



ROMANIA

PARLAMENTUL ROMÂNIEI

CAMERE DEPUTAȚILOR

DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ

doc@cdep.ro

SANȚIONAREA UNOR CONDUITE INFRAȚIONALE CARE INCLUD UTILIZAREA TEHNOLOGIILOR DE TIPUL DEEPPFAKE

VLAD DRAGUȘ, CONSILIER PARLAMENTAR

Legislația „deepfake” este încă în stadiul său incipient, atât în SUA cât și în Uniunea Europeană. Cu toate acestea, au fost (și sunt) depuse eforturi legislative în această direcție - prin propuneri legislative introduse în circuitele parlamentare sau a unor propuneri de reglementare anunțate ca priorități, în perioada imediat următoare. Este important de remarcat și faptul că utilizarea *deepfake* în scopuri infracționale este (încă) relativ rară. Cu toate acestea, pe măsură ce tehnologia care permite crearea de conținuturi *deepfake* continuă să se dezvolte și să devină mai accesibilă, este previzibilă creșterea utilizării acesteia pentru activități infracționale. În ceea ce privește exemplul unor state care au sancționat un astfel de comportament (sau au priorități în acest sens) enumerăm:

- Statele Unite: în 2020, Departamentul Trezorerie al SUA l-a sancționat pe cetățeanul Federației Ruse Aleksandr Viktorovich Malkevici pentru utilizarea tehnologiilor *deepfake* în vederea creării și difuzării de materiale video menite să interfereze cu alegerile prezidențiale din SUA (din 2020);
- Regatul Unit al Marii Britanii: în 2021, guvernul a anunțat că [are în vedere sancțiuni](#) împotriva persoanelor și companiilor care sunt implicate direct sau indirect în crearea și utilizarea de *deepfake*. Guvernul nu a anunțat încă nicio sancțiune/ sancțiuni specifică/ specifice, dar este evident că Regatul Unit ia în serios amenințarea reprezentată de *deepfake*;
- Canada: în 2022, guvernul canadian a introdus [Legea privind Streaming-ul online](#), care ar impune platformelor de *streaming online* să elimine conținutul dăunător, inclusiv de natură *deepfake*. Proiectul de lege nu a intrat încă în vigoare, dar este un semn că guvernul canadian se angajează să abordeze problema *deepfake*;
- Australia: în 2021, guvernul australian a anunțat că va elabora o nouă legislație pentru [a aborda problema deepfake](#). Guvernul nu a făcut încă niciun fel de detalii cu privire la legislația propusă, dar se preconizează că aceasta va fi introdusă în parlament în 2023;
- Noua Zeelandă: în 2022, guvernul Noii Zeelande a anunțat că are în vedere sancțiuni împotriva persoanelor fizice și a societăților care sunt implicate în crearea și utilizarea de *deepfake*. Guvernul nu a anunțat încă nicio sancțiune specifică, dar este clar că Noua Zeelandă ia în serios amenințarea reprezentată de *deepfake*, [fiind elaborate studii](#) care fundamentează această opțiune.

UNIUNEA EUROPEANĂ

[Propunerea de regulament privind serviciile digitale](#) (DSA) a Uniunii Europene, este preconizată să intre în vigoare în 2024; actul va institui obligația companiilor mari din domeniul IT&C să ia măsuri pentru a combate dezinformarea și *deepfake*-urile pe platformele proprii.

[EU Code of Practice on Disinformation](#) - și-a propus consolidarea măsurilor de reducere a comportamentelor manipulative utilizate pentru a răspândi dezinformarea (de exemplu, conturi false, multiplicarea mesajelor utilizând boți, furtul/uzurparea identității, falsuri *deepfake* rău intenționate/ malițioase) precum și stabilirea unei cooperări mai puternice (între semnatori) pentru a răspunde eficient și a combate provocările legate de astfel de tehnici (în propunerea de actualizare din 2022 au fost incluse cerințe mai stricte pentru eliminarea *deepfake*-urilor, iar platformele care încalcă codul ar putea suferi amenzi de până la 6% din veniturile lor globale).

SUA

În prezent, nu există legislație federală care să abordeze specific potențialele amenințări ale tehnologiei *deepfake* în Statele Unite. Cu toate acestea, în decembrie 2019, Congresul a adoptat [Actul de autorizare a apărării naționale](#) care, în secțiunea 5709, instituie obligația directorului de informații naționale (FBI) să raporteze despre utilizarea *deepfake*-urilor de către alte state, capacitatea acestor practici de a răspândi dezinformare și potențialele amenințări asupra securității naționale.

De la adoptarea acestui act, doar cinci state au adoptat legislație privind tehnologia *deepfake* emergentă. În 2019, statul Texas a adoptat [S.B. 751](#) și California [AB730](#), ambele interzicând utilizarea *deepfake*-urilor pentru a influența alegerile. Actul [S.B. 337](#) din Georgia, și actul [SB 1736](#) din Virginia¹ au fost adoptate pentru a interzice crearea și diseminarea pornografiei *deepfake* neconsensuale. În 2020, New York a adoptat legea [S6829A](#), care stabilește drepturile de acțiune în justiție împotriva publicării ilegale de *deepfake*.

În ceea ce privește [H.R.2231 - Algorithmic Accountability Act of 2019](#) și în baza acestui act propunerea legislativă [H.R.3230 - DEEP FAKES Accountability Act](#) scopul a fost acela de a impune răspunderea civilă și penală persoanelor care creează sau distribuie falsuri *deepfake* fără o declinare corespunzătoare. În ciuda presupuselor sale beneficii, [criticii](#) spun că această legislație ar împovăra de fapt utilizatorii legitimi ai tehnologiei (care e folosită manipulativ și de cei care produc *deepfake*) și ar greva instanțele cu litigii din cauza definiției prea ample a „*deepfake*”. În schimb, spun juriștii, abuzul de tehnologie pentru a produce *deepfake* ar trebui să fie abordat judiciar printr-

¹ Virginia Deepfake Law incriminează crearea și diseminarea *deepfake*-urilor explicate din punct de vedere sexual. Legea include excepții, cum ar fi parodiile și comentariile politice, și solicită procurorului general să înființeze un grup de lucru pentru a studia / monitoriza în continuare *deepfake*-urile.

o combinație a reglementărilor drepturilor de autor cu prevederile penale și delictuale pentru a impune răspunderea rău-utilizatorilor

Fransa

La 4 iulie 2023, Senatul a examinat [proiectul de lege](#) care vizează securizarea spațiului digital. Modificările aduse prin proiect se doresc a acționa pe mai multe dimensiuni ale spațiului digital (lupta împotriva hărțuirii cibernetice, controlul vârstei audienței conținutului pornografic, reglementarea site-urilor de închiriere turistică, probleme de *portare* la operatorii de contracte *cloud* etc.). Pe lângă aceste elemente, prin două amendamente aduse proiectului inițial, s-a adăugat problema cadrului legal pentru *deepfake*. Primul amendament prevede modificarea articolului 226-8 din [Codul penal](#), prin care se incriminează producerea montajelor realizate cu imaginea sau vocea unei persoane fără acordul acesteia din urmă. Aceasta ar presupune:

„Fapta de a publica, prin orice mijloc, conținut vizual sau audio generat prin prelucrare algoritmică și reproducerea „imaginii sau cuvintelor unei persoane, fără consimțământul acesteia, dacă nu este evident că este algoritmic”.

Sanctiunea propusă este de doi ani de închisoare și o amendă de 45.000 de euro atunci când publicarea montajului sau a conținutului generat prin prelucrare algoritmică a fost efectuată folosind un serviciu public de comunicare online”. Al [doilea amendament](#) urmărește introducerea unui articol 226-8-1 în Codul penal, care să prevadă: „Fapta de a publica, fără acordul său, prin orice mijloace, un montaj audio-video realizat cu cuvintele sau imaginea unei persoane și care prezintă o natură sexuală”.

Germania

La nivel federal, singura reglementare care ar pute intra în sfera tehnică a dezinformării prin intermediul *deepfake* este regăsită în Codul Penal la [secțiunea 201a](#)

Cu toate că nu se specifică, la conduita interzisă, o descriere în concret a unor materiale video create prin tehnologie specifică *deepfake*, textul legii face referire la materialele folosite pentru producerea materialelor compromițătoare. Secțiunea se referă la producere de imagini degradante sau jignitoare pentru imaginea publică a unei persoane, fie ea și decedată, și nu la imagini produse în scopul dezinformării în sens larg.

Irlanda

În momentul de față, se află în stadiul de dezbateri la comisii, [un act normativ](#) privind siguranța în mediul online. Actul cuprinde și o secțiune prin care se incriminează „crearea și diseminarea de informații dăunătoare”:

(1) Persoana care:

(a) creează sau produce informații false dăunătoare sau

(b) pune la dispoziția altora materiale de dezinformare dăunătoare,

comite o infracțiune.

„Dezinformarea dăunătoare” este definită în lege ca „informații care sunt false sau înșelătoare și care cauzează sau sunt susceptibile de a cauza prejudicii unei persoane, unui grup de persoane sau societății în ansamblu”. Legea menționează în deepfakes ca exemplu de dezinformare dăunătoare.

România

Senatul României a adoptat o propunere legislativă pentru reglementarea folosirii cu rea-intenție a tehnologiilor *deepfake*.

https://www.senat.ro/legis/lista.aspx?nr_cls=L295&an_cls=2023

LINKURI UTILE

[EU AI Act: first regulation on artificial intelligence](#)

[The 2022 Code of Practice on Disinformation](#)

IRLANDA [Online Safety and Media Regulation Act 2022](#)

ROMÂNIA / SENAT https://www.senat.ro/legis/lista.aspx?nr_cls=L295&an_cls=2023

SUA [DEEP FAKES Accountability Act Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019](#)

[H.R.3230 - DEEP FAKES Accountability Act](#)

<https://armedservices.house.gov/ndaa>

<https://capitol.texas.gov/tlodocs/86R/billtext/pdf/SB00751F.pdf>

[Deep Fakes Accountability Act: Overbroad and Ineffective](#)

<https://legiscan.com/VA/bill/HB2678/2019>

[S. 2065, Deepfake Report Act of 2019](#)

<https://www.wilmerhale.com/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law>

https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf