09 Aprilie 2026

RAPORT DE ANALIZĂ ȘI EVALUARE A AVIZULUI DEPARTAMENTULUI SECURITĂȚII NAȚIONALE (DSN) ASUPRA PROIECTULUI Pl-x nr. 565/2025

Rezumat executiv: Acest raport analizează avizul Departamentului Securității Naționale (DSN) aferent proiectului Pl-x nr.565/2025.

Evaluarea prin prisma cadrului Paul-Elder demonstrează că propunerile înaintate suferă de deficiențe majore de acuratețe juridică și echitate democratică. Propunerea de a utiliza operatori privați ca persoane împuternicite și de a omite informarea persoanei vizate reprezintă un blindaj juridic pentru capacități avansate de război cognitiv, nu o aliniere reală la standardele CEDO.

*· **Acuratețe**: Justificările DSN distorsionează sensul cauzelor CEDO (Rotaru, Big Brother Watch) și al Articolului 23 GDPR pentru a valida un regim de supraveghere opac și discreționar.*

*· **Echitate**: Interesul cetățeanului la intimitate și la o realitate factuală nepoluată este complet subordonat nevoilor operative ale serviciilor, creând o asimetrie de putere specifică regimurilor iliberale.*

*· **Riscuri**: Se trece de la riscul de abuz individual la **riscul de manipulare sistemică a populației** prin profilare psihografică automată și administrare de resurse online clandestine.*

CUPRINS

1. Standardul Paul-Elder al acurateței

În cadrul sistemului critic Paul-Elder, acuratețea reprezintă imperativul ca orice afirmație să fie verificabilă, precisă și susținută de fapte incontestabile. Avizul DSN pretinde a fi un instrument de „armonizare a regimului protecției datelor cu caracter personal cu cerințele CEDO". Totuși, o examinare riguroasă a justificărilor prezentate de DSN evidențiază o distorsiune semantică între obiectivele declarate și mecanismele procedurale propuse.

Incongruența cu standardele Big Brother Watch și Rotaru

Afirmația DSN conform căreia proiectul „creează condițiile pentru asigurarea securității naționale" în conformitate cu standardele europene este pusă sub semnul întrebării de jurisprudența Marii Camere a CEDO în cauza Big Brother Watch v. UK. Standardul european impune ca orice regim de colectare masivă de date să beneficieze de o autorizare independentă, preferabil judecătorească, anterioară momentului colectării. Proiectul de lege abilitează serviciile de informații să creeze și să administreze „resurse în mediul on-line" și baze de date fără a menționa necesitatea unui mandat judecătoresc prealabil pentru însăși arhitectura acestor sisteme.

Mai mult, DSN justifică necesitatea modificărilor prin cauzele Rotaru v. România și Bucur și Toma v. România. Însă, în cauza Rotaru, Curtea a sancționat statul român tocmai pentru absența unor norme clare privind stocarea informațiilor și lipsa unui control eficient asupra modului în care serviciile gestionează aceste date. Propunerea DSN de a utiliza operatori privați ca „persoane împuternicite" riscă să adâncească această lipsă de claritate, creând un strat suplimentar de opacitate între stat și cetățean, unde datele sunt procesate în afara controlului public direct, sub umbrela contractelor comerciale clasificate.

Interpretarea restrictivă a Articolului 23 GDPR

DSN invocă Articolul 23 din Regulamentul GDPR pentru a susține că excepțiile de securitate națională se aplică și persoanelor împuternicite de operator. Deși din punct de vedere tehnic afirmația este corectă în litera regulamentului, acuratețea aplicării sale în contextul acestei propuneri de lege este viciată de ignorarea principiului proporționalității. Articolul 23 GDPR stipulează că orice restricție trebuie să „respecte esența drepturilor și libertăților fundamentale și să constituie o măsură necesară și proporțională într-o societate democratică".

Propunerea DSN de a permite autorităților să „omită furnizarea datelor persoanei vizate" anulează tocmai această esență a dreptului. Fără informare, cetățeanul este privat de posibilitatea de a contesta eroarea sau abuzul, transformând dreptul la justiție într-o formă fără fond. Astfel, justificarea DSN

suferă de o lipsă de acuratețe sistemică: pretinde că implementează o protecție, în timp ce furnizează instrumentele pentru a o ocoli.

2. Echitatea și dezechilibrul de putere: securitatea națională vs. cetățean

Standardul echității în gândirea critică Paul-Elder impune luarea în considerare a tuturor perspectivelor relevante într-o manieră imparțială. Avizul DSN prezintă o viziune unilaterală, în care nevoile operative ale instituțiilor de forță primează în fața oricărei alte considerații constituționale.

Perspectiva securității naționale ca imperativ absolut

Departamentul Securității Naționale argumentează că „evoluțiile tehnologice actuale... au condus la apariția unor instrumente specifice de administrare în mediul online a unor baze de date... gestionate exclusiv la nivelul unor operatori privați". Această perspectivă vede datele cetățenilor nu ca pe un drept inalienabil, ci ca pe o resursă strategică ce trebuie capturată și utilizată pentru a asigura reziliența statului în fața amenințărilor hibride.

Echitatea ar fi cerut o analiză a modului în care această colectare afectează încrederea publică și integritatea spațiului digital. În schimb, DSN propune ca statul să poată inițiа raporturi juridice cu acești operatori, transformându-i în „persoane împuternicite" care prelucrează date sub instrucțiuni clasificate. Din perspectiva echității, aceasta creează o asimetrie informațională masivă: statul are acces la amprenta digitală a individului, în timp ce individul nu are nicio pârghie pentru a monitoriza statul.

Paternalismul epistemic și riscul suveranității individului

Analiza noastră inițială avertizează asupra paternalismului epistemic, fenomenul prin care statul devine singurul arbitru al adevărului în încercarea de a contracara dezinformarea. Propunerea DSN de a legaliza administrarea de resurse în mediul on-line oferă acoperire legală pentru ceea ce în termeni tehnici se numește „astroturfing" intern sau crearea de „honeypots" informaționale.
Dacă un serviciu de informații administrează o rețea de site-uri de știri pentru a colecta date despre cititori sau pentru a testa mesaje psihografice, se încalcă principiul echității democratice. Cetățeanul este tratat ca un subiect de experiment social, nu ca un actor suveran. Acest model de securitate prin

manipulare transformă mediul online dintr-un spațiu al dezbaterii într-un laborator de condiționare comportamentală.

3. Operatorii privați ca „persoane împuternicite”: privatizarea supravegherii

Una dintre cele mai semnificative propuneri ale DSN este modificarea pentru a include „persoanele împuternicite". Această schimbare nu este doar una terminologică, ci una structurală, cu implicații profunde asupra modului în care statul accesează viața privată.

Mecanismul cooptării și diluarea răspunderii

Prin definirea operatorilor privați ca persoane împuternicite, statul român creează o punte legală prin care poate externaliza colectarea și procesarea de date sensibile. Într-un raport juridic de tip operator (serviciu de informații) - persoană împuternicită (firmă privată), responsabilitatea principală privind legalitatea rămâne la operator, însă persoana împuternicită acționează sub paravanul secretului de stat.

Riscurile nou create prin această propunere includ:

- **Accesul la date comerciale fără mandat judecătoresc individual:** Serviciile pot accesa baze de date comerciale masive (de la furnizori de servicii internet, platforme de e-commerce sau brokeri de date) pretinzând că acestea sunt resurse necesare securității naționale.
- **Utilizarea infrastructurii private pentru operațiuni clandestine:** Operatorii privați pot fi folosiți pentru a găzdui aplicații sau „resurse online” fără ca utilizatorii să suspecteze implicarea statului, ocolind astfel mecanismele de auditare publică aplicabile instituțiilor guvernamentale.
- **Imunitatea contractuală:** Acești operatori privați pot dispune măsura amânării sau omiterii furnizării datelor persoanei vizate, ceea ce înseamnă că cetățeanul nu va ști niciodată că firma căreia i-a încredințat datele acționează de fapt ca un agent al serviciilor de informații.

Șantajul cognitiv și vulnerabilitățile individuale

Raportul nostru inițial subliniază că propunerea de lege permite păstrarea datelor despre viața intimă dacă acestea constituie o vulnerabilitate. În contextul utilizării operatorilor privați, riscul de șantaj cognitiv devine sistemic. Datele colectate incidental (conversații private, istoric de căutare, orientări sexuale sau politice) pot fi stocate pe termen de 5 ani sau mai mult sub pretextul că persoana vizată este șantajabilă.

În realitate, aceste date devin pârghii de influență. Dacă un algoritm AI determină că un jurnalist sau un politician are o vulnerabilitate psihologică (ex: o adicție ascunsă identificată prin monitorizarea plăților online), statul poate folosi această informație pentru a neutraliza această persoană. Propunerea DSN oferă infrastructura perfectă pentru acest tip de sabotaj cognitiv, mutând prelucrarea datelor în zona gri a operatorilor privați împuterniciți.

4. Limitarea informării persoanei vizate vs DPRC din SUA

O altă dimensiune critică a Avizului DSN vizează modificarea articolului care reglementează dreptul persoanei vizate de a fi informată despre prelucrarea datelor sale. DSN propune un mecanism în trei părți de limitare a acestui drept: amânarea, restricționarea și omiterea furnizării de informații.

Conform jurisprudenței Big Brother Watch, notificarea persoanei supravegheate este o garanție esențială care trebuie implementată de îndată ce acest lucru nu mai periclitează scopul supravegherii. Propunerea DSN de a permite omiterea informării atunci când simpla informare este de natură să afecteze activitatea de securitate națională riscă să transforme excepția în regulă.

În analiza Paul-Elder, acest lucru reprezintă o problemă de amploare și echitate. DSN acordă autorității puterea discreționară de a decide dacă un cetățean va afla vreodată că datele sale au fost prelucrate, fără a institui un mecanism de revizuire independentă a acestei decizii. Mai mult, amânarea pe o perioadă de un an, deși pare o limită temporală clară, poate fi prelungită în interiorul acestui termen, creând un potențial de tăcere perpetuă administrativă.

Această arhitectură a notificării opace este extrem de similară cu mecanismele DPRC din SUA, care au fost criticate de Comitetul European pentru Protecția Datelor (European Data Protection Board - EDPB) pentru lipsa de claritate sau a posibilității de contestare.

Cea mai contestată caracteristică a DPRC, care este foarte similară cu propunerile de omitere a informării din avizul DSN, este standardul de notificare către reclamant. În cadrul DPRC, indiferent dacă o încălcare a fost identificată sau nu, persoana vizată primește un răspuns invariabil: revizuirea fie nu a identificat nicio încălcare acoperită, fie DPRC a emis determinări care necesită remedierea corespunzătoare.

Din perspectiva dreptului european la un remediu eficient, această metodă constituie o barieră majoră. Reclamantul nu află niciodată dacă a fost sub supraveghere, ce date au fost colectate sau dacă remedierea dispusă a fost efectiv implementată. Această opacitate structurală este unul dintre motivele

principale ale criticii constante venite din partea autorităților europene de protecție a datelor.

1. Amânarea furnizării informațiilor

Măsura amânării este concepută ca o soluție temporară, aplicabilă atunci când condițiile care fac comunicarea imposibilă sunt limitate în timp.

Mecanism și justificare: Autoritățile sau persoanele împuternicite pot decide suspendarea accesului dacă această acțiune este considerată necesară și proporțională pentru protejarea securității naționale.

Limite Temporale: Amânarea nu poate depăși un an, deși poate fi prelungită în interiorul acestui termen. La expirarea perioadei, informațiile trebuie transmise persoanei vizate.

Critică: În contextul războiului cognitiv, amânarea de un an poate fi critică. Aceasta permite serviciilor să finalizeze operațiuni de influență sau de profilare fără ca subiecții să poată contesta legalitatea colectării datelor în fereastra de oportunitate tactică a operațiunii.

2. Restricționarea furnizării informațiilor

Această măsură intervine atunci când condițiile care împiedică comunicarea nu sunt limitate în timp, sugerând o stare de necesitate prelungită.

Mecanism: În loc de datele brute sau confirmarea procesării, autoritatea transmite un răspuns a cărui formă și conținut sunt stabilite individual de fiecare instituție.

Critică: Persoana vizată primește un document care, cel mai probabil, va fi evaziv. Această formă de restricție amintește de sistemul de răspunsuri standardizate din sistemul american, unde substanța este sacrificată în favoarea formei administrative.

3. Omisiunea furnizării informațiilor

Măsura omisiunii este cea mai radicală intervenție asupra dreptului persoanei vizate, fiind utilizată atunci când simpla informare este de natură să afecteze activitatea de securitate națională.

Mecanism: Statul alege să nu confirme în niciun fel existența prelucrării datelor. Similar restricționării, se poate transmite un răspuns neutru.

Critică: Această măsură golește de conținut dreptul la un remediu eficient, deoarece persoana vizată nu are niciun punct de sprijin pentru a iniția o acțiune în instanță.

Critica Uniunii Europene

Poziția Uniunii Europene față de aceste mecanisme este marcată de un scepticism profund.

În Opinia 5/2023, EDPB a salutat introducerea principiilor de necesitate și proporționalitate, dar a criticat faptul că acestea sunt definite prin prisma dreptului american, nu a celui european. Principalele puncte de critică includ:

Absența autorizării prealabile independente: Atât în sistemul SUA, cât și în propunerea PI-x 565, colectarea masivă nu este supusă unei autorizări prealabile din partea unei autorități administrative sau judiciare independente.

Eficacitatea remediului: EDPB a exprimat îndoieli că mecanismul DPRC oferă o protecție reală atâta timp cât reclamantul nu are acces la dosar și primește un răspuns standardizat.

Profilarea și deciziile automate: Critica UE subliniază lipsa unor reguli specifice pentru deciziile luate prin mijloace automate, o problemă majoră având în vedere că PI-x 565 legalizează explicit „mijloacele automate” pentru procesarea datelor.

5. Războiul Cognitiv

Analiza noastră inițială arată că arhitectura propusă este perfect compatibilă cu implementarea Mașinii de manipulare (AI Agentic).

Pentru a rula sisteme eficiente de micro-targetare, operatorii au nevoie de trei elemente, toate furnizate de varianta susținută de DSN:

1. **Acces neîngrădit la fluxuri de date brute:** Legalizat prin „alte resurse în mediul on-line” și utilizarea persoanelor împuternicite.

2. **Capacitate de stocare pe termen lung:** Propunerea de lege permite păstrarea datelor timp de 5 ani, perioadă ideală pentru a construi un istoric comportamental detaliat și a identifica axele morale dominante ale individului conform Teoriei fundamentelor morale (MFT).

3. **Libertate de procesare automată:** Propunerea de lege autorizează explicit prelucrarea prin „mijloace automate”, ceea ce permite utilizarea LLM-urilor (Large Language Models) pentru a deduce personalitatea din metadate fără intervenție umană.

Riscul de otrăvire a fântânii informaționale

Un risc major identificat în contextul internațional (cazul rețelei pro-Kremlin Pravda) este infiltrarea narativelor false în seturile de date de antrenament ale modelelor AI. Prin abilitatea serviciilor românești de a crea și administra „resurse online” fără supraveghere independentă, apare riscul ca statul să devină el însuși un generator de conținut sintetic.

Acest conținut poate fi indexat de motoarele de căutare și chatbot-urile comerciale, devenind parte din adevărul algoritmic. Dacă DSN propune ca aceste activități să fie desfășurate prin „persoane împuternicite” (operatori privați), procesul devine și mai greu de detectat. Rezultatul este o distorsiune fundamentală a realității obiective: cetățeanul caută informații neutre, dar primește un răspuns generat de un AI antrenat pe date produse de o resursă online administrată de un serviciu de informații, fără ca cetățeanul să fie informat despre această prelucrare.

6. Critica Ministerului Justiției

Avizul DSN include punctele de vedere ale Ministerului Justiției, care confirmă îngrijorările legate de lipsa de claritate și proporționalitate a proiectului.

Ministerul Justiției subliniază că sintagma „alte resurse în mediul on-line” este neclară și că nu se poate deduce la ce se referă. Din perspectiva Paul-Elder, această lipsă de precizie invalidează calitatea legii. O lege imprecisă este un cec în alb acordat puterii executive.

Ministerul Justiției invocă Decizia CCR care a stabilit că accesul la datele de comunicații trebuie supus autorizării prealabile a unui judecător. Proiectul acesta împreună cu propunerile DSN, ignoră această cerință pentru baze de date și resurse online, lăsând decizia exclusiv la nivelul autorităților de securitate.

Acest contrast este izbitor: în timp ce organele de urmărire penală au nevoie de mandat pentru a intercepta un singur suspect, organele de securitate națională

ar putea, sub noua lege, să creeze o infrastructură care monitorizează întreaga populație digitală fără niciun control judiciar prealabil.

Propunerea DSN de a utiliza operatori privați adâncește acest abuz, deoarece creează un circuit paralel de date care nu intră niciodată sub ochii magistraților.

7. Contrastul dintre securitatea națională și drepturile individuale

Pentru a evalua impactul global al propunerilor DSN, trebuie puse în contrast valorile fundamentale aflate în conflict.

Perspectiva securității naționale

În viziunea DSN, spațiul digital este un câmp de luptă unde statul trebuie să aibă libertate totală de acțiune pentru a preveni colapsul moral al populației sau atacurile hibride.
Securitatea colectivă este premisa libertății individuale. Prin urmare, drepturile individuale pot fi suspendate temporar sau omise dacă acest lucru servește obiectivului strategic de supraveghere totală a vulnerabilităților.
Utilizarea operatorilor privați este văzută ca o optimizare tehnică, o modalitate de a ține pasul cu oponentul (ex. rețelele rusești sau chinezești) care folosește deja aceste metode.

Perspectiva suveranității cetățeanului

În viziunea drepturilor omului, securitatea nu poate exista fără libertate. Orice ingerință în viața privată trebuie să fie excepțională, limitată în timp și sub control judiciar strict.
O populație supravegheată și manipulată nu mai este una democratică.
Distrugerea democrației sub pretextul apărării ei este riscul suprem.
Informarea persoanei vizate este singura garanție că cetățeanul rămâne un subiect de drept.

8. Riscuri noi și aprofundate prin propunerile DSN

Propunerile DSN nu doar că validează riscurile semnalate anterior, ci introduc vulnerabilități de securitate națională pe termen lung sub masca eficienței operative.

Riscuri aprofundate

Normalizarea supravegherii: Prin utilizarea persoanelor împuternicite (operatori privați), colectarea de date devine invizibilă și cvasi-permanentă. Nu mai vorbim de interceptarea unui risc, ci de monitorizarea constantă a comportamentului digital pentru a identifica vulnerabilități psihografice.

Erodarea căilor de atac efective: Dacă amânarea informării poate fi prelungită în interiorul unui an, dar omiterea informării este permisă atunci când informarea ar afecta activitatea, se instalează un regim de secret absolut care anulează orice control judiciar ulterior.

Riscuri noi

Riscul de sabotaj cognitiv prin proxy privat: Statul român devine vulnerabil la infiltrări în cadrul operatorilor privați împuterniciți. Dacă o firmă privată acționează ca persoană împuternicită a serviciilor, ea devine o țintă de spionaj industrial și politic de prim rang. Compromiterea acelei firme înseamnă compromiterea infrastructurii de securitate a statului.

Fragmentarea realității sociale (Splinternet-ul adevărului): Prin administrarea de resurse online nesupravegheate, statul poate fractura consensul social în tunele de realitate, creând realități paralele pentru segmente diferite de public (MFT reframing). Aceasta duce la polarizarea extremă a societății, erodând chiar reziliența pe care legea pretinde că o apără.

Transferul de date către state terțe sub umbrela „persoanelor împuternicite”: propunerea de lege permite transferul de date către alte autorități publice sau entități. Propunerea DSN de a include operatorii privați ar putea facilita transferul de date sensibile către parteneri externi (intelligence sharing) fără nicio urmă de autorizare judiciară, folosind circuitele comerciale ale persoanelor împuternicite.

9. Concluzii și recomandări

Analiza Avizului Departamentului Securității Naționale aferent proiectului PL-x nr. 565 prin prisma cadrului Paul-Elder demonstrează că propunerile înaintate suferă de deficiențe majore de acuratețe juridică și echitate democratică. Propunerea de a utiliza operatori privați ca persoane împuternicite și de a omite

informarea persoanei vizate reprezintă un blindaj juridic pentru capacități avansate de război cognitiv, nu o aliniere reală la standardele CEDO.

Sinteza evaluării

Acuratețe: Justificările DSN distorsionează sensul cauzelor CEDO (Rotaru, Big Brother Watch) și al Articolului 23 GDPR pentru a valida un regim de supraveghere opac și discreționar.
Echitate: Interesul cetățeanului la intimitate și la o realitate factuală nepoluată este complet subordonat nevoilor operative ale serviciilor, creând o asimetrie de putere specifică regimurilor iliberale.
Riscuri: Se trece de la riscul de abuz individual la riscul de manipulare sistemică a populației prin profilare psihografică automată și administrare de resurse online clandestine.

Recomandări strategice

Mandatul judecătoresc prealabil pentru infrastructură: Nicio bază de date sistemică sau „resursă online" majoră administrată de serviciile de informații (direct sau prin împuterniciți) nu ar trebui creată fără un mandat emis de Înalta Curte de Casație și Justiție, care să auditeze algoritmii și scopul colectării.

Eliminarea conceptului de omitere a informării: Legislația trebuie să prevadă doar amânarea informării, cu un termen maxim absolut, după care cetățeanul să fie notificat obligatoriu. Dreptul la justiție nu poate exista în absența cunoașterii actului de prelucrare.

Transparența algoritmică și auditul societății civile: Comisiile parlamentare de control trebuie să aibă acces la metodele și mijloacele care implică inteligență artificială generativă sau profilare psihografică, sub asistența unor experți independenți, pentru a preveni transformarea statului într-o mașină de manipulare.

Definirea strictă a „resurselor online": Această sintagmă trebuie limitată la paginile oficiale și la infrastructura tehnică de comunicații, excluzând explicit posibilitatea administrării unor site-uri de conținut (știri, forumuri) sub identități false sau sintetice.

Proiectul PL-x nr.565, în forma susținută de DSN, reprezintă o încercare de a codifica superioritatea mentală a statului asupra cetățeanului. Pentru a asigura o securitate națională reală, România trebuie să construiască reziliență prin transparență și respectarea suveranității epistemice a fiecărui individ, nu prin arhitecturi de supraveghere invizibilă care otrăvesc însuși fundamentul

încrederii sociale. Securitatea nu poate fi durabilă dacă prețul ei este sacrificarea discernământului propriului electorat.

Surse:

https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}
https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1228990
https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court
https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}
https://gdpr-info.eu/art-23-gdpr/
https://www.workforcebulletin.com/adequacy-of-the-eu-u-s-data-privacy-framework-survives-challenge
https://www.crowell.com/en/insights/client-alerts/the-edpbs-opinion-on-eu-us-data-privacy-framework

Document elaborat de: Manuela Boldisor-Buta, Expert Educație