru normativ relativ bine dezvoltat pentru protecția copiilor, inclusiv în situațiile care implică infracțiuni comise prin intermediul tehnologiilor informaționale. Lacuna cea mai importantă rămâne aplicarea practică a acestor prevederi. De multe ori, intervenția autorităților nu este suficient de rapidă, probele digitale nu sunt colectate și conservate prompt, iar victimele și familiile lor nu cunosc mecanismele disponibile de protecție și asistență. În ultimii ani, am observat îmbunătățiri semnificative în domeniul justiției pentru copii. Există mai multă specializare a profesioniștilor, proceduri mai prietenoase copilului și o mai bună înțelegere a nevoilor victimelor minore. Cu toate acestea, persistă provocări legate de identificarea timpurie a cazurilor, cooperarea interinstituțională și capacitatea de a răspunde eficient fenomenelor care evoluează foarte rapid în mediul digital. O altă problemă este că multe victime nu raportează abuzurile de teamă, rușine sau din cauza sentimentului că nu vor fi ajutate. În special în cazurile de șantaj sexual online, divulgare a imaginilor intime sau exploatare sexuală prin internet, copilul poate rămâne mult timp singur cu problema înainte ca un adult să intervină.

		De aceea, consider că eforturile viitoare trebuie concentrate nu doar pe adoptarea unor noi norme juridice, ci și pe consolidarea capacităților profesioniștilor, îmbunătățirea mecanismelor de intervenție și creșterea gradului de informare a copiilor și părinților. În practică, protecția eficientă a copilului depinde nu doar de existența legii, ci de capacitatea sistemului de a acționa rapid și coordonat atunci când copilul are nevoie de ajutor.
2	Ce mecanisme de sesizare și intervenție ar trebui să existe ca minorul sau familia să poată obține ajutor rapid? De ce întrebăm: Pentru a formula recomandări instituționale concrete. De ex.: Punct unic de contact, ghid procedural, rolul școlii, rolul serviciilor specializate.	În opinia mea, mecanismele de sesizare și intervenție trebuie să fie simple, accesibile și rapide. Atunci când un copil devine victima unei infracțiuni în mediul online, timpul este esențial pentru protejarea victimei și pentru conservarea probelor digitale. În primul rând, copiii și părinții trebuie să știe clar unde pot solicita ajutor. Este important să existe mecanisme ușor accesibile de raportare către poliție, autoritățile de protecție a copilului și serviciile specializate, inclusiv prin platforme online și linii telefonice de asistență. În al doilea rând, sesizările trebuie să genereze o intervenție rapidă și coordonată. Poliția, autoritățile tutelare, psihologii și alți specialiști trebuie să coopereze eficient pentru a evalua riscurile, a proteja copilul și a preveni continuarea abuzului. De asemenea, este esențial ca victimele și familiile acestora să aibă acces rapid la consiliere psihologică și asistență juridică. În multe situații, părinții nu cunosc pașii pe care trebuie să îi urmeze pentru a proteja copilul, pentru a păstra probele digitale sau pentru a solicita eliminarea conținutului abuziv de pe platformele online. Consider că trebuie consolidată și cooperarea cu platformele digitale pentru eliminarea promptă a materialelor care implică exploatarea sexuală a copiilor, divulgarea imaginilor intime sau alte forme de abuz online. Cel mai important este ca minorul și familia să nu fie lăsați singuri în fața problemei. Un sistem eficient trebuie să ofere un punct clar de contact, o reacție rapidă și servicii integrate care să asigure protecția copilului încă din primele momente după sesizare.
3	Cum ar trebui gândită protecția astfel încât copilul să nu fie revictimizat de proceduri sau de instituții?	Protecția copilului trebuie construită pornind de la principiul interesului superior al copilului și de la abordarea centrată pe victimă. Scopul nu este doar investigarea infracțiunii, ci și evitarea oricărei suferințe suplimentare cauzate de proceduri sau de interacțiunea cu instituțiile.

De ce întrebăm: Pentru a evita soluții care agravează efectul asupra copilului. De ex.: Confidențialitate, limbaj, timp de reacție, număr de interacțiuni, protejarea probei digitale.	Din experiența mea profesională, una dintre cele mai frecvente forme de revictimizare apare atunci când copilul este obligat să relateze în repetate rânduri aceleași fapte în fața mai multor specialiști și instituții. De aceea, este important ca audierea să fie realizată de profesioniști specializați, într-un mediu prietenos copilului, iar declarațiile să poată fi utilizate pe parcursul procedurilor pentru a evita expunerea repetată a minorului la retraumatizare. De asemenea, copilul și familia trebuie să primească informații clare despre drepturile lor, despre etapele procedurii și despre serviciile de sprijin disponibile. Lipsa informațiilor generează anxietate și neîncredere în sistem. Un alt aspect important este pregătirea continuă a profesioniștilor. Polițiștii, procurorii, judecătorii, avocații, psihologii și asistenții sociali trebuie să înțeleagă impactul traumelor asupra copiilor și să adopte o comunicare adecvată vârstei și nivelului de dezvoltare al acestora. În cazurile care implică abuzuri online, este esențială și protejarea vieții private a copilului. Informațiile despre victimă, imaginile sau alte date care permit identificarea acestuia trebuie tratate cu maximă confidențialitate pentru a preveni stigmatizarea și noi forme de victimizare. În ultimii ani, Republica Moldova a făcut progrese importante în domeniul justiției prietenoase copilului. Totuși, protecția eficientă presupune ca fiecare instituție care intră în contact cu minorul să acționeze coordonat, sensibil la traumă și orientat spre recuperarea copilului, nu doar spre administrarea procedurilor.
--	--

D. Feedback pe opțiunile de reglementare

#	Întrebare	Notițe / idei-cheie
1	Din perspectiva dvs., o interdicție generală de acces sub o anumită vârstă ar proteja real copiii sau ar muta problema în zone mai puțin vizibile? De ce întrebăm: Pentru a testa scenariul restrictiv din perspectiva protecției reale.	Din perspectiva mea, o interdicție generală de acces la platformele digitale sub o anumită vârstă nu ar rezolva problema și există riscul să o mute în zone mai puțin vizibile și mai greu de monitorizat. Experiența arată că majoritatea copiilor și adolescenților găsesc modalități de a ocoli restricțiile tehnice atunci când acestea nu sunt însoțite de educație și supraveghere adecvată. În aceste condiții, activitatea lor online poate deveni mai puțin transparentă pentru părinți și autorități, iar riscurile pot fi chiar mai greu de identificat.

	De ex.: Eludare, conturi ascunse, migrare către spații mai puțin controlate, efect simbolic vs. efect real. Consider că accentul trebuie pus pe educația digitală, dezvoltarea gândirii critice și informarea copiilor cu privire la riscurile pe care le pot întâlni online. Copiii trebuie să învețe cum să recunoască tentativele de manipulare, exploatare sexuală, șantaj, fraude sau recrutare pentru activități infracționale. Totodată, părinții trebuie sprijiniți să înțeleagă mediul digital în care trăiesc copiii lor și să dezvolte o relație bazată pe comunicare și încredere, astfel încât copilul să poată solicita ajutor atunci când se confruntă cu o situație periculoasă. Din practica mea, riscurile cele mai grave nu apar doar pentru că un copil are acces la internet, ci pentru că nu recunoaște pericolul sau nu știe cui să ceară ajutor. De aceea, cred că soluția nu este excluderea copiilor din mediul digital, ci pregătirea lor pentru a naviga în siguranță într-un spațiu care face deja parte din viața lor de zi cu zi. O interdicție poate fi un instrument complementar pentru anumite categorii de servicii sau platforme, dar nu poate înlocui educația, supravegherea parentală și mecanismele eficiente de protecție a copiilor.
2 Vi se pare mai util un model care obligă platformele să reducă riscurile și să își schimbe practicile? De ce întrebăm: Pentru a evalua acceptabilitatea modelului progresiv. De ex.: Profilare, recomandări, publicitate, raportare, contact cu necunoscuți, standarde minime.	Da, consider că un model care obligă platformele să identifice, să prevină și să reducă riscurile pentru copii este mult mai eficient decât unul bazat exclusiv pe interdicții adresate minorilor. O mare parte dintre riscurile din mediul online nu sunt generate de simpla prezență a copiilor pe internet, ci de modul în care anumite platforme sunt concepute și funcționează. Algoritmii care promovează conținut nociv, posibilitatea contactării minorilor de către persoane necunoscute, mecanismele insuficiente de raportare a abuzurilor sau reacțiile întârziate la sesizări contribuie la expunerea copiilor la pericole. Din experiența mea profesională, copiii care au devenit victime ale exploatării sexuale online, ale șantajului cu imagini intime sau ale recrutării pentru activități infracționale au fost adesea contactați și manipulați prin intermediul platformelor digitale. De aceea, responsabilitatea nu poate fi plasată exclusiv pe umerii copiilor și ai părinților. Un model eficient ar trebui să impună platformelor obligații concrete: evaluarea riscurilor pentru minori, măsuri de siguranță adaptate vârstei, limitarea contactului dintre adulți necunoscuți și copii, proceduri rapide de eliminare a conținutului abuziv și mecanisme accesibile de raportare. În același timp, este important ca aceste măsuri să fie însoțite de garanții privind respectarea drepturilor fundamentale, inclusiv dreptul la viață privată și accesul la informație.

		În opinia mea, protecția eficientă a copiilor în mediul digital presupune o responsabilitate comună. Copiii trebuie educați, părinții trebuie sprijiniți, autoritățile trebuie să intervină eficient, iar platformele trebuie să își asume un rol activ în reducerea riscurilor pe care propriile servicii le pot genera.
3	În ce condiții ar fi acceptabil un model de acces condiționat cu verificarea vârstei și implicarea părinților? De ce întrebăm: Pentru a testa limitele scenariului moderat. De ex.: Ce nu ar trebui colectat, rolul părinților, protecția datelor, proporționalitate.	În opinia mea, un model de acces condiționat, care implică verificarea vârstei și participarea părinților, poate fi acceptabil dacă este construit în interesul superior al copilului și respectă dreptul acestuia la viață privată. În primul rând, verificarea vârstei trebuie să fie proporțională și să nu presupună colectarea excesivă a datelor personale ale copiilor. Mecanismele utilizate trebuie să fie sigure, să protejeze confidențialitatea și să reducă la minimum riscul utilizării abuzive a datelor. În al doilea rând, implicarea părinților trebuie să fie una reală și orientată spre protecție, nu doar formală. Simpla solicitare a unui acord parental nu garantează siguranța copilului. Este important ca părinții să fie informați despre riscurile existente și să aibă instrumente prin care să poată sprijini și ghida copilul în utilizarea serviciilor digitale. Consider că un astfel de model este justificat în special pentru platformele și serviciile care prezintă riscuri sporite de exploatare sexuală, hărțuire, contact cu persoane necunoscute sau expunere la conținut dăunător. Totodată, trebuie să recunoaștem că nici verificarea vârstei și nici acordul parental nu reprezintă soluții suficiente în sine. Din experiența mea profesională, mulți copii care au devenit victime ale exploatării sexuale online sau ale altor forme de abuz aveau acces la tehnologie cu știrea părinților. Problema a fost că nici copiii, nici adulții nu au recunoscut la timp semnele pericolului. De aceea, un model eficient trebuie să combine verificarea vârstei și implicarea părinților cu obligații clare pentru platforme de a reduce riscurile, cu programe de educație digitală și cu mecanisme rapide de raportare și intervenție atunci când apare o situație de abuz. În final, cred că accentul trebuie pus nu pe controlul absolut al accesului, ci pe crearea unui mediu digital mai sigur, în care copiii să fie protejați fără a fi excluși de la oportunitățile pe care tehnologia le oferă.

E. Părinți, școală, instituții

#	Întrebare	Notițe / idei-cheie
1	Ce rol ar trebui să aibă părinții și ce rol nu ar trebui transferat abuziv asupra lor? De ce întrebăm: Pentru a evita formularea unei politici care mută întreaga responsabilitate spre familie. De ex.: Supraveghere, educație, acord parental, intervenție în criză.	Părinții au un rol esențial în protecția copiilor în mediul digital, însă responsabilitatea pentru siguranța online nu poate fi transferată exclusiv asupra lor. Rolul părinților este să comunice cu copiii despre riscurile existente, să dezvolte o relație bazată pe încredere, să stabilească reguli adecvate vârstei și să fie atenți la schimbările de comportament care pot indica faptul că minorul este victima unui abuz. De asemenea, părinții trebuie să fie informați despre mediul digital în care trăiesc copiii lor și să îi învețe cum să recunoască situațiile periculoase și cum să solicite ajutor. În același timp, nu consider că este corect sau eficient să transferăm asupra părinților întreaga responsabilitate pentru prevenirea și combaterea riscurilor online. În practică, mulți părinți nu au cunoștințe tehnice suficiente pentru a monitoriza toate platformele și aplicațiile utilizate de copii, iar infractorii folosesc metode tot mai sofisticate de manipulare și recrutare. Nu putem cere părinților să înlocuiască obligațiile statului, ale școlii sau ale platformelor digitale. Protecția copiilor trebuie să fie o responsabilitate comună. Platformele trebuie să reducă riscurile generate de propriile servicii, autoritățile trebuie să asigure mecanisme eficiente de prevenire și intervenție, iar sistemul educațional trebuie să contribuie la dezvoltarea competențelor digitale și de siguranță online. Din experiența mea profesională, atunci când un copil devine victima exploatării sexuale online, a șantajului cu imagini intime sau a recrutării pentru activități infracționale, rareori există o singură cauză sau o singură persoană responsabilă. De aceea, soluțiile trebuie să fie construite pe ideea de responsabilitate partajată, nu pe transferarea întregii poveri asupra familiei. Părinții trebuie să fie parteneri în protecția copilului, nu singurii responsabili pentru siguranța acestuia într-un mediu digital din ce în ce mai complex. Dacă ne dorim ca o astfel de inițiativă să funcționeze în practică, este esențial să fie construită pe o cooperare reală între instituțiile care interacționează cu copiii și familiile acestora. În primul rând, consider că instituțiile din domeniul educației trebuie să aibă un rol central. Copiii petrec o mare parte din timp în școală, iar profesorii și psihologii școlari pot identifica timpuriu situațiile de risc și pot contribui la dezvoltarea competențelor de siguranță digitală.
2	Ce instituții ar trebui implicate prioritar dacă vrem ca inițiativa să funcționeze în practică? De ce întrebăm: Pentru prioritizarea recomandărilor instituționale.	

De ex.: Educație, protecția copilului, date cu caracter personal, cyber, poliție, ombudsman, egalitate.	Poliția trebuie implicată prioritar atât în componenta de prevenire, cât și în cea de intervenție. În cazurile de exploatare sexuală online, șantaj, hărțuire sau recrutare pentru activități infracționale, reacția rapidă este esențială pentru protejarea copilului și identificarea autorilor. Un rol important revine și autorităților de protecție a copilului și asistenței sociale, care trebuie să evalueze situația copilului, să coordoneze măsurile de protecție și să ofere sprijin familiei. De asemenea, este necesară implicarea sistemului de justiție – procurori, judecători și avocați specializați – pentru a asigura investigarea eficientă a cauzelor și respectarea drepturilor copilului victimă pe parcursul procedurilor. Nu trebuie neglijată nici contribuția serviciilor de sănătate și a psihologilor, deoarece multe victime ale violenței digitale au nevoie de sprijin psihologic pentru a depăși efectele traumei. În același timp, consider că succesul unei astfel de inițiative depinde și de implicarea platformelor digitale și a furnizorilor de servicii online, care trebuie să coopereze în eliminarea conținutului abuziv și în reducerea riscurilor pentru copii. Din perspectiva mea, cea mai mare provocare nu este lipsa instituțiilor, ci cooperarea dintre acestea. Republica Moldova dispune deja de actori relevanți și de un cadru legal relativ bun. Ceea ce face diferența este capacitatea instituțiilor de a comunica, de a interveni coordonat și de a pune interesul superior al copilului în centrul fiecărei decizii.
3 Ce măsuri non-penale sau non-restrictive considerați esențiale? De ce întrebăm: Pentru a completa abordarea legislativă cu măsuri de suport. De ex.: Consiliere, educație digitală, intervenție timpurie, suport psihologic, ghiduri pentru școli.	Din perspectiva mea, măsurile non-penale și non-restrictive sunt la fel de importante, dacă nu chiar mai importante, decât sancțiunile. Majoritatea riscurilor din mediul digital pot fi prevenite mai eficient prin educație, informare și intervenție timpurie decât prin aplicarea unor pedepse după producerea prejudiciului. În primul rând, este esențială introducerea și consolidarea programelor de educație privind siguranța online pentru copii, părinți și cadre didactice. Copiii trebuie să învețe cum să recunoască tentativele de manipulare, exploatare sexuală, șantaj, fraude sau recrutare pentru activități infracționale. În al doilea rând, sunt necesare campanii publice de informare și conștientizare. Din experiența mea profesională, multe victime și familiile acestora nu cunosc riscurile existente și nici mecanismele prin care pot solicita ajutor.

O altă măsură importantă este dezvoltarea serviciilor de consiliere psihologică și suport specializat pentru copii și părinți. În multe situații, intervenția unui psiholog sau a unui specialist poate preveni agravarea consecințelor unui incident online.

Consider esențială și instruirea continuă a profesioniștilor – profesori, polițiști, asistenți sociali, psihologi, procurori și judecători – pentru a recunoaște noile forme de violență și exploatare din mediul digital și pentru a răspunde adecvat acestora.

De asemenea, platformele digitale ar trebui încurajate să adopte măsuri de siguranță prin design, inclusiv setări de protecție adaptate copiilor, mecanisme simple de raportare și instrumente eficiente de blocare și filtrare a conținutului abuziv.

În opinia mea, cea mai eficientă strategie este cea care reușește să prevină victimizarea înainte ca aceasta să se producă. Educația, informarea, sprijinul psihologic și cooperarea dintre instituții reprezintă investiții care oferă rezultate mai durabile decât măsurile exclusiv punitive sau restrictive.

