15 Ianuarie 2026

RAPORT DE ANALIZĂ ȘI EVALUARE A PROIECTULUI LEGISLATIV Pl-x nr. 565/2025 PRIVIND MODIFICAREA LEGII SECURITĂȚII NAȚIONALE

Rezumat executiv: Acest raport analizează proiectul de lege Pl-x nr. 565/2025, o inițiativă transpartinică (PSD, PNL, USR, AUR) ce vizează redefinirea capacităților operative ale statului român în spațiul digital:

· Deși proiectul introduce garanții procedurale necesare pentru alinierea la standardele CEDO, precum limite temporale de stocare a datelor, analiza avertizează asupra riscurilor majore privind viața privată și libertățile civile. Documentul subliniază ambiguitatea conceptului de „resurse în mediul on-line" și absența unui control judecătoresc prealabil pentru crearea bazelor de date.

· Analiza comparativă între tehnicile globale de manipulare cognitivă și modificările legislative propuse în România prin inițiativa PL-X 565/2025 arată că arhitectura legală propusă în PL-X 565/2025 este perfect compatibilă și necesară pentru implementarea tehnicilor de micro-targetare avansată și război cognitiv. Legea pare să fi fost desenată pentru a oferi acoperire legală infrastructurii de date necesare acestor operațiuni.

CUPRINS

Partea I: Cadrul Paul-Elder

1. SCOPUL ȘI OBIECTIVUL LEGISLAȚIEI (Standard: claritate și semnificație) Proiectul Pl-x 565/2025 prezintă o dualitate a obiectivelor:

- **Scopul declarat (Juridic):** Alinierea Legii nr. 51/1991 la exigențele CEDO pentru a elimina vulnerabilitățile care au dus la condamnări repetate ale României (cauzele *Rotaru*, *Bucur și Toma*). Se urmărește crearea unui

„blindaj juridic” prin norme clare și previzibile privind ingerințele în viața privată.
- **Scopul latent (Operațional):** Operaționalizarea capacităților de război cognitiv și obținerea hegemoniei informaționale în mediul online. Proiectul abilitează serviciile să treacă de la o postură reactivă de interceptare la una proactivă de modelare a percepției publice.

2. ÎNTREBAREA ÎN DISCUȚIE (Standard: precizie și complexitate) Întrebarea centrală a analizei este: „Poate fi reconciliată necesitatea unei supravegheri digitale omniprezente cu garanțiile constituționale privind viața privată, în absența unui control judecătoresc prealabil strict?”. Sub-întrebările critice includ:

- Care este natura juridică a „resurselor online” și dacă acestea constituie vectori de supraveghere mascată?
- Este suficient controlul parlamentar ulterior pentru a satisface standardul CEDO de „independență efectivă”?

3. INFORMAȚIA ȘI CONTEXTUL (Standard: acuratețe, relevanță și logică) Contextul este marcat de accelerarea tehnologică și de amenințările hibride de la granița de est. Analiza se bazează pe:

- **Inovația normativă (Art. 13 lit. e^1):** Abilitarea serviciilor de a crea și utiliza aplicații și baze de date.
- **Regimul datelor (Art. 23^1-23^8):** Introducerea, în premieră, a obligației de verificare a necesității stocării datelor la fiecare 5 ani.
- **Statusul procedural:** Proiectul se află în faza incipientă a avizelor, dar beneficiază de un consens politic larg.

4. CONCEPTE ȘI DEFINIȚII (Standard: profunzime și logică) Proiectul introduce termeni care funcționează ca și „containere juridice” ambigue:

- **„Resurse în mediul on-line”:** Sintagmă nedefinită care poate include de la platforme de colectare de date (honeypots) la identități sintetice (agenți AI) pentru operațiuni de influență.
- **Războiul cognitiv:** Trecerea de la controlul informației la controlul modului de gândire prin profilare bazată pe „Fundamente Morale” (MFT).
- **Paternalism epistemic:** Riscul ca statul să devină unicul arbitru al adevărului în încercarea de a contracara dezinformarea.

5. INTERPRETARE ȘI JURISPRUDENȚĂ (Standard: logică) Evaluarea conformității cu standardele Marii Camere a CEDO relevă vulnerabilități majore:

- **Standardul *Big Brother Watch*:** CEDO cere autorizare independentă (judecătorească) pentru colectarea masivă de date, cerință ignorată de PI-x 565, unde decizia rămâne internă serviciului.
- **Standardul *Rotaru*:** Deși introduce limite temporale, legea nu definește criteriile precise prin care o persoană este inclusă în sistemele de evidență.
- **Controlul Efectiv:** Mecanismul de recurs la comisiile parlamentare este considerat formal și ineficient, deoarece acestea nu pot dispune ștergerea datelor sau sancțiuni directe.

6. IMPLICAȚII ȘI CONSECINȚE (Standard: amploare)

- **Asupra drepturilor civile:** Risc de „fishing expeditions" prin interconectarea bazelor de date și normalizarea supravegherii vieții digitale cotidiene.
- **Constituționale:** Probabilitate ridicată de invalidare la CCR pentru lipsă de claritate și proporționalitate.
- **De securitate:** Creșterea rezilienței în fața atacurilor cibernetice prin capacități de tip „defend forward".

7. TABEL DE SINTEZĂ: CONFORMITATE CEDO

Standard CEDO (Cauza)	Cerință Specifică	Soluția în PI-x 565/2025	Nivel Conformitate
Rotaru v. RO	Limite temporale de stocare	Verificare la 5 ani, ștergere la dispariția amenințării	**Ridicat**(Inovație)
Big Brother Watch	Autorizare independentă prealabilă	Inexistentă pentru crearea bazelor de date/resurse	**Scăzut / Critic**
Dumitru Popescu v. RO	Căi de atac efective	Sesizare comisie parlamentară (fără puteri directe)	**Mediu-Scăzut**

8. PUNCT DE VEDERE ȘI RECOMANDĂRI Proiectul reprezintă un compromis imperfect între necesitatea modernizării tehnice și rigoarea juridică europeană. Deși „blindajul juridic" este superior legislației actuale, el prezintă fisuri structurale la capitolul control independent.

Recomandări:

- **Amendament critic:** Introducerea obligativității unui mandat judecătoresc specific emis de Înalta Curte de Casație și Justiție

pentru *crearea* oricărei baze de date sistemice sau resurse online majore.
- **Clarificarea definițiilor:** Definirea strictă a „resurselor on-line” pentru a exclude utilizarea acestora în scopuri de manipulare a opiniei publice.
- **Expertiză tehnică:** Dotarea comisiilor parlamentare cu un corp de experți independenți pentru a audita algoritmii de profilare utilizați

PARTEA II: Tehnici globale de manipulare cognitivă vs. PL-X 565/2025

Această analiză comparativă examinează intersecția dintre tehnicile globale de manipulare cognitivă și modificările legislative propuse în România prin inițiativa PL-X 565/2025.

Concluzia directă este că arhitectura legală propusă în PL-X 565/2025 este perfect compatibilă și necesară pentru implementarea tehnicilor de micro-targetare avansată și război cognitiv. Legea pare să fi fost desenată pentru a oferi acoperire legală infrastructurii de date necesare acestor operațiuni.

Iată analiza detaliată:

1. De ce date au nevoie tehnicile globale de manipulare vs. Ce oferă legea

Pentru a rula sistemele de Mașină de Manipulare (AI Agentic) și Profilare Psihografică (MFT), operatorii au nevoie de trei ingrediente:

1. Acces neîngrădit la fluxuri de date brute (pentru a antrena modelele de profilare).
2. Capacitate de stocare pe termen lung - 5 ani (pentru a construi istoricul comportamental).
3. Libertate de procesare automată (fără mandat judecătoresc individual pentru fiecare algoritm).

Propunerea legislativă din România bifează exact aceste cerințe:

Cerința tehnică (globală)	Soluția legislativă propusă (PL-X 565/2025)
Colectarea datelor comportamentale (amprenta digitală)	Art. 13 lit. e^1: Legalizează dreptul de a „crea, dezvolta, administra și utiliza... aplicații și alte resurse în mediul on-line”. Sintagma „alte resurse” este suficient de vagă pentru a include scraping-ul rețelelor sociale sau cumpărarea de date de la brokeri.
Profilare automată (Inference)	Art. 23^1: Autorizează explicit prelucrarea datelor „prin mijloace automate”. Aceasta este cheia pentru utilizarea AI-ului care deduce personalitatea din metadate fără intervenție umană.
Păstrarea datelor despre „vulnerabilități"	Art. 23^2 lit. f: Datele *nu* se șterg dacă au legătură cu „vulnerabilități”. În micro-targetare, profilul psihologic al unui alegător nevrotic sau temător este exact o „vulnerabilitate” exploatabilă.

2. Analiza calului Troian: conceptele vagi

A. „Resurse în mediul on-line” = Infrastructură de tip „Bot Farm”?

Termenul „administrarea de resurse în mediul on-line” (Art. 13) permite serviciilor nu doar să *citească* internetul, ci să *scrie* în el.

- Tehnica globală: Rețelele „Pravda” sau „Patriot Democracy” administrează mii de pagini web și conturi false.
- Legea românească: Dacă un serviciu de informații creează o rețea de site-uri de „știri” pentru a colecta date despre cititori (honeypot) sau pentru a testa mesaje psihografice, aceasta poate fi clasificată legal ca o „resursă on-line administrată pentru securitatea națională”. Legea ar legaliza, practic, operațiunile de tip astrotufing intern.

B. „Cunoașterea incidentală” și șantajul cognitiv

Tehnicile de război cognitiv se bazează pe identificarea pârghiilor emoționale (secrete rușinoase, frici, orientări sexuale ascunse).

- Legea: Art. 23^2 permite păstrarea datelor despre „viața intimă” cunoscute incidental, dacă acestea constituie o „vulnerabilitate”.
- Aplicabilitatea: Un algoritm AI poate stabili că un politician sau un jurnalist are o „vulnerabilitate” (ex: datorii la jocuri de noroc, identificate prin monitorizare online). Legea permite stocarea acestui profil pe termen nedefinit sub pretextul că persoana este „șantajabilă”, dar în

realitate, datele pot fi folosite pentru a micro-targeta acea persoană sau pentru a o neutraliza.

3. De ce este mecanismul de control „inutil” în fața AI-ului?

„SRI poate refuza să furnizeze Comisiei date despre metodele și mijloacele specifice” (Art. 23^6). În contextul AI-ului Generativ, acest lucru face controlul imposibil:

- Dacă un cetățean este targetat cu un mesaj manipulat (deepfake audio sau text generat de AI), serviciul poate susține că mesajul a fost generat de un „mijloc specific” (algoritmul AI clasificat) pe baza unor date obținute din „resurse online” (open source).
- Comisia parlamentară nu ar avea acces nici la algoritm (fiind „metodă”), nici la datele brute (fiind „siguranță națională”).

4. Concluzie: legea ca potențial de infrastructură pentru distorsionarea realității

Legea pare a fi o încercare de a moderniza capacitatea de supraveghere pentru a ține pasul cu tehnologia, dar fără a moderniza și garanțiile democratice.

- Ce date sunt necesare pentru distorsionarea realității? Date comportamentale granulare (ce faci online, cu cine vorbești, ce citești) pentru a alimenta algoritmii de profilare MFT (Moral Foundations Theory).
- Face legea posibila obținerea acestor date? Da. Prin legalizarea „mijloacelor automate” și a „bazelor de date” fără a defini limitativ sursele (input-ul), legea are potențial sa transforme serviciile de informații în brokeri de date cu puteri depline, capabili să stocheze profilul psihografic al întregii populații sub umbrela largă a „securității naționale”.

Surse:

https://www.pnas.org/doi/10.1073/pnas.2216261120
https://www.mdpi.com/2227-7390/12/13/2121
https://pmc.ncbi.nlm.nih.gov/articles/PMC10849795/
https://pmc.ncbi.nlm.nih.gov/articles/PMC12522429/
https://academic.oup.com/pnasnexus/article/3/2/pgae035/7591134
https://www.zerohedge.com/ai/new-mind-reading-ai-predicts-what-humans-will-do-next
https://gijn.org/resource/tipsheet-investigating-ai-audio-deepfakes/
https://workshop-proceedings.icwsm.org/pdf/2024_67.pdf

https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/
https://www.newsguardtech.com/special-reports/moscow-based-global-news-network-infected-western-artificial-intelligence-russian-propaganda/
https://pmc.ncbi.nlm.nih.gov/articles/PMC12500826/
https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3853187/cognitive-warfare-the-fight-for-gray-matter-in-the-digital-gray-zone/
https://arxiv.org/html/2506.06299v3

Document elaborat de: Manuela Boldisor-Buta, Expert Educație