EDRi
European Digital Rights

Document de poziție

Verificarea online a vârstei și drepturile copiilor

4 octombrie 2023

Acest document reprezintă poziția comună a 20 de organizații ale societății civile: Alternatif Bilisim (Turcia), ApTI (România), Bits of Freedom (Olanda), CCC (Germania), Defend Digital Me (Marea Britanie), Digitalcourage (Germania), Digitale Gesellschaft (Elveția), Electronic Frontier Foundation (internațional), EFN (Norvegia), epicentru.works (Austria), ESWA (Europa), European Digital Rights (Europa), FIPR (Regatul Unit), Homo Digitalis (Grecia), Irish Council for Civil Liberties (Irlanda), IT-Pol (Danemarca), Metamorphosis Foundation (Macedonia de Nord), Politiscope (Croația), SHARE Foundation (Serbia) și SUPERRR Lab (Germania).

Cuprins

Publicat la Bruxelles, 4 octombrie 2023.

European Digital Rights (EDRi) mulțumește sincer membrilor și partenerilor noștri care au contribuit la cercetarea, redactarea și revizuirea acestui document.

Traducere în limba româna de ApTI făcuta publica pe 19 decembrie 2023.

Rezumat

Legiuitorii apelează din ce în ce mai des la verificarea vârstei ca modalitate de combatere a daunelor și a activităților ilegale online, de exemplu în proiectul de regulament al UE privind abuzul sexual asupra copiilor. Însă, deși numai industria UE de verificare a vârstei atinge o valoare de câteva miliarde de euro, nu există dovezi că măsurile de verificare a vârstei îmbunătățesc siguranța copiilor online.

Acest studiu constată că, cu excepția metodelor de declarare a vârstei, verificarea vârstei reprezintă o amenințare la adresa vieții private, a protecției datelor și a dreptului la liberă exprimare a copiilor și a adulților deopotrivă. Acest lucru poate eroda libertățile democratice care se bazează pe anonimatul online (de exemplu, jurnalismul), poate încălca autonomia copiilor și poate lipsi de putere părinții și tutorii.

De asemenea, este probabil ca astfel de măsuri să aibă cele mai profunde consecințe negative pentru copiii și adulții care se confruntă deja cu niveluri ridicate de excluziune structurală sau de discriminare și pentru cei cu un nivel scăzut de alfabetizare digitală. Constatăm că, în special, este puțin probabil ca verificarea și estimarea vârstei pe bază de documente să treacă testul drepturilor omului privind necesitatea și proporționalitatea.

1. Declarația de vârstă:

- Declararea vârstei este termenul pentru măsurile prin care se cere unei persoane să își precizeze vârsta.
- Acest studiu constată că aceste metode prezintă cele mai puține riscuri pentru drepturile online ale tuturor și sunt deja legale în UE în temeiul GDPR.
- Cu toate acestea, aceste măsuri sunt, de asemenea, cele mai susceptibile de a fi eludate, astfel încât, pentru a fi eficiente, ar trebui privite ca parte a unei abordări holistice care să includă confidențialitatea și siguranța prin concepție, etichetarea conținutului, încrederea și supravegherea părinților/tutorelui și educația.

2. Verificarea vârstei pe bază de documente:

- Uneori denumită pur și simplu verificare a vârstei, aceasta înseamnă măsuri care privesc verificarea de informații dintr-un document oficial (cum ar fi scanarea unui pașaport, a unei cărți de identitate electronice sau a unui card de credit)
- Deși, în teorie, astfel de măsuri ar putea fi luate într-un mod care să protejeze datele persoanelor, acest studiu constată că metodele actuale și previzibile de verificare a vârstei pe bază de documente creează riscuri ridicate de încălcare a securității datelor, de supraveghere omniprezentă online, efecte disuasive asupra activităților legitime și de exacerbare a excluziunii structurale;
- Astfel de măsuri nu ar trebui să fie impuse. Utilizarea lor de la caz la caz ar trebui să fie strict controlată, protejată și numai atunci când este strict necesar (adică nu pe scară largă).

3. Estimarea vârstei:

- Estimarea vârstei se referă la măsurile care prezic sau estimează vârsta persoanelor, de exemplu, pe baza interacțiunilor acestora sau prin utilizarea unor instrumente bazate pe inteligență artificială pentru a le analiza chipul;

- Astfel de măsuri se bazează pe colectarea în masă de date personale sau pe practici comerciale toxice (de exemplu, crearea de profiluri). În mod frecvent, acestea includ prelucrarea datelor biometrice sensibile ale copiilor;
- Ca atare, măsurile de estimare a vârstei prezintă un risc inacceptabil şi nu ar trebui să fie utilizate.

Introducere

Guvernele din întreaga lume propun din ce în ce mai multe legi și politici menite să abordeze riscurile pentru copii (definiți în *Convenția ONU privind drepturile copilului* ca fiind orice persoană cu vârsta sub 18 ani) care pot apărea atunci când aceștia utilizează anumite spații online sau participă la anumite activități online. **Măsurile de evaluare sistematică a vârstei online au fost prezentate de către industria în creștere a verificării vârstei ca și cum ar fi un remediu pentru riscurile cu care se confruntă copiii în mediul online.** Propuneri de impunere a obligativității verificării online a vârstei au fost întâlnite în SUA, Regatul Unit, India, Australia, Uniunea Europeană (UE) și nu numai.

Acest raport se concentrează pe problema verificării online a vârstei și pe cele trei tipuri principale ale acesteia (verificarea pe bază de documente, estimare și declarație), acordând o atenție deosebită contextului UE și normelor din *Regulamentul general privind protecția datelor (GDPR)*. Această problemă este presantă în UE deoarece proiectul de *regulament privind abuzul sexual asupra copiilor* (CSA) propune să impună forme de verificare a vârstei pentru serviciile de mesaje private (de exemplu, WhatsApp, Signal) și magazinele de aplicații care operează în UE și să o stimuleze puternic pentru toate celelalte platforme și servicii digitale, cum ar fi rețelele sociale[1].

Problema verificării online a vârstei este complexă. Există o nevoie legitimă de a se asigura că copiii pot accesa conținuturi considerate adecvate din punct de vedere legal pentru vârsta lor. Unele țări au norme naționale privind accesul la anumite servicii cu restricții de vârstă (de exemplu, jocurile de noroc). În sens mai larg, guvernele și companiile au obligația de a proteja copiii împotriva abuzurilor, manipulării și exploatării online (toate acestea putând aduce atingere demnității, intimității și nu numai).

Cu toate acestea, **nu există dovezi că adoptarea pe scară largă a sistemelor de verificare a vârstei online ca măsură preliminară pentru a accesa mesageria privată, descărcarea de aplicații sau rețelele de socializare va menține copiii în siguranță**. Măsurile disponibile în prezent pentru verificarea vârstei au un impact potențial grav asupra drepturilor omului - în special pentru copiii pe care se presupune că îi protejează. **Unul dintre obiectivele acestui document este de a sensibiliza opinia publică cu privire la faptul că măsurile de verificare a vârstei nu ar trebui să fie considerate o soluție simplă pentru activități ilegale precum abuzul online asupra copiilor**. O concentrare excesivă asupra punerii în aplicare a sistemelor de verificare a vârstei poate ascunde problemele societale care facilitează sau exacerbează daunele online în primul rând, prin încadrarea problemei ca fiind una tehnică, când, de fapt, este una profund umană. **O abordare mai holistică, care consideră verificarea vârstei ca pe un spectru de măsuri de sprijin, mai degrabă decât restrictive - bazate pe confidențialitate și siguranță prin concepție - are mai multe șanse de a fi eficientă și de a respecta drepturile.**

După cum subliniază atât Organizația Națiunilor Unite, cât și UNICEF, copiii au dreptul la libertatea de exprimare și la accesul la informații online[2]. Autonomia și dezvoltarea lor personală - care pot fi o parte importantă a explorării identității lor, de exemplu, a sexualității sau a participării

[1]Propunerea Comisiei Europene se referă la măsuri de "verificare și evaluare a vârstei". Aceasta ar exclude declarațiile pe proprie răspundere (cum ar fi introducerea datei de naștere), dar ar permite verificări care utilizează documente de identitate legale sau instrumente predictive (adică bazate pe inteligență artificială).

[2]Comentariul general 25 al Organizației Națiunilor Unite: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F25&Lang=en; Toolkit-ul UNICEF privind confidențialitatea online a copiilor și libertatea de exprimare: https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

lor democratice - depind de posibilitatea de a căuta și de a comunica liber online. Având în vedere că instrumentele digitale reprezintă o parte importantă din viața majorității tinerilor și, mai ales în urma pandemiei de COVID-19, totul, de la educație la divertisment, a devenit și mai digitalizat. Prin urmare, orice măsură care ar putea avea ca rezultat limitarea sau controlul accesului tinerilor la servicii și conținuturi online legitime ar trebui abordată cu mare precauție.

Există riscuri serioase pentru adulți și copii deopotrivă dacă accesul anonim la internet este îngreunat sau imposibil, precum și riscuri de excluziune digitală pentru cei care nu au acces la instrumentele sau documentele adecvate. Ca societate, am văzut că nu s-a luat prea mult în considerare dacă este chiar de dorit să normalizăm nevoia de documente de identitate pentru a participa la viața socială. Dimpotrivă, EDRi avertizează că, din cauza informațiilor sensibile procesate și a impactului disproporționat asupra copiilor, a persoanelor fără adăpost, a persoanelor fără documente și a altor persoane care se confruntă cu excluziunea socială, cărțile de identitate ar trebui utilizate doar atunci când este strict necesar și în deplină conformitate cu legislația UE privind drepturile omului și cu *Convenția privind drepturile copilului*.

Pe baza metodelor și a riscurilor analizate în acest document, definim șase riscuri-cheie ale utilizării instrumentelor de verificare a vârstei și de estimare a vârstei în special, care sunt explicate mai detaliat în capitolul 4:

1. Încălcarea drepturilor copiilor la viață privată și la protecția datelor personale;
2. Încălcarea autonomiei și a exprimării de sine a copiilor în mediul online;
3. Permiterea companiilor să controleze ceea ce pot vedea și face online copiii;
4. Dificultatea sau imposibilitatea de a păstra anonimatul online;
5. Exacerbarea discriminării structurale; și
6. Crearea unui fals sentiment de securitate.

Analiza noastră constată că nu există instrumente de **verificare** sau de **estimare bazate pe documente la** nivelul UE care să minimizeze aceste riscuri în așa măsură încât utilizarea lor pe scară largă să poată fi considerată compatibilă cu drepturile copiilor în mediul online. Instrumentele de **declarare a** vârstei sunt mai susceptibile de a fi compatibile cu drepturile copiilor, dar necesită cercetări și dezvoltări suplimentare pentru a le spori eficiența. Din aceste motive, avertizăm că, ca regulă generală, **factorii de decizie politică și legislativă nu trebuie să impună măsuri de estimare a vârstei sau de verificare bazată pe documente.**

Prin urmare, considerăm că orice lege care obligă furnizorii să utilizeze sisteme de verificare a vârstei pentru a controla accesul la platformele și serviciile digitale în general - așa cum este propus de Regulamentul CSA - ar reprezenta o amenințare nejustificată la adresa drepturilor digitale ale copiilor și trebuie respinsă. În special, **instrumentele de verificare și estimare bazate pe documente nu ar trebui să devină obligatorii prin Regulamentul CSA și nici nu ar trebui ca utilizarea lor să fie stimulată prin intermediul procesului propus de evaluare și reducere a riscurilor.**

Recomandările, codurile de conduită și alte politici ar putea garanta că, în cazul în care se demonstrează că anumite metode de verificare a vârstei sunt eficiente, proporționale și nediscriminatorii, acestea vor fi utilizate într-un mod care să fie conform cu *Regulamentul general privind protecția datelor* și să atenueze riscurile discutate în capitolul 4. Șaptesprezece recomandări specifice sunt furnizate la sfârșitul acestui raport.

Capitolul 1. Contextul juridic

1.1. Carta drepturilor fundamentale a UE

Carta drepturilor fundamentale a UE ("Carta") garantează drepturile și libertățile tuturor, inclusiv drepturile fundamentale la viața privată, la libera exprimare și la accesul la informații. Drepturile copiilor la viața privată, la libera exprimare și la accesul la informații sunt codificate în continuare în *Convenția internațională privind drepturile copilului (*CDC). Aceste drepturi se aplică online, la fel ca și offline, și pot funcționa adesea ca porți de acces la exercitarea altor drepturi ale omului. De exemplu, votul în UE se desfășoară întotdeauna în mod anonim, deoarece este un principiu al democrației conform căruia viața privată este esențială pentru ca oamenii să își dezvolte și să își exercite drepturile democratice în mod liber și fără interferențe sau judecăți.

Din motive similare, în general, nu credem că prezentarea documentelor de identitate ar trebui să devină un element obligatoriu pentru implicarea în viața publică. Riscurile care decurg din identificarea persoanelor oriunde s-ar duce - de la un efect de restricționare a libertăților politice ale oamenilor, până la excluderea celor care nu au documentele necesare - pot fi grave. Deși pot exista scenarii specifice în care dezvăluirea documentelor de identitate poate fi justificată, adoptarea pe scară largă a unor astfel de practici nu este justificabilă într-o societate democratică.

Aceste preocupări sunt la fel de prezente și atunci când vine vorba de utilizarea metodelor de verificare a vârstei online. Noi contestăm premisa că fie copiii, fie adulții ar trebui să fie nevoiți să prezinte documente oficiale - sau să furnizeze date personale sensibile - pentru a face lucruri precum descărcarea unei aplicații de mesagerie pentru a-și contacta familia. Astfel de măsuri ar schimba în mod fundamental modul în care funcționează internetul, precum și relația noastră cu internetul. Nu există nicio dovadă că astfel de măsuri vor menține copiii în siguranță. Dimpotrivă, noile cercetări arată că confidențialitatea și siguranța prin concepție, de exemplu, activarea implicită a funcțiilor de confidențialitate, reprezintă o modalitate eficientă de a proteja copiii online fără a le încălca dreptul la viață privată, la liberă exprimare și la protecția datelor.[3]În mod esențial, aceste măsuri pot atinge același scop de a proteja copiii, fără restricțiile asupra libertăților fundamentale care apar atunci când anonimatul în spațiile online nu mai este posibil pentru oricine.

1.2. Regulamentul general privind protecția datelor (GDPR) și Regulamentul privind serviciile digitale (DSA)

Regulamentul general privind protecția datelor (GDPR) (2016/679) se bazează pe dreptul la protecția datelor personale stabilit în Cartă, atât pentru adulți, cât și pentru copii. Acesta creează o serie de drepturi pentru ca oamenii să aibă cunoștință și control asupra prelucrării datelor lor cu caracter personal, precum și obligații pentru cei care le prelucrează (inclusiv furnizorii de servicii și platforme digitale).

Furnizorii care își desfășoară activitatea în UE utilizează deja frecvent formulare de declarație de vârstă, prin care un utilizator își confirmă vârsta, pentru ca furnizorul să își îndeplinească obligațiile care îi revin în temeiul articolului 8 din GDPR. Acest lucru permite copiilor cu vârsta de peste 16 ani să își dea propriul consimțământ pentru prelucrarea datelor lor cu caracter personal atunci când utilizează un "serviciu al societății informaționale" (de exemplu, o aplicație de socializare sau de

[3] De exemplu, https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online și https://www.brookings.edu/articles/using-safety-by-design-to-address-online-harms/

mesagerie). În cazul copiilor cu vârsta sub 16 ani, este necesar consimțământul părinților lor. Cu toate acestea, statele membre ale statele UE pot decide să stabilească o limită inferioară pentru care se poate aplica consimțământul parental, care nu trebuie să fie sub 13 ani. Optsprezece dintre cele 27 de state membre ale UE au făcut acest lucru.[4]

Aceasta înseamnă că vârsta la care consimțământul parental nu mai este obligatoriu în UE variază între 13 și 16 ani, în funcție de locul de reședință al copilului și/sau al furnizorului. Întrucât furnizorii trebuie să demonstreze că consimțământul pe care l-au obținut este valabil, GDPR este în general interpretat ca impunând o formă de verificare a vârstei pentru platformele sau serviciile care sunt oferite direct copiilor.

GDPR este un mecanism important pentru protecția drepturilor copiilor în ceea ce privește practicile de verificare a vârstei. Acesta impune furnizorilor care prelucrează datele copiilor să ia măsuri adecvate pentru a proteja acești copii, dar fără a-i obliga să utilizeze un anumit instrument de verificare a vârstei. Autoritățile de protecție a datelor pot contribui, de asemenea, la interpretarea unui echilibru adecvat al drepturilor atunci când vine vorba de utilizarea sistemelor de verificare a vârstei, având în vedere cât de multe drepturi fundamentale sunt în joc.

De asemenea, GDPR stabilește mecanisme de avertizare a furnizorilor care nu protejează suficient datele copiilor, inclusiv în ceea ce privește vârsta acestora. De exemplu, în septembrie 2023, TikTok a fost amendat cu 345 de milioane de euro de către autoritatea irlandeză pentru protecția datelor pentru că a făcut ca profilurile utilizatorilor copii să fie publice în mod implicit, pentru că i-a determinat pe aceștia să accepte setări care nu le respectau confidențialitatea și pentru că nu avea suficiente măsuri de protecție în legătură cu utilizatorii minori.[5] Odată ce *Regulamentul privind serviciile digitale* (DSA) (2022/2065), care a fost adoptată în 2022, va intra pe deplin în vigoare, companiile și autoritățile de reglementare vor avea la dispoziție și mai multe mecanisme legale pentru a se asigura că copiii sunt protejați online. Articolul 35 litera (j) din DSA permite în mod specific furnizorilor să utilizeze măsuri de verificare a vârstei.

1.3. Evaluarea necesității și proporționalității

După cum se va arăta în acest document, există mai multe moduri în care procesele de verificare a vârstei pot restrânge grav drepturile fundamentale la viața privată, protecția datelor, accesul la informații, libertatea de exprimare și de asociere, egalitatea și nediscriminarea. În special, ne concentrăm asupra exercitării acestor drepturi de către copii, ceea ce face ca pragul pentru ceea ce este considerat necesar și proporțional să fie și mai ridicat. Cu toate acestea, observăm, de asemenea, că marea majoritate a riscurilor ridicate în acest document se vor aplica la fel de puternic și adulților. În timp ce toți adulții care se bazează pe instrumente și servicii digitale vor fi afectați, efectul va fi deosebit de profund pentru cei a căror profesie și/sau siguranță se bazează pe confidențialitatea lor online: jurnaliști, avocați, apărători ai drepturilor omului, supraviețuitori ai violenței online (și offline), lucrători sexuali, activiști și mulți alții.

În conformitate cu articolul 52 alineatul (1) din Cartă, toate drepturile fundamentale menționate mai sus pot fi supuse unor limitări din partea statului. Cu toate acestea, această limitare trebuie să fie întotdeauna **necesară (**ceea ce înseamnă că măsurile propuse sunt eficiente pentru urmărirea unui scop legitim, iar intruziunea este limitată la minimul necesar pentru atingerea acestui scop), **proporțională** (ceea ce înseamnă că consecințele negative ale limitării nu depășesc beneficiile) și

[4] [4] https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/ consent-use-data-children

[5] [5] https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of TikTok

trebuie să fie prevăzută de lege. Sarcina de a demonstra, cu dovezi, că restricția este necesară și proporțională revine statului. Analiza efectuată în acest document sugerează că este puțin probabil ca principiile necesității și proporționalității să fie îndeplinite de orice sistem de verificare a vârstei pe scară largă, cu excepția declarațiilor pe propria răspundere. Acest lucru se datorează faptului că:

- Măsurile propuse (verificarea vârstei pe baza documentelor sau estimarea vârstei) sunt foarte intruzive;
- Există măsuri alternative eficiente, cum ar fi confidențialitatea și siguranța prin concepție și declarațiile privind vârsta;
- Riscurile la adresa drepturilor copiilor sunt semnificative; și
- Consecințele sociale negative ale introducerii pe scară largă a infrastructurilor online de verificare a vârstei sunt semnificative.

Cu toate acestea, drepturile copilului înseamnă că răspunsul nu poate fi să nu facem nimic. Este esențial ca platformele și serviciile să ia măsuri care să respecte drepturile în limitele competențelor lor, cum ar fi cele legate de proiectarea serviciilor și de minimizarea colectării datelor, pentru a proteja copiii pe platformele lor.

1.4. Propunerea de regulament al UE privind abuzul sexual asupra copiilor (CSAR)

Regulile de verificare a vârstei sunt prezentate în propunerea de *regulament al* UE privind *abuzul sexual asupra copiilor* în patru locuri cheie[6]:

Articolul 3.2 litera (b) încurajează puternic toți **furnizorii de servicii digitale care își desfășoară** activitatea în UE (inclusiv platformele de socializare, furnizorii de e-mail și serviciile de cloud) să utilizeze măsuri de verificare a vârstei pe bază de documente. Textul sugerează că riscul de a li se emite un "ordin de detectare" (ordin care le cere să scaneze comunicațiile utilizatorilor lor) este redus dacă dispun de astfel de măsuri de verificare a vârstei;

- Acest lucru face probabil ca chiar și platformele sau serviciile care nu sunt obligate să introducă verificarea vârstei pe bază de documente să aleagă să facă acest lucru, pentru a evita sancțiunile prevăzute de CSAR;
- În plus, raționamentul autorilor legislației nu este clar: nu sunt furnizate dovezi care să arate că există o corelație între faptul că un furnizor are măsuri de verificare a vârstei și un risc redus de diseminare a materialelor de abuz asupra copiilor.
- Articolul 4.3 prevede că serviciile de mesagerie private, inclusiv cele oferite prin intermediul platformelor de jocuri de noroc, trebuie să utilizeze măsuri de verificare a vârstei pe bază de documente sau de estimare a vârstei, dacă au identificat un risc de manipulare (ceea ce, în conformitate cu profilul de risc al CSAR, este posibil să fie toate serviciile de mesagerie private).
- Articolul 6 impune magazinelor de aplicații (de exemplu, Google Play, Apple Store și F-Droid) să blocheze "utilizatorii copii" (sub 17 ani) de la descărcarea aplicațiilor care prezintă un risc "semnificativ" de manipulare sexuală [articolul 6 alineatul (1) litera (b)] și să utilizeze măsuri de verificare a vârstei pe bază de documente sau de evaluare a vârstei pentru toți utilizatorii [articolul 6 alineatul (1) litera (c)].
- Articolele 7-11 pot obliga furnizorii de servicii să caute dovezi de manipulare sexuală în mesajele scrise sau audio sau în alte comportamente ale utilizatorilor lor în conversații care implică cel puțin un "utilizator copil". Informațiile colectate prin măsurile anterioare de

[6] [6] Rețineți că, întrucât nu există termeni stabili în legislația UE, RAA utilizează termenul "verificare a vârstei" pentru a se referi în mod specific la practicile de verificare a vârstei bazate pe documente.

verificare a vârstei ar fi utilizate pentru a obliga furnizorii să scaneze conversațiile în care cel puțin o persoană este un utilizator copil (de ex. fie între o persoană de peste 17 ani și o altă persoană sub 17 ani, fie între două sau mai multe persoane sub 17 ani):

- Acest lucru presupune că platformele vor ține o evidență permanentă a vârstei tuturor utilizatorilor lor, astfel încât să poată face în permanență distincția între utilizatorii copii și utilizatorii adulți;
- Problema mai amplă a motivelor pentru care detectarea grooming-ului nu este o practică solidă sau care respectă drepturile, precum și preocupările mai largi ale EDRi cu privire la CSAR sunt explicate în detaliu în documentul de poziție al EDRi și, prin urmare, nu sunt elaborate în continuare aici.[7]

Aceste măsuri propuse vor genera riscuri legate de drepturile omului, care sunt analizate pe larg în capitolul 4. În special, prin aceste măsuri, furnizorii ar fi obligați să prelucreze datele sensibile ale copiilor pentru a verifica vârsta acestora, precum și să blocheze accesul copiilor la anumite aplicații. Având în vedere că propunerea consideră că există un risc "semnificativ" la un prag foarte scăzut, este probabil ca aplicațiile axate pe protejarea vieții private a utilizatorilor lor - cum ar fi abținerea de la colectarea de date inutile și securizarea mesajelor prin criptare - să fie cele mai susceptibile de a fi blocate. Existența GDPR și a DSA pune și mai mult sub semnul întrebării necesitatea de a impune măsuri de verificare a vârstei la nivelul UE, de exemplu în Regulamentul CSA. Acest lucru se datorează faptului că măsurile de verificare a vârstei pot fi deja puse în aplicare în temeiul GDPR și al DSA [articolul 35 litera (j)] dacă se demonstrează că sunt necesare și proporționale.

[7] EDRi, "A safe internet for all: upholding private and secure communications" (Un internet sigur pentru toți: susținerea comunicațiilor private și sigure), octombrie 2022, disponibil la: https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf.

Capitolul 2. Categorii de verificare a vârstei

Deși terminologia nu este întotdeauna utilizată în mod consecvent, folosim termenul "**verificarea vârstei**" ca termen generic pentru o gamă largă de metode care încearcă să verifice - cu diferite niveluri de încredere - vârsta unei anumite persoane online. Vă recomandăm să evitați termenul "asigurarea vârstei", care este un termen frecvent promovat de sectorul comercială din acest domeniu. În 2021, o asociație a furnizorilor din domeniu a estimat că, până în 2026-2028, piața de verificare a vârstei din UE va valora aproape 4 miliarde de euro.[8] Pare probabil că oportunitatea financiară semnificativă care ar fi creată de adoptarea pe scară largă a acestor instrumente este un factor de motivare pentru multe companii care recomandă utilizarea unor astfel de instrumente.

În această lucrare, împărțim problema generală a verificării vârstei în categoriile "**declarație**" (denumită uneori "verificare a vârstei", "porți de vârstă" sau "atestare"), "**verificare pe bază de documente**" (denumită uneori "certificare") și "**estimare**" (denumită uneori "notare", "evaluare" sau "asigurare"), în fiecare dintre acestea fiind incluse numeroase metode, în funcție de funcționalitatea de bază pe care o utilizează pentru a determina vârsta unui anumit utilizator.[9] Acești termeni nu sunt definitivi, dar, la momentul redactării acestui document, par a fi cel mai bun mod de a face distincția între tipurile largi de metode.

Metodele de **declarare a vârstei** *funcționează, în general, cerând utilizatorului data nașterii sau categoria de vârstă (de exemplu, "confirmați că aveți peste 18 ani") pentru a obține accesul sau pur și simplu declarând (de exemplu, în termenii și condițiile de utilizare) că anumite servicii sau caracteristici nu sunt disponibile pentru utilizatorii sub o anumită vârstă. Unele metode cer contactelor să "garanteze" pentru un alt utilizator.*

Articolul 5 alineatul (1) litera (c) din GDPR impune furnizorilor să reducă la minimum datele cu caracter personal pe care le colectează și le prelucrează cu privire la utilizatorii lor. Citit împreună cu articolul 8 din GDPR, se interpretează de obicei că metodele de declarare a vârstei oferă un echilibru acceptabil - acestea evaluează în mod rezonabil vârsta fără a fi prea intruzive sau a acumula date sensibile. Această metodă nu este infailibilă, dar sensibilitatea datelor copiilor înseamnă că autoritățile de reglementare s-au ferit, pe bună dreptate, să încurajeze furnizorii să prelucreze în mod sistematic datele persoanelor, cu excepția cazului în care acest lucru este *strict* necesar.

În unele țări și în scopuri specifice, de exemplu pentru accesul la servicii pornografice sau de jocuri de noroc, un număr mic de guverne din UE au cerut sau au în vedere să ceară furnizorilor să verifice dacă utilizatorii au peste 18 ani. Astfel de sisteme de verificare a vârstei funcționează prin utilizarea documentelor oficiale sau a unor substitute pentru documente oficiale (de exemplu, un card de credit sau prin solicitarea ca persoanele să obțină un cod sau un simbol de dovadă a vârstei de la o locație

[8] https://avpassociation.com/thought-leadership/estimating-the-size-of-the-global-age-verification-market

[9] Există și alte categorii și metode de verificare a vârstei întâlnite în alte scenarii - cum ar fi testarea cu ultrasunete sau a densității osoase a copiilor care depun cereri de azil - care pot avea un impact foarte grav asupra drepturilor omului. Cu toate acestea, astfel de metode nu fac parte din domeniul de aplicare al prezentei informări, care se limitează la principalele metode de verificare a vârstei utilizate pentru serviciile sau platformele online.

fizică, cum ar fi un magazin sau un oficiu poștal, pe care o pot introduce apoi pentru a accesa serviciile online). Astfel de propuneri au fost frecvent întâmpinate cu îngrijorarea că acestea creează infrastructuri de supraveghere de mari dimensiuni care pot fi ușor folosite în mod abuziv sau reproiectate pentru alte forme de urmărire omniprezentă a vieții digitale a oamenilor.[10]

Metodele de **verificare a vârstei bazate pe documente** *funcționează, în general, prin solicitarea ca utilizatorul să furnizeze un document oficial de identitate sau un alt document pentru care există o limită de vârstă. Acesta poate fi verificat manual sau automat, fie de către un furnizor, fie de către un sistem guvernamental (de exemplu, eID) sau de către o terță parte.*

Deși, în teorie, ar fi posibil să existe în acest scop sisteme de identificare digitală eficiente și care să respecte drepturile fundamentale,[11] nu reprezintă în prezent o soluție fezabilă la nivelul UE. În fiecare stat membru al UE nu există dispozitive naționale de identitate electronică pentru toate persoanele care au depășit vârsta consimțământului digital. În plus, portofelul de identitate digitală planificat la nivelul UE în cadrul reformei eIDAS (ale cărui specificații exacte sunt încă în curs de negociere și, prin urmare, s-ar putea să nu fie suficient de protectiv pentru viața privată) nu va fi disponibil pe scară largă decât după câțiva ani de la adoptarea Regulamentului CSA. Copiii care nu dispun de propriile dispozitive sau ale căror țări nu eliberează o identitate electronică la vârsta lor vor fi fie excluși, fie dependenți de identitatea electronică a unui părinte sau tutore. În cazul tinerilor care riscă să fie controlați sau abuzați de către părinți sau tutori, aceștia ar putea fi în imposibilitatea de a accesa servicii și platforme digitale.

Comisia Europeană a estimat că, în cel mai optimist scenariu, până în 2030, portofelul european de identitate digitală va fi utilizat de 80% din populația eligibilă, ceea ce înseamnă un risc serios de excluziune digitală pentru restul de 20%.[12] Persoanele fără documente nu vor fi niciodată eligibile.

Având în vedere riscurile potențiale pe care le prezintă metodele de verificare a vârstei bazate pe documente, în special atunci când acestea pot lega utilizarea internetului de identitatea unei persoane, mulți furnizori au apelat recent la tehnici de estimare a vârstei în încercarea de a minimiza datele pe care le colectează și de a evita necesitatea de a se baza pe documente de identitate. Acest lucru este deosebit de relevant în contextul siguranței online a copiilor, deoarece este posibil ca unii tineri să nu dispună de documente de identitate oficiale sau să nu aibă acces la instrumente de identitate electronică solide, ceea ce înseamnă că estimarea vârstei este deja testată de servicii utilizate pe scară largă de copii, cum ar fi Instagram.

Metodele de **estimare a vârstei** *funcționează, în general, prin utilizarea datelor despre utilizator, combinate cu analize predictive (cum ar fi analiza facială sau alte instrumente bazate pe inteligență artificială), pentru a ghici vârsta acestuia. Aceasta se poate baza pe aspectul utilizatorului, pe preferințele sale online sau pe istoricul de internet.*

---

[10] [10] A se vedea, de exemplu: https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety și https://www.theguardian.com/australia-news/2023/aug/31/roadmap-for-age-verification-online-pornographic material-adult-websites-australia-law

[11] [11] Autoritatea franceză pentru protecția datelor a descris o dovadă de concept pentru un sistem de verificare a vârstei care să păstreze confidențialitatea. Cu toate acestea, sistemul nu este în prezent funcțional și nici nu rezolvă multe dintre problemele ridicate în acest document, cum ar fi excluderea structurală sau necesitatea legală. Disponibil la: https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process

[12] https://www.biometricupdate.com/202305/universal-global-digital-identity-still-7-years-away-oix-presenter

Cu toate acestea, aceste metode de estimare pot fi inexacte, discriminatorii și profund invazive. Cei care - cum ar fi Yoti, o companie de "asigurare a vârstei" cu sediul în Marea Britanie - pretind, de exemplu, că sunt conforme cu GDPR deoarece nu prelucrează datele biometrice în scopul identificării (ceea ce înseamnă că utilizează scanarea feței utilizatorului doar pentru a estima vârsta acestuia, nu pentru a-l identifica sau recunoaște). Considerăm că această afirmație este înșelătoare, deoarece instrumentele utilizate au în mod clar capacitatea de a identifica persoana.

Practicile de estimare a vârstei pot constitui, de asemenea, o profilare automată interzisă în temeiul articolului 22 din GDPR. Articolul 22 din GDPR prevede o excepție pentru crearea de profiluri pe baza consimțământului explicit [articolul 22 alineatul (2) litera (c)]. Cu toate acestea, este discutabil dacă copiii care utilizează astfel de metode își dau cu adevărat consimțământul, având în vedere lipsa de conștientizare a consecințelor potențiale ale acestei prelucrări. Există, de asemenea, faptul că este posibil ca consimțământul lor să nu fie dat în mod liber, deoarece, în practică, acesta este necesar pentru ca ei să acceseze platforme online, cum ar fi serviciile de mesagerie sau rețelele sociale.

Capitolul 3. Analiza metodelor cheie

3.1. Prezentare generală și tabel de sinteză

În ceea ce privește robustețea măsurilor de **verificare a vârstei, se** poate presupune că numai metodele de **verificare a vârstei bazate pe documente** au un nivel de acuratețe rezonabil de ridicat - deși, chiar și în acest caz, acest lucru poate fi eludat prin utilizarea documentelor altcuiva. De asemenea, aceste metode pot fi foarte invazive și prezintă riscuri semnificative. Există, de asemenea, o problemă de ordin practic: în cadrul acestei cercetări, nu am găsit nicio metodă de verificare bazată pe documente, actuală sau previzibilă în mod rezonabil, care să fie disponibilă în întreaga UE și care să îndeplinească cerințele privind drepturile omului. Autoritatea franceză pentru protecția datelor, CNIL, a constatat că, deși este teoretic posibil să se creeze un sistem de verificare a vârstei cu pseudonim, acesta nu există în prezent.[13] Orice soluție previzibilă ar putea fi, de asemenea, eludată de un VPN, adaugă cercetătorii.[14]

Declararea vârstei este mai ușor de falsificat, dar, în general, prezintă mult mai puține riscuri atât pentru utilizatorii copii, cât și pentru cei adulți. După cum subliniază autoritatea franceză, CNIL, completarea declarației de vârstă cu un design adecvat vârstei, precum și cu măsuri non-tehnice - de exemplu, supravegherea părinților - poate face ca metodele de declarare a vârstei să fie adecvate în multe cazuri.[15] Acest fapt a fost, de asemenea, subliniat în avizul Comisiei pentru piețe interne a Parlamentului European privind Regulamentul CSA (considerentul 16b).

Metodele de **estimare a vârstei,** în general, nu par a fi suficient de precise, având adesea o marjă de eroare de câțiva ani, în special în cazul persoanelor de culoare. Acestea sunt foarte intruzive și încurajează colectarea în masă a datelor cu caracter personal și crearea de profiluri pe scară largă. Metodele de recunoaștere facială pot fi, de asemenea, ușor de eludat prin utilizarea unui prieten sau a unei rude pentru înscriere. Această problemă ar putea fi evitată prin solicitarea de verificări de fiecare dată când o persoană se conectează, dar acest lucru ar stimula prelucrarea de rutină a datelor sensibile și ar putea chiar stimula crearea unor baze de date biometrice de bază ale copiilor - ceea ce ar reprezenta un risc clar inacceptabil.

Prin urmare, ceea ce speră cel mai mult să sublinieze această secțiune este faptul că **nu există o soluție perfectă pentru verificarea vârstei.** În plus, **există de obicei un compromis între invazitate și risc, pe de o parte, și eficacitate, pe de altă parte.** Este posibil ca măsurile cele mai eficiente din punct de vedere teoretic să nu reușească să atingă pragul necesar pentru a proteja datele sensibile ale tinerilor și să prezinte riscuri mai largi de excludere și supraveghere. Este posibil ca metodele care respectă drepturile să nu ofere suficientă încredere în rezultatele lor decât dacă sunt completate cu alte măsuri (adesea non-tehnice). **Aceasta este o problemă nerezolvată în prezent atât pentru furnizori, cât și pentru legiuitori.**

De asemenea, este posibil ca factorii de decizie să se concentreze prea mult asupra verificării vârstei și să supraestimeze beneficiile presupuse ale acesteia. De exemplu, după cum subliniază grupul pentru drepturile digitale ale copiilor 5 Rights Foundation, "o atenuare eficientă a riscurilor poate,

[13] https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process
[14] https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety
[15] https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety

dimpotrivă, să anuleze nevoia de verificare a vârstei".[16] Prin descurajarea nevoii copiilor de a furniza o vârstă falsă prin îmbunătățirea serviciilor și o supraveghere adecvată din partea părinților, măsurile de verificare a vârstei potențial dăunătoare, cum ar fi verificarea pe bază de documente, ar putea să nu fie necesare.

Tabelul următor compară metodele de verificare a vârstei în timpul înscrierii la serviciile și platformele online pe o bază generală (adică așa cum este propus de Regulamentul CSA al UE) și nu pentru un serviciu specific (de exemplu, jocurile de noroc). Criteriile în funcție de care am evaluat categoriile și metodele sunt următoarele:

- **Invazitate** = necesită (sau chiar impun) o mare cantitate de colectare și prelucrare a datelor, în special a datelor sensibile, și le tratează în moduri care ar putea dăuna utilizatorului?
- **Eficacitate** = evaluează cu precizie și corectitudine vârsta persoanei în contextul platformelor și serviciilor online? Este ușor de eludat/înșelat? Poate fi accesat/utilizat de către toți cei care ar trebui să poată accesa serviciile și platformele digitale?
- **Nivelul de risc** = ce risc prezintă pentru drepturile și libertățile fundamentale ale tuturor utilizatorilor de internet, în special ale copiilor? Riscă să excludă persoane (care au depășit vârsta necesară), de exemplu, pentru că nu pot îndeplini cerințele de verificare a vârstei (acces la eID sau la documente de identitate fizice) sau pentru că nu doresc să facă acest lucru din cauza pierderii anonimatului online sau a altor efecte negative?

Vă rugăm să rețineți că, deși acest tabel sintetizează unsprezece metode de verificare a vârstei pe care le-am identificat și clasificat în trei categorii generale, nu este exhaustiv. Acesta este menit să reprezinte cele mai comune metode.

Metoda	Invazitate	Eficacitate	Nivelul de risc	Concluzie
Declarația de vârstă				
1: Declarație implicită prin intermediul termenilor și condițiilor	Scăzut	Scăzut	Scăzut	Utilitate limitată
2: Declarație pe proprie răspundere că depășește un anumit prag de vârstă	Scăzut	De la scăzut la mediu	Scăzut	Promițătoare, dar trebuie să fie susținută de alte măsuri
3: Declarație pe propria răspundere privind data nașterii	Scăzut	De la scăzut la mediu	De la scăzut la mediu	Metoda 2 este preferabilă
4. Garanția socială	Scăzut spre mediu	Scăzut	De la scăzut la mediu	Nu recomandăm

[16] Contribuția Fundației 5Rights la consultarea Comisiei Europene cu privire la Regulamentul privind abuzul sexual asupra copiilor: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse

Verificarea vârstei pe bază de documente				
Metoda	**Invazitate**	**Eficacitate**	**Nivelul de risc**	**Concluzie**
5: Încărcarea documentelor oficiale către furnizor sau către o terță parte	Foarte mare	Mediu	Foarte mare	Nu recomandam
6: Utilizarea documentelor oficiale pentru a crea un token (de către furnizor sau de către o terță parte)	Mare	Mediu	De la mare la foarte mare	Nu se recomandă. Sunt necesare cercetări suplimentare.
7. Utilizarea unei intermediar pentru documente oficiale (de exemplu, card de student, card de credit/debit)	Medie spre ridicată	Scăzută	De la scăzut la mediu	Nu recomandam
8: Utilizarea sistemului național sau internațional de identificare digitală (eID) pentru a crea un token.	De la scăzut la ridicat, în funcție de arhitectură	Mare în teorie; scăzut în curent și forme previzibile	Mare	Nu se recomandă. Sunt necesare cercetări suplimentare

Estimarea vârstei				
9: Folosirea analizei facială sau alt sistem de inteligență artificială pentru a prezice vârsta utilizatorului	Foarte mare	Scăzut mediu	Foarte mare	Nu se recomandă.
10: Utilizarea altor date pentru a prezice vârsta utilizatorului	Foarte mare	Scăzut mediu	Foarte mare	Nu se recomandă.
11: Solicitarea ca utilizatorii să îndeplinească o sarcină sau o activitate pentru a-și "dovedi" vârsta	Scăzut	Scăzut	Mare	Nu se recomandă.

3.2. Categoria: Declarația de vârstă

Aceste metode sunt atractive, deoarece sunt simple, în mare parte neinvazive și ușor de aplicat de către furnizori pentru a îndeplini cerințele lor de a proteja în mod specific datele utilizatorilor cu vârste cuprinse între 13 și 16 ani și de a preveni abonarea de către persoanele sub 13 ani (articolul 8 din GDPR). Excepție face metoda 4, care creează o dependență față de alte persoane care ar putea lipsi de putere utilizatorul care solicită verificarea vârstei.

Metoda 1 nu este suficient de robustă în sine, iar metodele 2 și 3 pot necesita măsuri suplimentare de proiectare sau de supraveghere. Prin urmare, acestea nu sunt de sine stătătoare, ci necesită o abordare mai holistică a siguranței online, care să se concentreze, de asemenea, pe proiectare și supraveghere - în caz contrar, copiii pot fi stimulați să introducă o vârstă falsă. După cum s-a discutat în secțiunea 1.1, cu astfel de adăugiri, metoda 2 de declarare a vârstei este probabil adecvată pentru majoritatea cazurilor generale de utilizare a verificării online a vârstei. Notă: din punctul de vedere al protecției datelor, este mai puțin riscant

pentru furnizor să ceară utilizatorului să aleagă o categorie de vârstă (adică metoda 2), decât să furnizeze informații specifice despre data nașterii (metoda 3). Cu toate acestea, niciuna dintre metode nu conține vreo modalitate de validare a informațiilor.

Metoda 1: Declarație implicită prin descrierea restricțiilor de vârstă în termenii serviciului sau în liniile directoare ale comunității.

Pro	Contra	Riscuri
Simplu	Pasiv și, prin urmare, ușor de ignorat sau de trecut cu vederea	Niciuna semnificativă
	Este puțin probabil să îndeplinească cerințele articolului 8 din GDPR de unul singur (ar trebui să fie combinat cu o altă metodă).	

Metoda 2: Declarație pe proprie răspundere că am depășit un anumit prag de vârstă (de exemplu, am "peste 13 ani", "peste 16 ani" sau "peste 18 ani").

Pro	Contra	Riscuri
Ieftin de aplicat	Declarațiile false ar putea crea probleme legate de acuratețea datelor, ceea ce ar putea fi o problemă pentru articolul 5 din GDPR (datele cu caracter personal trebuie să fie exacte) și legalitatea prelucrării (consimțământul nu este valabil dacă este dat de un copil cu vârsta sub vârsta de consimțământ)	
Simplu	Dificil de prevenit declarațiile false	publicitate personalizată
Nu este invazivă		
În general, se înțelege că acestea permit furnizorilor să își îndeplinească obligațiile care le revin în temeiul articolului 8 din GDPR (date privind copiii), deși se pot baza pe alte mecanisme, cum ar fi proiectarea adecvată vârstei și supravegherea părinților.		
Compatibil cu articolul 5.1 litera (c) din GDPR (minimizarea datelor)		
Permite utilizatorilor să rămână anonimi, ceea ce este important pentru a beneficia de o gamă largă de drepturi ale omului online.		

Metoda 3: Declarație pe propria răspundere privind data nașterii

Pro	Contra	Riscuri
Simplu	Dificil de prevenit declarațiile false	Furnizorul ar putea prelucra în mod inutil data nașterii
Ieftin de aplicat	Ar putea crea probleme în ceea ce privește articolul 5.1 litera (c) din GDPR (minimizarea datelor).	Furnizorul ar putea folosi aceste informații pentru a personaliza publicitatea sau pentru a le vinde unei terțe părți
Nu foarte invaziv	Declarațiile false ar putea crea probleme legate de acuratețea datelor, ceea ce ar putea constitui o problemă pentru GDPR (a se vedea metoda 2).	
Permite utilizatorilor să rămână anonimi, ceea ce este important pentru a beneficia de o gamă largă de drepturi ale omului online.		
Este probabil să îndeplinească cerința articolului 8 din GDPR (date privind copiii)		

Metoda 4: Garantarea socială (solicitând altor utilizatori să confirme dacă o persoană are mai puțin sau mai mult de 18 ani)

Pro	Contra	Riscuri
	Se bazează pe faptul că oamenii au legături cu prieteni sau rude care îi cunosc în viața reală și sunt activi pe platformă sau serviciu	Face ca utilizarea internetului de către oameni dependenți de alții, ceea ce poate aduce atingere demnității și autonomiei lor
	Poate dura mult timp pentru a obține un răspuns	
	Erorile ar putea crea probleme de acuratețe a datelor, ceea ce ar putea fi o problemă pentru articolul 5 din GDPR și legalitatea prelucrării (dacă copilul nu are vârsta de consimțământ, numai părinții sau tutorii pot da un consimțământ valabil pentru prelucrarea datelor cu caracter personal ale copilului).	

3.3. Categoria: Verificarea vârstei pe bază de documente

Deoarece metodele de verificare a vârstei bazate pe documente se bazează pe o anumită formă de document de identitate, acestea necesită declararea de informații sensibile unui furnizor sau unei terțe părți (care ar putea fi un guvern sau o entitate comercială precum Yoti) ca un element esențial (pentru toate metodele). Acest lucru creează riscuri inerente, atât în ceea ce privește utilizarea deliberată a datelor în scopuri de supraveghere sau publicitate, cât și riscurile ca datele să fie furate, divulgate către terți sau exploatate

pentru furt de identitate și fraudă. Având în vedere că o mare parte din activitatea EDRi din ultimii ani a fost concentrată asupra încălcărilor sistemice ale datelor oamenilor de către furnizorii online, precum și de către guverne, avem motive întemeiate pentru a fi precauți în privința acestor sisteme.

Există, de asemenea, un risc de excludere pe baza naționalității sau a altor caracteristici. Acest lucru se datorează faptului că unele țări nu dispun de sisteme naționale de identitate digitală și chiar și țările care dispun de astfel de sisteme nu au o acoperire uniformă (în general, pașapoartele sunt necesare doar pentru călătoriile internaționale în afara UE). Este o problemă în special având în vedere faptul că principala necesitate în acest caz este de a separa copiii de adulți: în unele state membre, actele de identitate naționale sunt destinate doar persoanelor de peste 16 sau 18 ani, ceea ce înseamnă că cerința articolului 8, de a distinge copiii cu vârste cuprinse între 13 și 16 ani, ar putea fi greu de îndeplinit. Există, de asemenea, faptul că persoanele fără documente și comunitățile care se confruntă cu niveluri ridicate de discriminare structurală, cum ar fi roma și sinti, pot să nu aibă acces la niciun document de identitate, ceea ce le exclude de la serviciile digitale. Utilizarea de documente intermediare (metoda 7), cum ar fi cardurile de credit sau cardurile de student, este ineficientă și nu rezolvă problema excluderii.

Teoretic, este posibil ca un viitor sistem de identitate digitală (metoda 8), care să fie disponibil pe scară largă, care să poată verifica vârsta într-un mod cu adevărat anonim și permanent nedetectabil și care să respecte pe deplin viața privată și protecția datelor, să poată fi utilizat pe scară largă. Cu toate acestea, o astfel de infrastructură nu este confirmată în prezent, nici măcar pentru portofelul de identitate digitală al UE, care ar putea sau nu să adere la aceste standarde, în funcție de acordul final al trialogului instituțiilor europene. De asemenea, nu ar aborda problema excluderii structurale a celor care nu au documente de identitate, care reprezintă un risc grav pentru aceste persoane.

Pentru a fi acceptabil, un sistem de verificare a vârstei ar trebui să:

- *Împiedice permanent orice legătură între activitatea sau istoricul de internet și identitatea persoanei sau cu profiluri anonime sau pseudonime, asigurând că o persoană nu poate fi urmărită (adică "zero cunoștințe");*
- *Să nu furnizeze nicio informație furnizorului, în afară de un da/nu, și să nu faciliteze accesul furnizorului sau al unui părinte, tutore sau alt actor;*
- *Asigurarea faptului că utilizarea anonimă a internetului în general poate continua;*
- *Utilizarea de token-uri în loc de a stoca date cu caracter personal și ștergerea imediată a datelor cu caracter personal prelucrate în scopul generării token-ului;*
- *Să nu permită ca datele colectate sau prelucrate să fie utilizate în orice alt scop;*
- *Să nu permită prelucrarea datelor biometrice sau a datelor bazate pe date biometrice;*
- *Să se abțină de la a solicita sau de la a încuraja toți (tinerii) să aibă un act de identitate digital, asigurându-se că oamenii își păstrează dreptul la un act de identitate analogic;*
- *Să fie robust și sigur din punct de vedere al securității cibernetice;*
- *Să fie consensual și să nu fie prea împovărător pentru cei care nu doresc sau nu au mijloacele necesare pentru a-și verifica identitatea în acest mod;*
- *Să se utilizeze numai atunci când este strict necesar;*
- *Să fie atent la potențialul efect de descurajare, în special că accesul la materiale educaționale și de sănătate (inclusiv de sănătate reproductivă) nu este supus verificării vârstei, ceea ce ar putea avea un efect de descurajare asupra faptului dacă copiii se simt sau nu confortabil să acceseze aceste informații.*

Metoda 5: Încărcarea unei scanări sau a unei fotografii a pașaportului, a cărții de identitate naționale sau a unui alt document oficial care să ateste vârsta furnizorului sau a unei terțe părți

Pro	Contra	Riscuri
Permite furnizorului să verifice data de naștere auto declarată a utilizatorului în raport cu un document de identitate oficial. Acest lucru înseamnă că eludarea și falsificarea sunt mai dificile, deoarece necesită modificări ale copiei digitale. Pe de altă parte, cu excepția cazului în care cerința de verificare este globală,	Foarte invaziv, mai ales dacă furnizorul verifică documentul în raport cu alte părți ale contului	Discriminarea celor care nu au un document de identitate, în special a celor care se confruntă deja cu un nivel ridicat de discriminare structurală (persoane fără documente, solicitanți de azil, comunități de roma și sinti - inclusiv copii din toate aceste comunități),
întregul proces de verificare poate fi eludat cu ajutorul unui VPN.		ceea ce duce la o exacerbare a excluziunii sociale
În teorie, se bazează pe un document validat oficial, astfel încât vârsta ar trebui să fie exactă.	Nu toată lumea are documente de iden anumitor comunități la un risc ridicat	risc, de exemplu, lucrătorii din industria sexului, care s-au dovedit a fi supuși unui risc mai mare de exploatare prin aceste măsuri.
	Necesită ca utilizatorul să aibă încredere într-un entitate privată/comercială cu documentul de identitate al acesteia	Îngreunarea anonimatului online, inclusiv pentru persoanele a căror siguranță depinde de acest lucru. (jurnaliști, denunțători, persoane care au fost supuse hărțuirii sau abuzurilor online)
	pune toate aceste date sensibile în mâinile Big Tech, opusul a ceea ce legi precum DSA încearcă să realizeze.	Crearea posibilității de a urmări utilizarea internetului de către fiecare persoană și de a o lega de identitatea juridică a acesteia, ceea ce creează condiții pentru supravegherea și păstrarea datelor
	Întrucât unele țări nu furnizează în prezent documente de identitate copiilor de toate vârstele relevante, acest lucru ar împiedica granularitatea (de exemplu, această metodă ar putea fi utilizată numai pentru serviciile transfrontaliere pentru a dovedi că un utilizator are peste 18 ani). De asemenea, ar putea motiva țările să elibereze documente de identitate pentru copii.	Risc ridicat de utilizare abuzivă a datelor foarte sensibile în scopuri publicitare sau de vânzare către terți
	Trebuie să fie verificată individual, deci necesită foarte multe resurse (cu excepția cazului în care se utilizează inteligența artificială, ceea ce creează propriile probleme de (in)acuratețe și un risc de profilare automată).	Păstrarea unui număr atât de mare de date sensibile într-un singur loc poate stimula hackerii. În cazul în care sunt piratate, acest lucru poate crea riscuri de fraudă de identitate.
	Fiecare persoană trebuie să se identifice pentru a utiliza platforma/serviciul, ceea ce poate fi descurajează unele persoane	

	Este foarte puțin probabil să fie compatibil cu articolul 5.1 litera (c) din GDPR (minimizarea datelor), deoarece solicită în mod sistematic schimbul de date inutile. Ar fi necesar doar să se știe dacă utilizatorul este peste sau sub un prag de vârstă, dar acesta trebuie să furnizeze o mulțime de informații sensibile despre el însuși.	
	Scanările/încărcările pot fi falsificate sau alterate digital	
	Normalizează nevoia de a avea un document de identitate pentru a participa la viața de zi cu zi	

Metoda 6: Încărcarea unei scanări sau fotografii sau realizarea unei capturi video a unui pașaport, a unui document național de identitate sau a unui alt document oficial de identitate către o terță parte, care furnizează apoi un token furnizorului pentru a confirma categoria de vârstă a utilizatorului (de exemplu, "peste 13 ani" sau "peste 18 ani").

Pro	**Contra**	**Riscuri**
Relativ dificil de eludat/înșelat (aceeaș metodă ca și metoda 5). Pe de altă parte, cu excepția cazului în care cerința de verificare este globală, întregul proces de verificare poate fi eludat cu ajutorul unui VPN.	Este posibil ca tinerii să folosească token-urile celorlalți sau să folosească un ID-ul părintelui/rudei pentru a crea un token, reducând eficiența	Discriminarea celor care nu au un document de identitate, în special a celor care se confruntă deja cu un nivel ridicat de discriminare structurală (persoanele fără documente, solicitanții de azil, comunitățile de romi și sinti - inclusiv copiii din toate aceste comunități), ceea ce ar putea duce la o exacerbare a discriminării sociale.

Token-ul face mai puțin probabil ca activitatea pe internet să fie legată de identitatea juridică	Relativ invaziv (deși arhitectura exactă a sistemului are posibilitatea de a minimiza acest lucru)	Îngreunarea condițiilor de anonimat online, inclusiv pentru persoanele a căror siguranță depinde de acest lucru. (jurnaliști, denunțători, persoane care au fost supuse hărțuirii sau abuzurilor online, lucrători sexuali etc.).
În cazul în care jetoanele sunt emise ca fiind de unică folosință pentru fiecare platformă online, jetoanele nu pot fi utilizate pentru a urmări utilizatorii pe mai multe platforme.	Se bazează pe încrederea în partea terță, adesea pe promisiuni mai degrabă decât pe transparență și posibilitatea de verificare..	Crearea posibilității de a urmări utilizarea internetului de către fiecare persoană și de a o lega de identitatea juridică a acesteia, ceea ce creează condiții pentru supravegherea și păstrarea datelor
	Nu toată lumea are documente de identitate	Posibilul risc de utilizare abuzivă a datelor foarte sensibile în scopuri publicitare sau de vânzare către terți

	Necesită ca utilizatorul să aibă încredere într-o entitate privată/comercială cu documentul de identitate al acesteia	În cazul în care datele sunt stocate, păstrarea unui număr mare de date sensibile într-un singur loc poate stimula hackerii. În cazul în care sunt piratate, acest lucru poate crea riscuri de fraudă de identitate.
	Deoarece unele țări nu furnizează în prezent documente de identitate copiilor de toate vârstele relevante, acest lucru ar împiedica granularitatea (de exemplu, această metodă ar putea fi utilizată numai pentru serviciile transfrontaliere pentru a dovedi că un utilizator are peste 18 ani).	Unele implementări ale acestuia au fost combinate cu biometrie. Sisteme de identificare sau de verificare, încurajând adoptarea sistemelor biometrice
	Costisitoare pentru furnizori, ceea ce poate descuraja adoptarea (și poate fi imposibil pentru furnizorii mici sau cu sursă deschisă)	
	Fiecare persoană trebuie să aibă și să fie dispusă să își împărtășească identitatea legală pentru a utiliza platforma/serviciul.	Cercetătorii au arătat că astfel de metode sunt foarte vulnerabile la probleme de securitate[17]
	Pune toate aceste date sensibile în mâinile unor companii private. Aceasta nu este independentă și va fi stimulată de profit.	
	Riscul de incompatibilitate cu articolul 5.1 litera (c) din GDPR (minimizarea datelor)	
	Dacă nu există o alternativă, ar putea încălca cerința de consimțământ în conformitate cu GDPR (dacă acesta este temeiul pe care furnizorul a ales să îl folosească).	
	Scanările/încărcările pot fi falsificate sau alterate digital	
	Normalizează nevoia de a avea un document de identitate pentru a participa la viața de zi cu zi	

Metoda 7: Utilizarea unui proxy (document intermediar) pentru documente oficiale (de exemplu, card de student, card de credit/debit)

Pro	Contra	Riscuri
	Ușor de falsificat	Creează condiții în care cei care pot utiliza această metodă sunt aleși în cel mai bun caz în mod arbitrar, iar în cel mai rău caz în mod discriminatoriu.

[17] https://www.golem.de/news/manipulierte-ausweise-ccc-macht-videoident-kaputt-2208-167530.html

	Diferitele țări permit emiterea de carduri de credit sau de debit la vârste diferite, deci nu oferă o soluție la nivelul UE	
	Privilegiază pe cei care au un anumit nivel de educație sau situații financiare	
	Riscul de incompatibilitate cu articolul 5.1 litera (c) din GDPR (minimizare) în funcție de documentația aleasă, deoarece aceasta poate dezvălui informații sensibile suplimentare despre persoana respectivă.	

Metoda 8: Utilizarea unui sistem național sau internațional de identitate digitală/identitate electronică, care furnizează apoi un token furnizorului pentru a confirma vârsta utilizatorului.

Pro	**Contra**	**Riscuri**
În teorie, dificil de ocolit/înșelat. Cu toate acestea, cercetătorii cibernetici au deja a demonstrat riscul de furt de identitate și de fraudă prin aceste metode (a se vedea coloana "Riscuri").	În prezent, nu este disponibil în mod uniform (adică nu în toate țările), deci nu poate funcționa ca o soluție la nivelul UE, ci doar ca o soluție națională.	Discriminarea celor care nu au un document de identitate (care este o condiție prealabilă pentru a avea acces la o identitate electronică), în special pentru cei care se confruntă deja cu un nivel ridicat de discriminare structurală. (persoane fără acte, solicitanți de azil, comunități de romi și sinti - inclusiv copii din toate aceste comunități), ceea ce duce la o exacerbarea excluziunii sociale
Teoretic, nu face legătura între activitatea pe internet și identitatea juridică (deși viitorul portofel de identitate digitală (eID) al UE ar putea permite utilizatorilor să fie de anonimizat)	Acolo unde sunt disponibile, pot avea probleme de securitate, deoarece tehnologiile nu sunt întotdeauna mature sau fiabile.	Discriminarea pe bază de naționalitate (de exemplu, doar persoanele din anumite țări ar avea acces).
Planuri pentru o identitate electronică la nivelul UE care să fie operațională abia la sfârșitul anilor 2020 (în prezent, UE speră ca până în 2030 să fie adoptată în proporție de 80 %).	Creează posibilitatea ca guvernul să urmărească toate utilizările internetului; se bazează pe faptul că se poate avea încredere că guvernul nu va supraveghea activitatea pe internet (ceea ce reprezintă în prezent un risc real pentru "soluția" la nivelul UE).	Să facă foarte dificilă păstrarea anonimatului online, inclusiv pentru persoanele a căror siguranță depinde de acest lucru (jurnaliști, denunțători, persoane care au fost supuse hărțuirii sau abuzurilor online, lucrători sexuali etc.).
	Se bazează pe faptul că identitatea electronică nu trebuie să fie cunoscută și nu trebuie să fie urmărită, ceea ce nu este cazul în prezent pentru identitatea electronică la nivelul UE.	Crearea posibilității de a urmări utilizarea internetului de către fiecare persoană și de a face legătura cu identitatea juridică a acesteia, ceea ce creează condiții pentru supravegherea și păstrarea datelor
	Dacă nu există o alternativă, ar putea încălca cerința de consimțământ în conformitate cu GDPR (dacă acesta este temeiul pe care furnizorul a ales să îl	Păstrarea unui număr atât de mare de date sensibile într-un singur loc poate stimula hackerii. În cazul în care sunt piratate, acest lucru poate crea

	folosească).	Riscuri de fraudă de identitate.
	Faptul că sunt deținute de guvern nu înseamnă că datele sunt neapărat sigure	Nu se preconizează că identitatea electronică la nivelul UE va avea niciodată o acoperire completă în întreaga UE, ceea ce înseamnă un risc continuu de excluziune digitală.
	Deoarece unele țări nu oferă în prezent eID copiilor, această metodă ar împiedica granularitatea (de exemplu, această metodă ar putea fi utilizată numai pentru serviciile transfrontaliere pentru a dovedi că un utilizator are peste 18 ani). În comunicarea BIK+ [COM(2022) 212 final], Comisia ia act de această limitare a eID-urilor pentru verificarea vârstei copiilor și afirmă că va colabora cu statele membre pentru a le determina să elibereze eID-uri pentru copii.	Cercetătorii au demonstrat că aceste sisteme îi pot face pe oameni vulnerabili la furtul de identitate și la furtul de date.[18]
	În cazul în care copiii trebuie să se bazeze pe identitatea electronică a părintelui sau tutorelui acest lucru ar putea expune la un risc și mai mare copiii ai căror părinți sau tutori controlează, abuzează sau exploatează, condiționând accesul lor la internet de un părinte/tutore abuziv.	
	Normalizează necesitatea de a avea un document de identitate digital pentru a participa la viața de zi cu zi și poate crea un efect de disuasiune pentru anonimitate.	

3.4. Categoria: Estimarea vârstei

Evaluarea metodelor de estimare a vârstei:

Metodele de estimare a vârstei (9 și 10) sunt profund problematice prin esența lor, deoarece se bazează pe existența unei cantități suficiente de date despre utilizator pentru a face estimarea. În contextul mai larg al capitalismului de supraveghere și având în vedere că Regulamentul UE privind serviciile digitale interzice furnizorilor să direcționeze reclamele online către copii, măsurile de estimare a vârstei ar putea fi considerate incompatibile cu abordarea UE privind protecția copiilor online.

De asemenea, nu există doar riscul de a crea stereotipuri dăunătoare pentru oameni, ci și de a forța un furnizor să definească ceea ce ar putea considera a fi un comportament "acceptabil" sau "normal" pentru copii și adolescenți în comparație cu adulții. Aceasta este o chestiune sociologică complexă și nu una care poate fi ușor de transpus într-un instrument tehnologic. Metoda 11, de exemplu, prezintă, de asemenea, un potențial extrem de discriminatoriu față de persoanele cu dizabilități și persoanele neurodivergente.

[18] https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du musst-dich-ausweisen-829293739fa0

În plus, metodele de estimare a vârstei se bazează în mod intrinsec pe predicții, mai degrabă decât pe certitudine, ceea ce poate crea probleme în ceea ce privește acuratețea datelor, precum și modul de abordare a nivelului inevitabil ridicat de utilizatori care vor fi estimați ca fiind mai în vârstă decât sunt cu adevărat sau mai tineri decât sunt cu adevărat. Acest lucru ar putea însemna că adulților li s-ar putea permite să intre în spații presupuse a fi rezervate exclusiv copiilor sau că adulții sau adolescenții mai mari ar putea fi blocați în spații la care se presupune că pot avea acces. Faptul de a le pune sarcina de a corecta acest lucru poate, în sine, să suprime libertatea de exprimare a unor persoane.

Natura predictivă a acestor sisteme poate crea, de asemenea, o problemă în conformitate cu articolul 22 din GDPR, care ar trebui să oprească crearea de profiluri, cu excepția cazului în care există un consimțământ explicit - ceea ce, conform secțiunii 1.1 din acest briefing, este puțin probabil să fie cazul în acest caz. În plus, ideea ca societățile private să folosească fețele copiilor pentru a le face profilul în scopul de a decide dacă pot sau nu să acceseze un serviciu sau un spațiu este îngrijorătoare în contextul mai larg al abuzurilor de date biometrice atât de către entități private, cât și de stat.[19] Având în vedere că legea UE privind inteligența artificială (IA) este încă în curs de negociere la momentul publicării, practicile care utilizează IA pentru a crea profiluri sau a clasifica persoanele pe baza fețelor lor sau a altor părți sau caracteristici corporale ar putea fi restricționate în continuare sau chiar interzise în UE.

Metoda 9: Utilizarea analizei faciale sau a altor instrumente bazate pe inteligență artificială pentru a prezice vârsta persoanei

Pro	**Contra**	**Riscuri**
Nu necesită identitate legală, deci riscul de excludere este mai mic pentru cei care nu au documente de identitate.	Profund invaziv	Posibilitatea de a crea o situație sistemică discriminarea, deoarece instrumentele bazate pe inteligența artificială nu sunt fiabile în mod uniform și arată în mod repetat că nu sunt fiabile în cazul anumitor categorii demografice
Disponibil în întreaga UE	Recunoașterea facială sau alte predicții/estimări ale vârstei bazate pe inteligență artificială nu sunt suficient de fiabile pentru un context	Este probabil să nu reușească să răspundă copiilor care se apropie de un prag de vârstă, deoarece aceste sisteme sunt în cel mai bun caz precise cu o precizie de un
	în cazul în care este importantă determinarea exactă a vârstei. EDRi se opune de mult timp utilizării sistematice a datelor biometrice în astfel de scopuri, avertizând că astfel se creează infrastructura pentru supravegherea biometrică în masă. practici.	prag de 2-4 ani. Ar putea exclude copiii de la servicii sau informații, precum și adulții care par tineri.
	Necesită prelucrarea sistematică a datelor foarte sensibile ale tuturor utilizatorilor, inclusiv ale copiilor (și, prin urmare, este posibil să încalce și articolul 9 din GDPR).	Poate dezvălui alte informații sau caracteristici care ar putea fi folosite pentru a direcționa publicitatea sau în alte scopuri inacceptabile
	În special, este posibil să nu fie fiabil pentru persoanele de culoare, brune și asiatice, precum	Păstrarea unui număr atât de mare de date sensibile într-un singur loc poate stimula accesul

[19] https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

	și pentru persoanele cu anumite dizabilități	neautorizat. În cazul în care sunt piratate, acest lucru poate crea riscuri de fraudă de identitate.
	Ușor de falsificat/eludat prin prezentarea unei alte persoane	Riscul de a permite accesul copiilor minori în spații care nu le sunt destinate
	Indiferent dacă este vorba de furnizor sau de o terță parte, acesta este exact genul de colectare de date pe care DSA și AI Act ar trebui să le reducă la minimum.	Poate duce la o normalizare a verificărilor biometrice online (așa cum se întâmplă în China)[20] fără o înțelegere adecvată a riscurilor și consecințelor, de exemplu, supravegherea sau furtul de identitate.
	Poate încălca articolul 22 din GDPR (crearea de profiluri)	
	Erorile ar putea crea probleme legate de acuratețea datelor, ceea ce ar putea constitui o problemă pentru articolul 16 din GDPR (dreptul la rectificare).	

Metoda 10: Utilizarea altor date pentru a prezice sau verifica vârsta persoanei

Pro	**Contra**	**Riscuri**
Nu necesită identitate legală, deci riscul de excludere este mai mic pentru cei care nu au documente de identitate.	Se bazează pe profilurile de bază ale fiecărui utilizator	Stimulează colectarea, păstrarea și analiza în masă a datelor copiilor de către platforme
Disponibil în întreaga UE	Poate dezvălui informații foarte sensibile. EDRi a pledat pentru interzicerea categorisirii persoanelor pe baza unor caracteristici sensibile, inclusiv a vârstei, folosind datele lor biometrice, care a fost adoptată ca poziție a Parlamentului European în 2023.[21]	O mulțime de dovezi că aceste tipuri de profiluri sunt folosite pentru a manipula achizițiile oamenilor, pentru a-i exclude de la anumite locuri de muncă, pentru a-i radicaliza sau pentru a le influențează modul în care aceștia votează[22]
	Nu va funcționa pentru persoanele cu o amprentă de internet limitată sau care au setări de confidențialitate mai stricte	Stimulează crearea de profiluri pentru copii
	Bazat pe stereotipuri	Risc ridicat de discriminare
	Se știe că unii furnizori folosesc metode invazive pentru a verifica data de naștere declarată de utilizator, cum ar fi scanarea postărilor din social media și poate chiar a mesajelor private pentru felicitări de ziua de naștere.[23]	

[20] https://www.bbc.com/news/world-asia-china-50587098
[21] https://edri.org/our-work/european-parliament-draws-red-line-against-biometric-surveillance-society/
[22] https://edri.org/our-work/surveillance-based-advertising-an-industry-broken-by-design-and-by-default/
[23] https://www.theverge.com/2022/6/23/23179752/instagram-age-verification-ai-social-vouching-methods

	Se bazează pe definirea prealabilă a tipurilor de comportamente pe care platforma consideră că reprezintă un copil vs. un adult, care poate fi lipsit de context cultural sau de altă natură	

	Poate încălca articolul 22 din GDPR (crearea de profiluri) și articolul 5.1 litera (c) (minimizarea datelor).	
	Exact genul de colectare de date pe care DSA și AI Act ar trebui să le reducă la minimum.	
	Erorile ar putea crea probleme legate de acuratețea datelor, ceea ce ar putea constitui o problemă pentru articolul 16 din GDPR (dreptul la rectificare).	

Metoda 11: Bazată pe sarcini (Task-based)

Pro	**Contra**	**Riscuri**
Nu necesită identitate legală, deci riscul de excludere este mai mic pentru cei care nu au documente de identitate.	Nu există o măsură standard a sarcinilor pe care le poate face un copil sau un adult, astfel încât aceasta se va baza întotdeauna pe stereotipuri și presupuneri	Discriminarea și excluderea persoanelor cu probleme fizice și psihice, dizabilități intelectuale, precum și persoane neurodivergente
Potențial mai puțin invaziv - nu se referă la cine sunteți, cum arătați sau la preferințele dumneavoastră, ci mai degrabă la o sarcină specifică, unică.	Acest lucru poate fi ușor de evitat, de exemplu, întrebând un frate sau o soră mai mare sau căutând pe internet soluții pentru sarcina sau activitatea respectivă.	
Disponibil în întreaga UE	Marjă de eroare ridicată, ceea ce este important atunci când scopul acestor sisteme este de a evalua vârsta	
	Această acuratețe scăzută ar putea crea probleme în temeiul articolului 16 din GDPR (dreptul la rectificare).	

Capitolul 4. Principalele riscuri legate de drepturile omului

4.1. Încălcarea drepturilor copiilor la viață privată și la protecția datelor

Marea majoritate a metodelor discutate mai sus, în special metodele de estimare a vârstei și metodele de verificare a vârstei pe bază de documente, se bazează pe - și chiar încurajează - colectarea, prelucrarea și, în unele cazuri, păstrarea pe scară largă a datelor copiilor și adulților deopotrivă. Întrucât copiii sunt principala țintă a acestor instrumente, acest lucru poate constitui o încălcare gravă a dreptului la viață privată și la protecția datelor personale atât pentru copii, cât și pentru adulți. Utilizarea datelor biometrice în acest scop, indiferent dacă acestea identifică sau nu în mod unic persoanele, nu poate fi niciodată considerată necesară, având în vedere caracterul sensibil al acestor date.[24]

În combinație cu metode precum analiza facială (metoda 9), acest lucru poate însemna prelucrarea sistematică și crearea de profiluri ale celor mai sensibile date ale copiilor. Având în vedere sensibilitatea datelor biometrice și a datelor bazate pe biometrie (acest din *urmă termen fiind utilizat din ce în ce mai mult pentru a acoperi sisteme cu riscuri echivalente în materie de drepturi ale omului, dar fără a identifica în mod unic persoanele vizate*), aceste metode ar trebui să fie considerate ca fiind inutil de intruzive și profund inadecvate pentru utilizarea de rutină de către copii.

În ciuda afirmațiilor contrare ale furnizorilor, multe sisteme de verificare a vârstei sunt susceptibile de a încălca GDPR, în special articolul 5.1 litera (c) (minimizarea datelor), articolul 9 (protecția datelor biometrice) și articolul 22 (protecția împotriva creării automate de profiluri). Având în vedere vulnerabilitățile specifice ale copiilor și faptul că aceștia au dreptul necesar de a explora și de a se exprima atât online, cât și offline, datele lor sunt de obicei înțelese ca necesitând garanții și mai mari decât cele ale utilizatorilor adulți (deși merită remarcat faptul că aceste metode încalcă, de asemenea, drepturile la confidențialitate și la protecția datelor ale adulților).

Ca atare, am considera (cel puțin) metodele 5 (verificarea pe bază de documente), 9 și 10 (ambele estimări) ca fiind inacceptabile în ceea ce privește protecția datelor și a vieții private a copiilor, indiferent de măsurile de protecție care ar putea fi puse în aplicare. Alte metode, cum ar fi 6 și 8 (ambele verificare pe bază de documente), sunt încă foarte riscante, dar - după cum s-a explicat mai sus - ar putea avea potențialul de a fi făcute conforme cu drepturile copiilor la protecția vieții private și a datelor în viitor. Acesta este motivul pentru care metode precum 2 și 3 (metode de declarare a vârstei) pot fi considerate deja ca având mai multe șanse de a respecta cerințele de protecție a vieții private și a datelor copiilor. Cu toate acestea, dacă nu sunt combinate cu alte măsuri de reducere a riscului de inexactitate a datelor, ele pot încălca cerința de acuratețe prevăzută la articolul 5.1 litera (d) din GDPR și cerința de a demonstra că și consimțământul utilizatorului este valabil (articolul 7).

În cazul în care furnizorii folosesc consimțământul ca bază pentru a efectua verificarea vârstei, aceștia vor trebui să se asigure că persoana este informată în mod corespunzător și că are o opțiune reală de a refuza. Cu toate acestea, având în vedere caracterul central al rețelelor de socializare și al aplicațiilor de mesagerie în viața multor copii din întreaga lume, este discutabil dacă aceștia pot

[24] https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

refuza cu adevărat măsurile care le sunt oferite.

În plus, poate fi dificil pentru un copil să înțeleagă pe deplin ceea ce își dă consimțământul. Chiar și pentru adulți, riscurile legate de prelucrarea datelor biometrice sau problemele de profilare și manipulare de către platformele Big Tech, nu sunt foarte cunoscute. Este discutabil dacă ne putem aștepta ca un copil - în special un copil mai mic - să cunoască potențialele consecințe ale accesului la astfel de date.

4.2. Încălcarea autonomiei și a exprimării de sine a copiilor pe internet

Prin plasarea unor bariere de verificare a vârstei în calea accesului online al copiilor, aceștia pot fi împiedicați să acceseze anumite conținuturi sau servicii pe care ar trebui să le poată accesa. Sau ar putea fi făcuți să se simtă "răi" sau "ciudați" pentru că accesează conținut sau servicii care sunt legitime - și poate chiar necesare pentru a se exprima și a avea acces la informații. Acest lucru ar putea avea un impact deosebit asupra conținutului legat de educația sexuală și sexuală, a informațiilor privind sănătatea sexuală și a asistenței medicale în materie de reproducere, care pot fi foarte importante pentru copii, dar care nu sunt întotdeauna susținute de părinți sau de culturi mai largi.

În unele țări, accesul la astfel de informații este chiar incriminat, iar orice măsură care ar putea dezvălui că un tânăr a accesat acest conținut îl poate pune în pericol. Deoarece internetul este global, măsurile care sunt introduse în UE, de exemplu, ar putea fi impuse în alte jurisdicții, unde copiii ar putea fi grav afectați de aceste măsuri. Chiar și acolo unde sunt sprijiniți, copiii ar putea dori (pe bună dreptate) să păstreze acest acces confidențial.

Există o problemă legată de faptul că termenul "copii" ca bloc omogen nu este util. Cu toate că, în conformitate cu legislația internațională privind drepturile copilului, un copil este orice persoană sub 18 ani, există o diferență clară între ceea ce ar fi adecvat pentru un copil de opt ani, față de un copil de doisprezece ani, comparativ cu un copil de șaisprezece sau șaptesprezece ani. GDPR are protecții speciale pentru copiii de toate vârstele, permițând în același timp copiilor de peste 13-16 ani (în funcție de statul membru) să își dea singuri consimțământul, în conformitate cu autonomia în creștere a copiilor mai mari. În toate statele membre ale UE, vârsta consimțământului sexual variază între 13 și 17 ani. Prin urmare, unele activități online care ar putea fi perfect legale pentru un copil de 14 ani într-o țară din UE ar fi ilegale pentru un copil de aceeași vârstă într-o altă țară din UE, însă sistemele de estimare a vârstei i-ar considera în continuare pe amândoi ca fiind copii. Acesta este un nivel de granularitate și nuanță care este foarte greu de evaluat de către furnizori fără a avea acces la o cantitate mult mai mare de date despre țara de reședință a copiilor - ceea ce creează și mai multe riscuri.

Există, de asemenea, o problemă mai amplă, și anume că măsurile de verificare a vârstei trebuie să se bazeze pe o evaluare prealabilă a faptului că un anumit conținut este adecvat pentru copii, iar un alt conținut nu este adecvat. Deși acest lucru poate fi adevărat, este departe de a fi un standard universal. Ceea ce este considerat adecvat de către un părinte poate să nu fie considerat adecvat de către un alt părinte. Prin urmare, stabilirea unui standard generic cu privire la ceea ce pot sau nu pot face online poate dăuna în mare măsură dezvoltării și autonomiei copiilor.

În plus, părinții nu sunt o autoritate infailibilă în ceea ce privește ceea ce este sau nu este adecvat - un părinte care încearcă să își împiedice copilul de 15 ani să acceseze conținuturi care l-ar putea ajuta să își exploreze sexualitatea ar putea cauza mult rău acelui copil și i-ar încălca autonomia. În astfel de cazuri, faptul că metodele de declarare a vârstei pot fi ocolite cu o relativă ușurință poate

fi, de fapt, un lucru pozitiv, deoarece le poate permite copiilor (în special adolescenților) să ia propriile decizii cu privire la ceea ce ar trebui să vadă. Acesta este motivul pentru care organizații precum Child Rights International Network (CRIN) subliniază importanța primordială a autonomizării și a rezilienței tinerilor, precum și a faptului că aceștia trebuie să aibă un adult de încredere la care să apeleze în cazul în care ceva nu este în regulă. Aceștia explică faptul că acest lucru este mai bun decât orice instrument sau tehnologie care se presupune că este concepută pentru a menține copiii în siguranță (și care, în schimb, poate duce adesea la supraveghere)[25].

Un risc suplimentar provine din faptul că, în unele cazuri, copiii pot fi expuși riscului din partea propriilor părinți sau tutori. Pentru mai multe dintre metodele de verificare a vârstei pe bază de documente analizate, în special pentru metodă 8, adolescenții care nu au propriile documente de identitate oficiale ar putea fi încurajați să primească verificarea din portofelul de identitate electronică al părintelui sau tutorelui lor. În acest fel, accesul tinerilor la anumite servicii și platforme online ar fi condiționat de existența unui părinte sau a unui tutore abuziv sau care controlează. La rândul său, acest lucru ar putea, de fapt, să-i expună mai mult riscului de abuz sau de alte prejudicii. Părinții sau tutorii ar putea, de asemenea, să simuleze că "garantează" pentru copilul lor, oferindu-le acces la un cont pentru copii.

Chiar și atunci când conținutul ar putea fi conceput doar pentru persoanele de peste 18 ani, trebuie, de asemenea, să ne întrebăm dacă este proporțional să mergem atât de departe încât să blocăm accesul copiilor la acel conținut. De exemplu, unii părinți vor decide că nu au nimic împotrivă ca adolescenții lor să se uite la filme clasificate "18". Alte conținuturi ar putea să nu fie destinate copiilor, dar ar putea fi în regulă ca aceștia să le acceseze. Și încă alte conținuturi care ar fi proporționale atunci când sunt blocate pentru un copil de 14 ani ar putea fi disproporționate atunci când sunt blocate pentru un copil de 16 ani. Acest lucru este foarte complex, în timp ce verificarea vârstei este un instrument contondent.

4.3. Să lăsăm companiile să controleze ceea ce pot vedea și face copiii online

O altă problemă este premisa irațională că este fezabil și eficient să "protejăm internetul pentru copii". Cu toate acestea, după cum s-a discutat în secțiunea 2.2, nu există un utilizator universal pentru copii și nici un standard universal pentru ceea ce este și ceea ce nu este acceptabil pentru copii. Această lipsă de universalitate a ceea ce este și ceea ce nu este adecvat pentru copii creează o problemă. Furnizorii cărora li se cere să pună în aplicare verificarea vârstei trebuie să ia o decizie ideologică cu privire la ceea ce consideră că este și nu este adecvat și trebuie să se asigure că aceasta se va traduce în toate contextele și culturile.

Având în vedere că aceasta este o sarcină imposibilă, este posibil ca aceștia să opteze pentru cel mai mic numitor comun: să fie cât mai restrictivi în ceea ce privește ceea ce pot vedea și face copiii și să restricționeze accesul acestor copii la conținutul care este legal pentru ei. Sau, dimpotrivă, este posibil ca acestea să le ofere copiilor conținuturi referitoare la tulburări alimentare, sinucidere și alte subiecte periculoase, deoarece algoritmii care stau la baza platformelor lor se hrănesc cu atenție. În orice caz, acest lucru oferă furnizorilor - în special platformelor Big Tech - un control periculos asupra a ceea ce pot vedea și face copiii online.

Aceste riscuri sunt prezente în special în solicitările bine intenționate, dar adesea profund greșite, ca platformele să împiedice accesul copiilor la conținuturi "dăunătoare". Deși toată lumea ar trebui să fie protejată împotriva manipulării și exploatării online, nu tot ceea ce este dăunător este neapărat inacceptabil. Poate fi important pentru copii să fie expuși la un anumit nivel de conținut online

[25] https://home.crin.org/issues/digital-rights/childrens-right-digital-age?rq=digital%20age

dăunător sau inadecvat, deoarece acest lucru le poate dezvolta rezistența. Împiedicarea lor de a face acest lucru, în virtutea unui internet protejat în mod artificial împotriva copiilor, le poate răpi copiilor oportunitățile de explorare și de dezvoltare personală online. La împlinirea vârstei de 18 ani, aceștia riscă să treacă de la un mediu digital protejat la realitatea restului internetului, fără a avea instrumentele necesare pentru a ști cum să navigheze în siguranță. Prin urmare, este important ca părinții/tutorele și educatorii să îi sprijine pe copii să știe *cum să facă* față experiențelor dificile sau dăunătoare online.

În plus, din cauza problemelor de clasificare a conținutului dăunător (deoarece acesta nu este definit în lege), este probabil ca sistemele de recomandare care încearcă să blocheze conținutul dăunător pentru copii să excludă categorii largi de conținuturi care nu sunt dăunătoare, doar pentru a fi în siguranță. Acest lucru a fost deja observat în cazul conținutului legal LGBTQI+ postat pe platformele de socializare. Dacă copiii nu pot dezactiva astfel de filtre de conținut prea largi, acest lucru poate avea un impact nejustificat asupra dreptului lor la informare.

Convenția cu privire la drepturile copilului stabilește că responsabilitatea principală pentru educația copiilor revine părinților sau tutorelui (tutorilor). După cum subliniază ONU, statele trebuie să le permită părinților și tutorilor să își îndeplinească acest rol[26].Cu toate acestea, verificarea obligatorie a vârstei ar însemna ca supravegherea și implicarea părinților să fie efectiv externalizate către companii. De exemplu, prin instituirea obligativității unor astfel de practici la nivelul UE, legiuitorii ar submina implicarea părinților și, prin urmare, nu și-ar îndeplini obligațiile față de părinți și tutori, impunând un proces care transferă responsabilitatea către o societate privată. Acest lucru lipsește de putere atât copilul, cât și rolul părintelui sau al tutorelui.

Această problemă indică, de asemenea, întrebări normative mai largi cu privire la internet și societate. Încă de la începuturile sale, internetul a fost conceput ca un spațiu liber și deschis pentru schimbul de cunoștințe și crearea de comunități. Așa cum am criticat în repetate rânduri în activitatea noastră privind Regulamentul cu privire la serviciile digitale (DSA), modelele de supraveghere ale marilor companii de tehnologie și "grădinile cu ziduri" ale platformelor de socializare au centralizat în ultimii ani puterea și controlul asupra spațiilor digitale și a vieților noastre digitale.[27]Modelele de afaceri toxice înseamnă că întreprinderile profită de pe urma scandalului și a prejudiciilor, în timp ce oamenii sunt manipulați, exploatați și viața privată și datele lor sunt încălcate în mod repetat prin publicitate de supraveghere, sisteme de recomandare algoritmică și alte practici dăunătoare. Răspunsul la aceste probleme nu ar trebui să fie concentrarea și mai mare a puterii acestor companii asupra vieților noastre prin sisteme de verificare a vârstei, ci mai degrabă înlocuirea modelelor de afaceri bazate pe supraveghere cu ecosisteme de internet care se bazează pe standarde comunitare, principii deschise și democratice, responsabilitate, precum și pe împuternicirea și controlul utilizatorilor.

4.4. Asigurarea dificilă sau imposibilă a anonimatului online

Măsurile de verificare a vârstei (metodele 5, 6, 7 și 8) și, în unele cazuri, măsurile de estimare a vârstei (cum ar fi metoda 9, care prelucrează date biometrice ce pot fi utilizate pentru a identifica persoane, sau metoda 10, care poate crea un portret detaliat al vieții online) prezintă un risc serios de a face imposibil anonimatul online. Acest lucru se datorează faptului că acestea creează posibilitatea - în unele cazuri, inevitabilitatea - de a vă conecta identitatea legală la tot ceea ce faceți online.

[26] https://www.unicef.org/montenegro/en/parenting-0
[27] https://edri.org/our-work/digital-service-act-document-pool/

Deoarece pentru unele persoane este extrem de important să rămână anonime online, pot apărea probleme foarte grave. Faptul de a fi cunoscut și urmărit online poate fi incredibil de periculos pentru jurnaliștii și activiștii anticorupție care caută informații; pentru apărătorii drepturilor omului și activiștii care contestă puterea; pentru avertizorii de integritate și sursele a căror siguranță depinde de păstrarea confidențialității; pentru lucrătorii sexuali care pot fi expuși unui risc ridicat de violență sau abuz atunci când identitatea lor este cunoscută; pentru comunitățile marginalizate care s-au confruntat cu hărțuire sau abuzuri offline și online; și pentru supraviețuitorii abuzurilor sexuale asupra copiilor sau ai abuzurilor domestice. Dincolo de aceasta, viața privată și anonimatul sunt un pilon al democrației și un instrument care permite respectarea drepturilor noastre umane.

De asemenea, o verificare pe scară largă a vârstei ar submina complet, de exemplu, servicii precum TOR (*"onion routing"*) dacă ar fi obligate să o implementeze. TOR este foarte utilizat de persoanele din țările cu un nivel ridicat de cenzură, control și închidere a internetului și este folosit de jurnaliști, apărători ai drepturilor omului și de alte persoane ca mijloc de a rămâne online în ciuda acțiunilor statelor represive.

După cum s-a discutat în capitolul 1, acest lucru nu înseamnă că verificarea vârstei nu ar putea fi făcută niciodată în viitor într-un mod care să respecte drepturile. Este deja mai puțin dăunător să se utilizeze token-uri (ca în metodele 6 și 8) și să se șteargă aproape instantaneu toate datele cu caracter personal, decât să se ceară oamenilor să furnizeze scanări ale documentelor de identitate, mai ales dacă acestea sunt păstrate. Cu toate acestea, aceste metode nu sunt disponibile în prezent pentru a fi utilizate la nivelul UE și nici nu este probabil să fie disponibile în următorii câțiva ani. În plus, ar fi nevoie de mult mai multă supraveghere și control din partea autorităților de reglementare pentru a se asigura că aceste metode sunt aplicate în mod corespunzător și că nu deschid calea pentru o urmărire omniprezentă și alte prejudicii. Suntem sceptici cu privire la faptul că o soluție care îndeplinește toate aceste criterii ar putea fi pusă în aplicare la scară largă.

4.5. Exacerbarea discriminării structurale

Multe persoane nu au documente de identitate oficiale sau alte documente pe care le pot folosi ca substitut pentru un document de identitate pentru adulți (cum ar fi un card de credit sau un card de student - deși acestea sunt problematice, deoarece nu confirmă vârsta în același mod ca documentele emise de guvern, sunt disponibile la vârste diferite în anumite state membre ale UE și prezintă, de asemenea, riscuri mai mari de a fi eludate, deci sunt mai puțin eficiente). Este probabil ca acest lucru să afecteze în mod disproporționat acele persoane care se confruntă deja cu cele mai ridicate niveluri de excluziune structurală și socială. De exemplu, persoanele fără documente - inclusiv, bineînțeles, copiii fără documente - și solicitanții de azil (care, în unele țări, nu primesc documente oficiale până când nu li se acordă azil) ar putea fi complet excluși de la internet. Prejudiciul de a împiedica un copil aflat în această situație să folosească un serviciu de mesagerie pentru a-i contacta pe cei dragi, de exemplu, este profund și trebuie prevenit.

În plus, unele persoane nu au un act de identitate oficial din motive economice (de exemplu, persoanele sărace nu își pot permite un pașaport) sau din cauza discriminării structurale (de exemplu, unele comunități de romi și sinti cărora li s-a refuzat accesul la serviciile publice sau au fost făcute să se simtă mai puțin capabile să le solicite). Prin urmare, orice sistem care se bazează pe existența unei documentații oficiale poate reprezenta o barieră economică sau socială pentru persoanele aflate în aceste situații - ceea ce servește apoi la exacerbarea decalajului digital între cei care pot accesa liber serviciile digitale, pe de o parte, și cei cărora li se refuză în mod sistematic, pe de altă parte.

Chiar și în rândul celor care au documente oficiale de identitate, nu toți vor avea acces la o identitate electronică. Acest lucru poate duce la discriminare pe bază de naționalitate (deoarece unele naționalități nu au acces la eID) sau pe baza altor criterii (cum ar fi vârsta, deoarece persoanele în vârstă pot fi mai puțin confortabile sau mai puțin capabile să utilizeze metode digitale).

În plus, în cazul celor care au acces la o identitate electronică, ar putea exista motive întemeiate pentru care nu se simt confortabil să își asocieze identitatea cu utilizarea internetului. De exemplu, lucrătorii sexuali se bazează din ce în ce mai mult pe serviciile de internet pentru a-și desfășura activitatea. Cu toate acestea, ei se confruntă cu exploatarea sistematică din partea platformelor, cu discriminarea din partea guvernelor și, uneori, cu violențe și abuzuri. Deoarece lucrătorii sexuali au adesea identități intersecționale (cum ar fi faptul că sunt trans sau fără documente), riscurile pentru ei pot fi și mai complexe. Cu toate acestea, fără a fi dispuse să se supună verificării vârstei (metoda 5, de exemplu, a fost folosită de mai multe platforme de muncă sexuală), acestea și-ar putea pierde mijloacele de trai. În sens mai larg, orice persoană care dorește să utilizeze internetul ar putea experimenta un "efect de reținere", prin care teama că istoricul și comunicațiile pe internet vor fi conectate la identitatea lor i-ar descuraja să utilizeze astfel de servicii sau platforme.

O altă fațetă a discriminării care poate apărea în utilizarea metodelor de estimare a vârstei bazate pe sarcini (metoda 11). A cere cuiva să îndeplinească o sarcină pentru a "dovedi" vârsta sa se va baza întotdeauna pe stereotipuri despre ceea ce pot sau nu pot face persoanele de o anumită vârstă. Dar acest lucru nu este întotdeauna accesibil pentru persoanele cu dizabilități fizice care utilizează un cititor de ecran sau alte tehnologii de asistență. Pentru persoanele cu dizabilități intelectuale sau neurodivergente, aceste sarcini ar putea fi extrem de discriminatorii și, prin urmare, ar putea să-i excludă pe cei care nu îndeplinesc sarcina așa cum s-ar aștepta furnizorul să o facă un copil sau un adult "standard".

4.6. Crearea unui fals sentiment de securitate

Toate metodele discutate pot fi, într-o măsură mai mare sau mai mică, eludate. Cu excepția cazului în care oamenii comunică numai cu cei pe care îi cunosc deja, nu există garanții că o persoană are vârsta pe care pretinde că o are.

Acest lucru creează riscul ca spațiile care par a fi accesibile doar copiilor să poată fi de fapt exploatate de actori rău intenționați. În cazul în care copiii și adulții care îi supraveghează cred că instrumentele de verificare a vârstei i-au împiedicat pe adulți să intre într-un anumit spațiu, acest lucru poate crea un fals sentiment de securitate. În secțiunea 4.2, de exemplu, am evidențiat faptul că părinții sau tutorii ar putea utiliza sistemele de identitate electronică pentru a crea conturi care pretind că sunt copiii lor, ceea ce ar putea permite abuzatorilor care sunt, de asemenea, părinți/tutori să vizeze alți copii. Astfel, în loc să fie atenți la riscuri - așa cum ar trebui să fim cu toții atunci când comunicăm online cu persoane pe care nu le cunoaștem - copiii pot crede că se află printre semeni și astfel pot lăsa garda jos. Acest lucru i-ar putea face mai vulnerabili în fața manipulării și a altor forme de exploatare.

De fapt, într-un mod contra-intuitiv, utilizarea verificării vârstei poate chiar *încuraja* actorii rău intenționați să exploateze în mod deliberat instrumentele de verificare a vârstei pentru a obține acces și, prin urmare, încredere în spații închise. Aceștia ar putea face acest lucru prin utilizarea de produse cosmetice și proteze pentru a păcăli sistemele de recunoaștere facială (de exemplu, metoda 9); prin utilizarea documentelor de identitate care aparțin altei persoane (de exemplu, metodele 5, 6 sau 7), poate obținute prin încălcări ale datelor, care vor apărea în mod inevitabil mai frecvent

atunci când platformele sunt obligate să obțină și să stocheze informații de verificare a vârstei utilizatorilor lor; sau prin imitarea comportamentelor care sunt asociate cu copiii (de exemplu, metodele 10 și 11). Cercetările care demonstrează riscul ridicat al furtului de identitate și al fraudei de date au fost descrise în capitolul 3, ceea ce creează și mai multe riscuri pentru securitatea online a persoanelor.

Capitolul 5: Concluzii

5.1. Focalizarea pe protecția vieții private și asigurarea securității încă din proiectare

Nu există dovezi că măsurile de verificare a vârstei aplicate pe scară largă (de exemplu, pentru majoritatea sau pentru toate serviciile de mesagerie, serviciile de socializare etc.) vor fi benefice pentru copii. Dimpotrivă, măsurile de **verificare a vârstei bazate pe documente se bazează** pe adoptarea pe scară largă a unui sistem de identitate digitală adecvat. După cum s-a explicat în acest document, UE sigur nu va avea acest lucru până în 2030 (dacă va avea vreodată, în funcție de faptul dacă eventualul portofel eID este sau nu cu adevărat anonim și cu zero cunoștințe). Chiar și atunci, este probabil să excludă 20% dintre utilizatorii legitimi. Pentru cei care nu au documentele necesare, cum ar fi tinerii fără documente, nicio evoluție tehnologică nu va împiedica excluderea lor.

Măsurile de **estimare a vârstei** evită provocarea reprezentată de necesitatea unei identități legale formale, dar creează noi provocări, cum ar fi prelucrarea sistematică și invazivă a datelor tinerilor, contrară obiectivelor Regulamentului privind serviciile digitale (DSA). De asemenea, astfel de practici sunt susceptibile să echivaleze cu crearea de profiluri și să implice un risc serios de discriminare. Temeiul juridic al consimțământului pentru o astfel de profilare, care ar putea fi necesar să fie invocat de furnizori în temeiul art. 22 din GDPR, este puțin probabil să fie legal în acest context coercitiv.

Unii furnizori experimentează combinarea **verificării vârstei pe bază de documente și a măsurilor de estimare a vârstei** pentru a oferi o alegere utilizatorilor. Cu toate acestea, această "alegere" va fi probabil iluzorie, deoarece atât verificarea vârstei pe bază de documente, cât și estimarea vârstei sunt însoțite de o gamă largă de riscuri deja discutate. De exemplu, ambele măsuri permit în continuare furnizorilor să stabilească parametrii a ceea ce pot vedea copiii online. În plus, ele riscă să blocheze accesul copiilor la anumite conținuturi sau să îi facă să se simtă vinovați sau să se teamă să le acceseze (de exemplu, conținuturi privind sănătatea sau LGBTQI+).

Premisa că problemele de siguranță online pot fi rezolvate prin suprapunerea mai multor măsuri ascunde, de asemenea, realitatea că măsurile de verificare a vârstei pot crea un fals sentiment de securitate. De fapt, confidențialitatea și securitatea prin concepție, precum și o supraveghere adecvată (în conformitate cu autonomia crescândă a copiilor) sunt susceptibile de a fi mult mai eficiente, după cum se discută pe larg pe parcursul acestui document. Atunci când sunt combinate cu măsuri de **declarare a** vârstei, care sunt cele mai puțin riscante pentru drepturile copiilor, considerăm că astfel de măsuri sunt cel mai probabil să reprezinte un echilibru adecvat al drepturilor copiilor în mediul digital.

În sens mai larg, am contestat, de asemenea, premisa de a solicita documente formale sau o prelucrare invazivă a datelor ca etapă preliminară al accesului la lumea digitală, precum și limitările privind libertatea de exprimare și accesul la informații pe care aceasta le implică. În plus, subliniem că, în conformitate cu Carta, este puțin probabil ca verificarea și estimarea pe scară largă sau sistematică a vârstei pe bază de documente și estimarea vârstei să îndeplinească pragurile necesare de **necesitate** și **proporționalitate**.

O altă concluzie care poate fi trasă din acest document este că verificarea vârstei nu ar trebui să fie considerată în cadrul limitat al instrumentelor tehnice (în special, instrumentele de verificare a vârstei bazate pe documente și de estimare a vârstei). În schimb, verificarea vârstei ar trebui privită

ca un spectru în care mai multe măsuri neinvazive sunt disponibile, care pot fi acumulate (inclusiv cu măsuri de declarare a vârstei) pentru a atinge un standard suficient de protecție a copilului. Pe lângă cele câteva măsuri de siguranță și de protecție a vieții private prin concepție deja discutate în acest document, ar trebui explorate în continuare idei precum etichetarea conținutului/avizele privind conținutul sau versiunile de servicii pentru copii, ca metode de creștere a siguranței în conformitate cu drepturile fundamentale.

5.2. Recomandări

Pentru politicieni

1. Având în vedere lipsa actuală a unor instrumente eficiente și conforme cu drepturile, precum și gravitatea și amploarea riscurilor, **factorii de decizie politică și legislativă nu trebuie să impună măsuri de asigurare a vârstei** (un termen folosit uneori ca o umbrelă pentru numeroasele metode diferite), de **estimare a vârstei sau de verificare a vârstei (bazate pe identitate) la** nivel general/la nivelul UE;
2. În ceea ce privește în mod specific Regulamentul CSA al UE, măsurile de "asigurare" a vârstei (termenul utilizat în propunere), de verificare sau de estimare nu ar trebui să devină obligatorii pentru niciun furnizor (articolele 4 și 6) și nici nu ar trebui ca utilizarea lor să fie stimulată prin intermediul procesului de evaluare și de reducere a riscurilor (articolele 3 și 4);
3. În cazul în care măsurile opționale de verificare sau estimare a vârstei rămân în Regulamentul CSA, acestea trebuie să fie protejate pentru a se asigura că respectă pragurile de la pagina 17 și recomandările de la punctele 8, 9, 12, 13 și 14 de mai jos. De asemenea, acestea ar trebui să le ofere furnizorilor posibilitatea de a-și îndeplini obligațiile prin măsuri de declarare a vârstei;
4. Este esențial ca factorii de decizie politică și legislativă, precum și părinții și tutorii, să se informeze mai bine cu privire la modul în care funcționează instrumentele de verificare a vârstei, la riscurile pe care le implică aceste instrumente și la posibilele alternative la aceste măsuri intruzive;
5. Ar putea fi efectuate mai multe cercetări cu privire la măsurile de estimare a vârstei și de verificare pe bază de documente care respectă drepturile, deoarece niciuna dintre metodele disponibile în prezent pentru implementarea practică nu poate fi considerată ca fiind conformă cu drepturile copilului.[28]
6. Comisia Europeană, Agenția pentru Drepturi Fundamentale (FRA) și Comitetul european pentru protecția datelor (EDPB) ar trebui să emită orientări privind verificarea vârstei în conformitate cu *Regulamentul general privind protecția datelor*, adoptând o abordare holistică care să meargă dincolo de verificările de vârstă și să ia în considerare întregul spectru de măsuri de siguranță și de confidențialitate prin concepție;
7. Grupul special al UE privind proiectarea adecvată vârstei ar trebui să elaboreze recomandări privind caracteristicile de proiectare și măsurile societale care vor reduce stimulentele pentru ca tinerii să declare în mod fals vârsta greșită online, sporind astfel eficiența metodelor de declarare a vârstei; [29]

[28] Aceasta este, de asemenea, concluzia CNIL în analiza *Verificarea online a vârstei: echilibrul între viața privată și protecția minorilor* https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors[29]
[29]https://zephoria.medium.com/protect-elders-ban-television-2b18ab49988b

Pentru furnizorii de platforme și servicii online

8. Ori de câte ori se utilizează măsuri de verificare a vârstei, acestea trebuie să fie necesare, proporționale și suficient de sigure; nu trebuie să permită utilizarea datelor în alte scopuri; nu trebuie să păstreze nu trebuie să prelucreze date biometrice sau bazate pe date biometrice; nu trebuie să permită niciodată asocierea persoanei cu identitatea sa legală sau crearea vreunui profil al acesteia; și trebuie să se asigure că persoanele pot rămâne complet anonime online;
9. Orice propunere de utilizare a măsurilor de estimare a vârstei sau de verificare pe bază de documente trebuie să fie evaluată de la caz la caz, cu ajutorul unei evaluări a impactului asupra protecției datelor (DPIA) și - în cazul în care riscurile sunt semnificative - cu consultarea prealabilă a autorității naționale pentru protecția datelor (DPA);
10. Ca regulă generală, și cu excepția cazului în care legislația națională impune altfel, furnizorii ar trebui să utilizeze numai metode de declarare a vârstei, până când riscurile și dezavantajele grave ale măsurilor de verificare a vârstei vor fi atenuate, acordând o atenție deosebită excluderii structurale și potențialelor efecte de intimidare;
11. În cazul în care se dovedește că măsurile de verificare a vârstei pe bază de documente sunt strict necesare (de exemplu, pentru cazuri de utilizare specifice la nivel național), acestea ar trebui să fie strict controlate și ar trebui să se ia măsuri pentru a aborda toate riscurile prezentate în această informare;
12. Pe baza acestei analize, pare puțin probabil ca riscurile metodelor de estimare a vârstei discutate să poată fi atenuate suficient de mult pentru a face acceptabilă utilizarea lor. În special, prelucrarea datelor biometrice sau a altor date sensibile în acest scop reprezintă o linie roșie. Cu toate acestea, în cazul în care evoluțiile viitoare vor arăta că acestea pot fi utilizate într-un mod care respectă drepturile, utilizarea lor ar trebui, de asemenea, să fie strict controlată și ar trebui luate măsuri pentru a aborda toate riscurile prezentate în această informare;
13. În cazul în care instrumentele de verificare a vârstei sunt furnizate de terți, aceștia trebuie să fie independenți și nu trebuie să aibă caracter comercial;
14. Întrucât măsurile de declarare a vârstei au, în general, un nivel de eficacitate scăzut spre mediu, acestea ar trebui să fie completate cu alte măsuri, de la caz la caz. Acestea ar putea include modificări ale algoritmilor de furnizare a conținutului (sisteme de recomandare); asigurarea securității, siguranței și confidențialității din momentul concepției și în mod implicit pentru toți utilizatorii; etichetarea conținutului; și făcând mai puțin atractiv pentru utilizatori să mintă în legătură cu vârsta lor;

Pentru întreaga societate

15. Încurajăm o dezbatere societală mai amplă cu privire la necesitatea și utilizarea măsurilor de verificare a vârstei, inclusiv dacă instrumentele de verificare a vârstei sunt cele mai potrivite pentru a rezolva problemele în cauză sau dacă acestea sunt probleme sociale care necesită o intervenție structurală;
16. Subliniem faptul că participarea la societatea online și offline nu ar trebui să devină niciodată condiționată de documentele de identitate;
17. Recomandăm ca părinții, profesorii, asistenții sociali și alți educatori și persoane aflate în poziții de autoritate să ofere îndrumare și sprijin pentru a-i însoți pe copii să se raporteze și să înțeleagă riscurile conținutului online, recunoscând în același timp nevoia de autonomie și de confidențialitate a copiilor.