ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Regulamentul privind serviciile digitale - protecția minorilor în mediul online-

Campanie de informare publică

Ce este Regulamentul privind serviciile digitale (DSA)?

- Adoptat la 19 octombrie 2022, este aplicabil în integralitate începând cu 17 februarie 2024
- DSA se aplică **furnizorilor de servicii intermediare** oferite în Uniunea Europeană, indiferent de locul de stabilire al acestora.
- Obiectivele DSA:
  - crearea unui **mediu online mai transparent**, **mai sigur și mai responsabil**
  - protejarea **drepturilor fundamentale în spațiul digital** prin stabilirea de noi norme
- Reglementează nu doar **eliminarea conținutului ilegal**, ci și **responsabilitatea** pentru modul în care informația este amplificată, recomandată și monetizată.
- Coordonatorii Serviciilor Digitale (DSC): Supravegherea aplicării DSA este descentralizată, fiecare stat UE desemnând o **autoritate națională cu rol de coordonator** (în România - ANCOM).

ANCOM

Contextul european: De ce era imperativă reglementarea?

- **Platformele online** sunt accesate de **un număr tot mai mare de minori**

- **Riscurile digitale** au evoluat de la simpla expunere la conținut ilegal la riscuri comportamentale, precum **grooming**, **cyberbullying** și **dependența** cauzată de algoritmi.

- **Modelele de autoreglementare** au eșuat, deoarece măsurile voluntare au fost fragmentate și subordonate obiectivelor de creștere a timpului de utilizare.

- **În Uniunea Europeană**, **siguranța este tratată ca un drept fundamental**, iar **interesul superior al copilului** trebuie să primeze în fața intereselor comerciale ale furnizorilor de servicii.

Articolul 28 din DSA: Un nou cadru pentru protecția minorilor

- Conform **articolului 28 alineatul 1**, orice platformă online accesibilă minorilor trebuie să instituie măsuri adecvate și proporționale pentru a asigura un nivel ridicat de **confidențialitate, siguranță și securitate**.
- Platformele **nu mai beneficiază de imunitate pasivă**, ci trebuie să adopte o **abordare proactivă**, anticipând riscurile și blocând funcționalitățile periculoase pentru copii.
- **Măsurile de protecție** trebuie implementate astfel încât să respecte **drepturile fundamentale ale copiilor**, inclusiv libertatea de exprimare, asociere și accesul la informații educative.
- **Articolul se aplică într-un mod larg**, vizând nu doar platformele dedicate copiilor, ci **orice platforme online** pe care minorii le pot accesa, precum rețele sociale, forumuri sau platforme de e-commerce.

Rolul strategic al Orientărilor Comisiei Europene (Iulie 2025)

- Orientările **clarifică cerințele legale**, explicând concret ce înseamnă noțiuni precum **„măsuri adecvate”** și oferind exemple aplicate pentru **protecția copiilor și adolescenților**.

- Deși **nu modifică legislația**, ele stabilesc un **reper practic** pentru evaluarea conformității cu prevederile Regulamentului.

- Platformele **pot alege să nu urmeze Orientările**, dar trebuie să demonstreze că soluțiile adoptate oferă un **nivel de protecție echivalent**.

- În același timp, Orientările funcționează ca un **ghid practic** pentru echipele de dezvoltare, sprijinind proiectarea unor **funcționalități mai sigure**.

Interfețele: Protecție integrată încă de la început

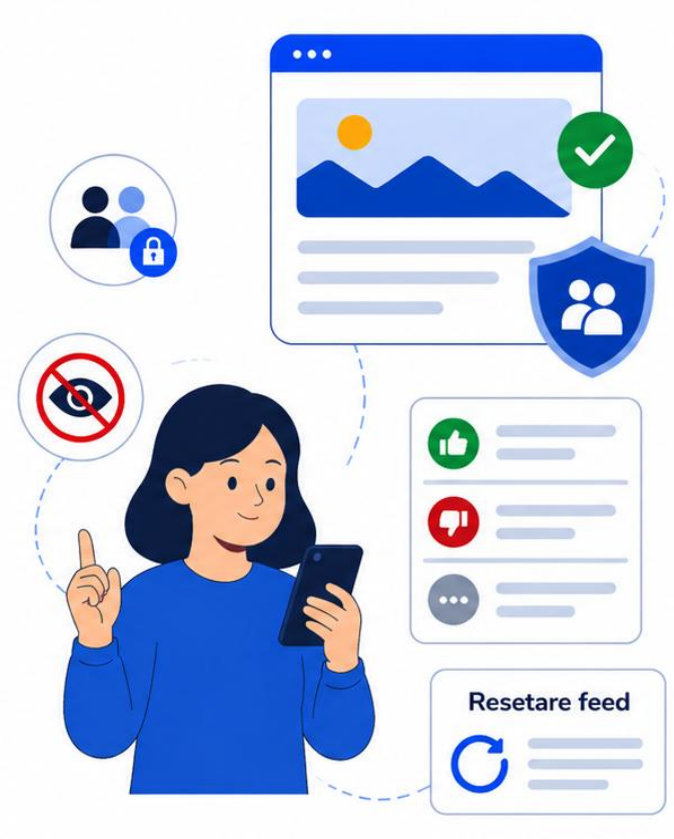
- **Interfața** reprezintă modul în care utilizatorii văd și folosesc platforma, iar o proiectare adecvată contribuie la crearea unui **mediu sigur**, în care copiii și adolescenții se simt încrezători și confortabil online.
- **Setările de siguranță** și instrumentele de **semnalare și feedback** trebuie să fie ușor de găsit, înțeles și utilizat.
- Pentru a preveni utilizarea excesivă și dependența, platformele trebuie **să evite practici manipulative**, precum derularea infinită, notificările constante sau recompensele automate.
- Platformele trebuie să includă instrumente pentru **gestionarea timpului petrecut online**, să asigure **accesibilitate** pentru toți utilizatorii și să ofere **avertismente clare** în cazul interacțiunii cu sisteme de **inteligență artificială**.

Măsuri de siguranță - Setările implicite și limitarea expunerii

- **Dezactivarea funcțiilor riscante** precum: localizarea geografică, redarea automată a videoclipurilor, microfonul sau sincronizarea contactelor.
- **Conturile trebuie să fie private** și să permită doar interacțiuni de la conturi pe care aceștia le-au acceptat în prealabil
- **Restricționarea mesageriei directe** - Conturile minorilor nu ar trebui să poată primi mesaje de la adulți pe care nu îi au deja în lista de contacte aprobată.
- Niciun cont **să nu poată descărca sau efectua capturi de ecran** cu datele de contact, informațiile privind locația, contul sau conținutul încărcat sau partajat de minori pe platformă.
- **Tranziția către vizibilitate** - Orice reducere a nivelului de intimitate trebuie să necesite o acțiune manuală, conștientă și explicată pe larg minorului.

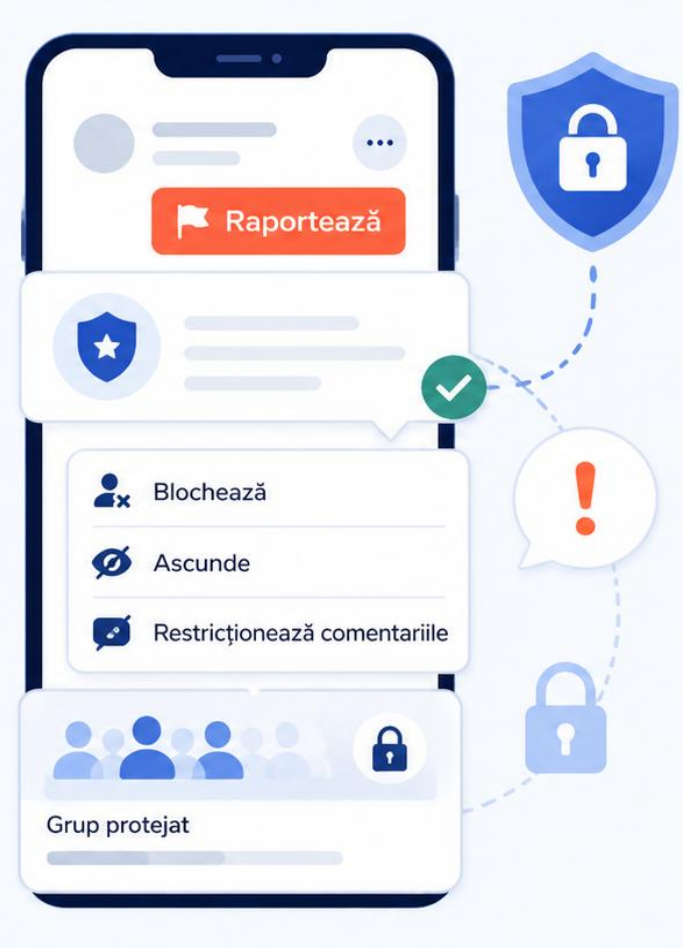
Optimizarea și limitarea Sistemelor de Recomandare

- ✓ Platformele online trebuie să **afișeze conținut adecvat vârstei utilizatorilor**.
- ✓ Se impune **limitarea profilării invazive**: reducerea volumului de date colectate și utilizate pentru recomandări
- ✓ Să acorde prioritate alegerilor și feedbackului activ al utilizatorilor, precum:
  - „Arată-mi mai puțin/mai mult din asta”
  - „Nu vreau să văd asta”
  - „Nu mă interesează asta”
- ✓ Utilizatorii trebuie să aibă acces la **feed-uri alternative**, inclusiv:
  - opțiunea de **resetare completă și permanentă a fluxului de conținut**



Moderare și mecanisme de raportare

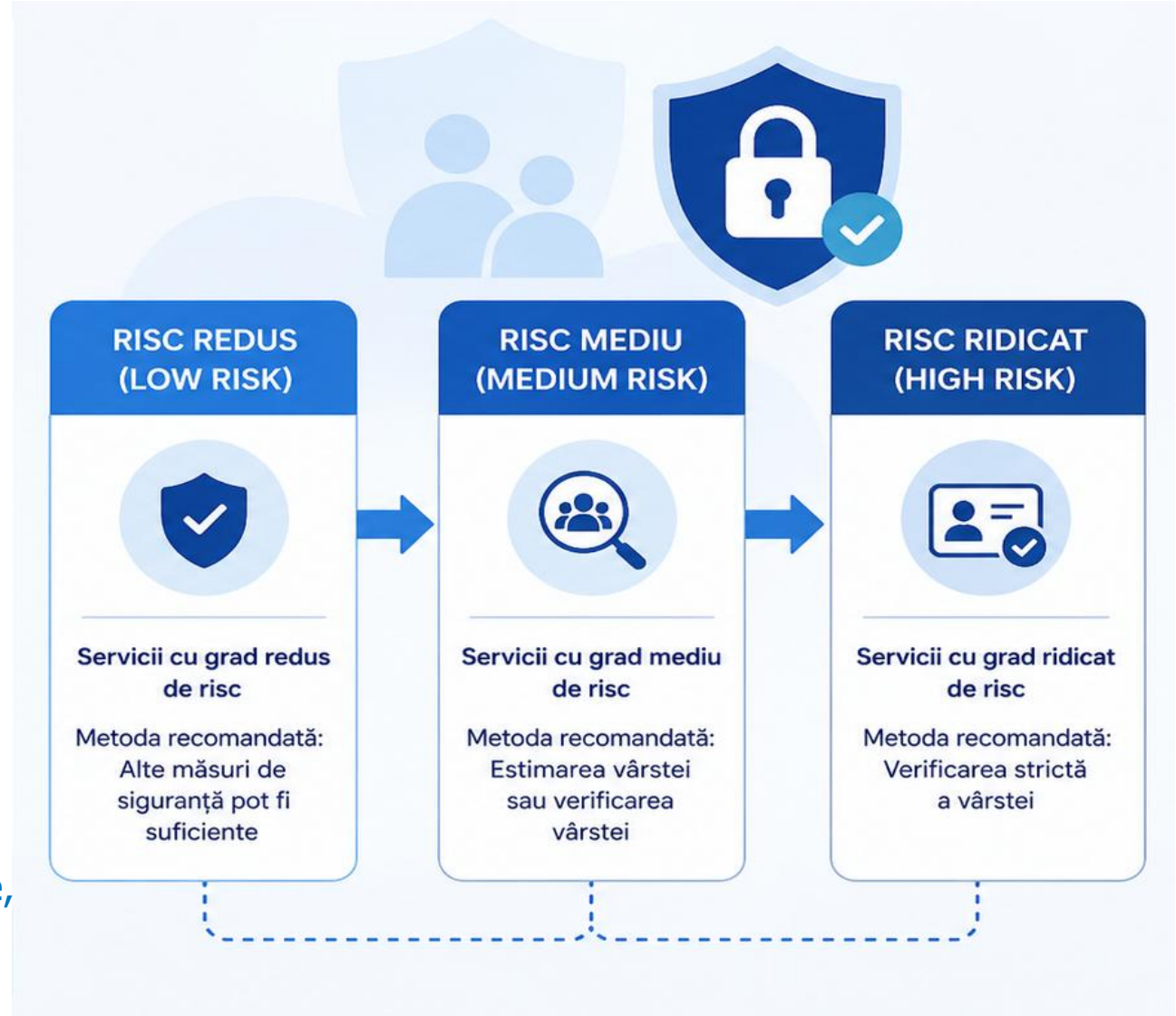
- **Raportare rapidă și accesibilă**
  Butoanele de raportare trebuie să fie **vizibile și ușor de utilizat**, fără navigare prin meniuri complexe.
- **Prioritizarea cazurilor sensibile**
  Conținutul care afectează **confidențialitatea, siguranța și securitatea minorilor** trebuie analizat cu prioritate.
- **Instrumente de control pentru utilizatori**
  Posibilitatea de a **bloca, ascunde sau restricționa** comentarii și interacțiuni nedorite.
- **Protecția minorilor în grupurile online**
  Mecanisme clare pentru a **preveni adăugarea minorilor fără consimțământ** în grupuri mari de chat.



Verificarea vârstei - Echilibrul între siguranță și confidențialitate

- **Dincolo de simpla bifare a unei căsuțe**
  Formularele clasice ('Am peste 18 ani') sunt considerate insuficiente pentru serviciile care prezintă un risc mediu sau ridicat pentru copii.
- **Spectrul soluțiilor tehnologice**
  Include auto-declararea, estimarea vârstei prin analiză de comportament sau AI și verificarea strictă a identității prin aplicații de verificare a vârstei.
- **Principiul proporționalității**
  Măsurile trebuie să fie adaptate nivelului de risc pentru a proteja eficient copiii, fără a impune bariere inutile

Aceste metode trebuie să fie fiabile, precise și sigure, dar în același timp neintruzive



Ce pot face minorii pentru a fi în siguranță online

- ✓ Păstrarea setării conturilor ca **private** și limitarea accesului persoanelor necunoscute

- ✓ Evitarea distribuirii de **informații personale** (adresă, școală, număr de telefon)

- ✓ Utilizarea funcțiilor de **blocare și raportare** în cazul comportamentelor nepotrivite

- ✓ Verificarea conținutului și **evitarea accesării** materialelor suspecte sau dăunătoare

- ✓ Gestionarea timpului petrecut online și **evitarea utilizării excesive** a platformelor

- ✓ Discuția cu un adult de încredere în cazul unor situații neplăcute

ANCOM

Cum își pot proteja parintii copiii în mediul online

- ✓ **Discuții deschise** și constante despre activitatea copiilor în mediul online

- ✓ Stabilirea unor **reguli clare** privind utilizarea dispozitivelor și platformelor

- ✓ Utilizarea instrumentelor de **control parental** și monitorizare adecvată

- ✓ **Informarea** despre platformele utilizate de copii și riscurile asociate

- ✓ **Reacția promptă și sprijinul** acordat copilului în cazul unor situații problematice

Rolul mediului educațional

- **Rolul instituțiilor de învățământ în ecosistemul DSA**
  - creșterea nivelului de **conștientizare a elevilor** privind riscurile din mediul online;
  - sprijinirea dezvoltării **competențelor digitale și a gândirii critice**;
  - **identificarea și semnalarea situațiilor de risc** (conținut dăunător, comportamente abuzive);
  - **colaborarea cu părinții și alte instituții relevante** pentru protecția minorilor;

Activități și exemple practice pentru profesori

💬 Discuție ghidată

Obiectiv: Constientizarea riscurilor online

- exemple reale de riscuri online;
- cyberbullying și comportamente toxice;
- protecția datelor personale;
- utilizarea responsabilă a rețelelor sociale

🔍 Analiza unui caz

Obiectiv: Dezvoltarea gândirii critice

- identificarea riscurilor într-o situație online;
- cum reacționează elevii;
- ce instrumente pot folosi;
- discutarea soluțiilor corecte.

🛡️ Atelier practic

Obiectiv: Dezvoltarea competențelor digitale

- verificarea setărilor de confidențialitate;
- utilizarea funcțiilor „block” și „report”;
- identificarea conținutului manipulator;
- gestionarea timpului petrecut online.

🤝 Proiect de clasă

Obiectiv: promovarea unui climat online sigur

- elevii creează afișe sau prezentări despre siguranța online;
- colaborare cu părinții și consilierul școlar;
- campanii de conștientizare în școală.

Resurse utile pentru profesori:
https://edu.ro/ghid_orientari_metodologice_profesori_combatere_dezinformare_si_promovare_alfabetizare_digitala

ANCOM

Vă mulțumesc!