

II Ce este legal și ilegal în conținutul online?

1. Conținutul legal și conținutul ilegal

Stabilirea legalității conținutului online este realizată prin prisma excluderii conținutului ilegal, iar acesta din urmă se referă la informația care nu se află în conformitate fie cu dreptul Uniunii Europene, fie cu dreptul unui stat membru. **Astfel, tot ceea ce nu încalcă o lege națională sau europeană ar trebui să fie, în principiu, conținut online legal.** De asemenea, ca regulă nu ar trebui să existe diferențe între ceea ce este considerat ilegal în mediul offline și în mediul online.

Conform articolului 3(h) din Regulamentul 2022/2065 DSA, conținutul ilegal “înseamnă orice informație care, în sine sau prin raportare la o activitate, inclusiv vânzarea de produse sau furnizarea de servicii, nu este conformă cu dreptul Uniunii sau cu dreptul oricărui stat membru care este conform cu dreptul Uniunii, indiferent de obiectul sau natura exactă a dreptului respectiv.”

Însă cine declară că un conținut este ilegal? În lipsa vreunei dispoziții legale specifice, doar o instanța de judecată este în măsură de a stabili faptul că un anumit conținut este ilegal.

Există însă instituții precum CNA, CNCD sau ANSPDCP au atribuții în stabilirea caracterului ilegal al unui conținut însă exclusiv pe un domeniu specific reglementat (de ex., după caz conținut audio-video, conținut discriminatoriu, date personale prelucrate ilegale).

2. Conținut legal, dar nepermis pe o anumită platformă:

În mediul online pot exista informații care, deși nu sunt interzise prin lege, contravin condițiilor generale de utilizare a unei platforme online, stabilite de acestea din urmă, însă respectând drepturile fundamentale ale utilizatorilor. Platformele online au posibilitatea de a lua măsuri împotriva unor astfel de informații. Cu toate că Regulamentul DSA prevede reguli cu privire la conținutul ilegal, platformele online nu sunt împiedicate să utilizeze aceleași mecanisme și pentru a combate conținutul ce încalcă termenii și condițiile lor, în special conținutul dăunător unor categorii de utilizatori precum minorii. Mai mult, Platformele online foarte mari (VLOPS) și Motoarele de căutare online foarte mari (VLOSE) sunt obligate să țină cont și de efectele negative reale sau previzibile asupra unor categorii de persoane și subiecte când evaluează și atenuează riscurile sistemice.

2.1. Conținut dăunător (harmful content)

Conținutul dăunător se poate referi atât la un conținut cu **efect negativ actual**, cât și la unul cu **efect negativ potențial**, și posibilă sa influență asupra comportamentelor și atitudinilor persoanelor vulnerabile, conform unui raport asupra protecției copiilor față de conținutul dăunător realizat pentru Consiliul Europei. Conținutul violent, conținutul ce face referire la consumul de droguri, scenele horror, sau conținutul ce promovează tulburările de alimentație sunt câteva exemple de conținut dăunător pentru minori.

2.2. Alt tip de conținut care încalcă Termenii și condițiile platformelor

Însă nu doar conținutul dăunător poate fi în contradicție cu termenii și condițiile stabilite de platforme. Platformele online pot stabili reguli prin care să interzică un conținut ce în principiu este permis prin lege, însă pe care platformele respective nu îl agreează. Interzicerea limbajului licențios ori interzicerea nudității pentru toate categoriile de utilizatori pot fi exemple în acest sens.

III Reglementare conținut online - Cine sunt actorii și rolul lor?

Reglementările europene aduc o serie de noutăți nu doar din perspectiva obligațiilor și interdicțiilor introduse, ci și prin termenii utilizați. Înțelegerea rolurilor îndeplinite de actorii reglementați prin noile acte legislative europene și plasarea lor în contextul corect este importantă atât pentru cei vizați de schimbările legislative, cât și pentru utilizatorii obișnuiți din spațiul online.

1. Competent Authorities

(în română: *Autoritățile competente*)

Regulamentul 2022/2065 DSA articolul 49

Sintagma “autorități competente” se referă în contextul Regulamentului DSA la autoritățile naționale, prezente în fiecare Stat Membru al Uniunii Europene, cu atribuții stabilite prin legislația europeană pentru supravegherea modului în care sunt respectate prevederile europene. O astfel de entitate este autoritatea responsabilă cu supravegherea furnizorilor de servicii intermediare, cu atribuții stabilite prin Regulamentul DSA. În România acest rol este îndeplinit de Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM). Un alt exemplu al unei autorități competente naționale, însă într-un domeniu diferit (protecția datelor personale), este autoritatea de supraveghere prevăzută de Regulamentul General Privind Protecția Datelor, denumită “Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal” în România.

2. Digital Services Coordinator

(în română: *Coordonator al serviciilor digitale*)

Regulamentul 2022/2065 DSA articolele 49-51

Statele Membre UE sunt obligate să desemneze câte o autoritate competentă ca un Coordonator al serviciilor digitale conform prevederilor Regulamentului DSA. Printre competențele Coordonatorului se regăsesc posibilitatea de a efectua inspecții în cazul unei presupuse încălcări a prevederilor legale, dispunerea încetării încălcărilor și impunerea amenzilor. În România acest rol este îndeplinit de Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM). Așa cum îi spune și numele, rolul său este de coordonare între autoritățile competente, și nu de preluarea a competențelor pe domeniul digital al altor autorități.

3. European Commission / Comisia Europeană

Regulamentul 2022/2065 DSA, Regulamentul 2022/1925 DMA

La nivelul întregii Uniuni Europene, Comisia Europeană are un rol crucial de reglementare directă stabilit prin noile reglementări. Conform Regulamentului DSA, Comisia este cea care desemnează serviciile care se încadrează în categoria de platforme online foarte mari (VLOPS) sau de motoare de căutare online foarte mari (VLOSE). De asemenea, în conformitate cu Regulamentul DMA, Comisia desemnează controlorii de acces (gatekeepers) ce își desfășoară activitatea în Uniune.

4. Providers of intermediary services

(în română: *Furnizorii de servicii intermediare*)

Regulamentul 2022/2065 DSA capitolele II - III

Conform Regulamentului DSA, **un serviciu intermediar** poate fi un serviciu al societății informaționale de trei tipuri: **de simplă transmitere, de stocare în cache sau de găzduire**. În această ultimă categorie intră și **platformele online** ce găzduiesc conținut postat de utilizatori. Tot în categoria de serviciu intermediar intra și un **motor de căutare online**.

Ce **nu** se încadrează în categoria de serviciu al societății informaționale? Spre exemplu, serviciile de difuzare a conținutului audio-video.

Răspunderea furnizorilor variază în funcție de tipul de serviciu intermediar prestat. Regulamentul DSA stabilește de asemenea obligații comune tuturor furnizorilor de servicii intermediare, dar și obligații specifice în funcție de tipul de serviciu intermediar furnizat. Un exemplu este obligația stabilită doar pentru furnizorii de servicii de găzduire, de a implementa mecanisme de notificare a conținutului ilegal în cadrul serviciului pe care îl oferă.

5. Very Large Online Platforms (VLOPS), Very Large Online Search Engines (VLOSE)

(în română: *Platforme Online Foarte Mari și Motoare de Căutare Online Foarte Mari*)

Regulamentul 2022/2065 DSA articolul 33

Platforme sau motoare de căutare care au un număr mediu lunar de destinatari activi ai serviciilor în Uniune mai mare sau egal cu 45 de milioane și care sunt desemnate Platforme Online foarte mari și motoare de căutare online foarte mari de către Comisia Europeană în urma unor consultări. Acestea au diferite obligații stabilite prin lege, precum **evaluarea riscurilor sistemice** și **atenuarea** acestora. Astfel, este necesar să identifice, analizeze și evalueze riscurile sistemice cauzate de serviciile lor, dar și să instituie măsuri de atenuare față de aceste riscuri. [Lista serviciilor desemnate ca VLOPS și VLOSE](#) este publicată de Comisia Europeană. Până în acest moment au fost desemnate 25 de servicii de la 19 furnizori, printre ele numărându-se Amazon Store, Google Search, Tik Tok, Facebook și Instagram.

6. Trusted Flaggers

(în română: *Notificatori de încredere*)

Regulamentul 2022/2065 DSA articolul 22

Statutul de notificatori de încredere este un statut acordat la cerere de către coordonatorul serviciilor digitale dintr-un stat membru unei entități care îndeplinește o serie de condiții: are **cunoștințe de specialitate și competențe specifice** în detectarea, identificarea și notificarea conținutului ilegal, este **independent** de orice furnizori de platforme online, își desfășoară activitățile de așa manieră încât să transmită notificări cu **diligență, acuratețe și obiectivitate**. Pot transmite notificări pentru a semnala existența conținutului ilegal în cadrul unui serviciu de găzduire (hosting service) iar acestea vor fi tratate cu prioritate. De asemenea, notificatorii de încredere au obligația de a publica cel puțin anual rapoarte cu privire la notificările trimise. Lista notificatorilor de încredere este publicată de către Comisia Europeană, iar una dintre entitățile ce deține deja acest statut este Organizația Salvați Copiii România.

7. Users (“any individual or entity”)

(în română: *utilizatori obișnuiți* (orice persoană fizică sau entitate))

Regulamentul 2022/2065 DSA articolul 16

În ceea ce privește utilizatorii obișnuiți ai platformelor online, aceștia au posibilitatea de a se implica în combaterea conținutului ilegal conform Regulamentului DSA. Furnizorii de servicii de găzduire trebuie să pună la dispoziția oricărei persoane mecanisme prin care aceștia să poată notifica existența unui conținut ilegal pe platformele online. Practic, nu doar notificatorii de încredere (trusted flaggers) au acest drept de raportare, ci orice utilizator al unei platforme online. Diferența dintre notificările realizate de utilizatorii obișnuiți și cele realizate de entități desemnate ca trusted flaggers este că notificările celor din urmă trebuie tratate cu prioritate. Însă furnizorii nu sunt împiedicați să trateze în mod similar și notificările primite de la utilizatorii obișnuiți.

8. Gatekeepers

(în română: *Controlori de acces*)

Regulamentul 2022/1925 DMA capitolele II - III

Un controlor de acces este o întreprindere care furnizează **servicii de platformă esențiale**, precum servicii de intermediere online, motoare de căutare online, servicii de rețele de socializare online etc., fiind **desemnată** ca gatekeeper în cazul în care are un **impact semnificativ** asupra pieței interne, furnizează un serviciu de platformă esențial care **reprezintă un punct de acces important** prin care utilizatorii comerciali ajung

la utilizatorii finali și **beneficiază de o poziție solidă și durabilă**, în ceea ce privește operațiunile sale, sau este previzibil că va beneficia de o astfel de poziție în viitorul apropiat.

Gatekeepers desemnați până acum: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, Booking

Exemple de servicii de platformă esențiale: TikTok, Facebook, Instagram, LinkedIn, Google Search, Youtube, WhatsApp, Google Maps, Amazon Marketplace etc.

Controlorii de acces au o serie de obligații și interdicții stabilite prin regulamentul DMA. Spre exemplu, pe de o parte, trebuie să le permită **utilizatorilor comerciali**, cu titlu gratuit, să promoveze oferte utilizatorilor finali dobândiți prin intermediul serviciului de platformă esențial. Pe de altă parte, trebuie să le permită **utilizatorilor finali** să utilizeze, prin intermediul serviciilor sale, conținut, abonamente sau alte elemente utilizând aplicația software a unui utilizator comercial.

9. Providers of Artificial Intelligence systems or of general use Artificial Intelligence models

(în română: *Furnizori de sisteme de Inteligență Artificială sau de modele de Inteligență Artificială de uz general*)

Regulamentul 2024/1689 AI Act articolele 2(1), 3(3)

Furnizorii de **sisteme** de Inteligență Artificială (IA) sau de **modele** de Inteligență Artificială de uz general intră sub incidența Regulamentului AI Act (AIA) când introduc pe piață sau pun în funcțiune astfel de sisteme sau modele în Uniunea Europeană. Furnizorii înșiși nu trebuie să se afle pe teritoriul Uniunii. De asemenea, în situația în care rezultatele produse de sistemele lor de Inteligență Artificială sunt utilizate în Uniune, acestora li se vor aplica prevederile regulamentului, chiar dacă își au sediul în afara Uniunii.

Furnizorul poate să fie o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism. Poate să dezvolte el însuși sistemul sau modelul, ori doar să comande dezvoltarea sa. Răspunderea este generată de introducerea pe piață sau punerea în funcțiune sub numele sau marca comercială proprie, iar acest lucru poate fi realizat contra cost ori gratuit, regulamentul aplicându-se în ambele situații.

10. Deployers of AI systems

(în română: *Implementatori de sisteme de IA*)

Regulamentul 2024/1689 AI Act articolul 3(4)

Implementatorii de sisteme de Inteligență Artificială sunt persoane fizice sau juridice, inclusiv autorități publice, care **utilizează un sistem de IA aflat sub autoritatea lor**. În cazul în care sistemul de IA este utilizat în cursul unei activități personale, fără caracter profesional, utilizatorul nu va fi considerat implementator.