PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAŢILOR **SENATUL ROMÂNIEI**

LEGE
privind consolidarea controlului asupra datelor din sistemele publice şi protecţia acestora în mediile de cloud şi inteligenţă artificială

Parlamentul României adoptă prezenta lege

CAPITOLUL I – Dispoziţii generale

Art. 1. – Obiect şi scop

(1) Prezenta lege instituie măsuri de guvernanţă, evaluare a riscurilor, securitate şi transparenţă pentru prelucrarea datelor în sistemele informatice ale autorităţilor şi instituţiilor publice din România, inclusiv în servicii de cloud şi în sisteme de inteligenţă artificială.

(2) Scopul legii este reducerea dependenţelor tehnologice critice, prevenirea accesului neautorizat, asigurarea continuităţii serviciilor publice şi facilitarea exercitării drepturilor persoanelor vizate, inclusiv ale cetăţenilor români din străinătate.

(3) Prezenta lege se aplică fără a aduce atingere Regulamentului (UE) 2016/679, liberei circulaţii a datelor în Uniunea Europeană, legislaţiei privind securitatea cibernetică, achiziţiile publice, informaţiile clasificate şi regimurilor sectoriale speciale.

Art. 2. – Domeniul de aplicare

(1) Legea se aplică autorităţilor şi instituţiilor publice care stabilesc scopurile şi mijloacele prelucrării datelor prin sisteme informatice proprii sau contractate.

(2) Obligaţiile furnizorilor privaţi decurg din clauzele contractelor încheiate cu entităţile prevăzute la alin. (1), fără instituirea unei obligaţii generale de localizare a datelor tuturor operatorilor economici.

(3) Prelucrările efectuate în scopul prevenirii, cercetării şi urmăririi penale, cele privind securitatea naţională şi informaţiile clasificate rămân supuse regimurilor juridice speciale aplicabile.

Art. 3. – Definiţii

În sensul prezentei legi:

a) sistem critic de date publice – sistem a cărui indisponibilitate, compromitere sau divulgare poate produce un impact grav asupra funcțiilor publice esențiale, stabilit prin evaluarea prevăzută la art.5;

b) furnizor de cloud – prestatorul serviciilor de prelucrare a datelor astfel cum este definit de dreptul Uniunii Europene;

c) acces extraterritorial – solicitare de divulgare sau acces la date formulată în temeiul dreptului unui stat terț;

d) portabilitate tehnică – posibilitatea de export și migrare a datelor și sarcinilor informatice în condițiile legislației europene aplicabile.

CAPITOLUL II – Evaluarea riscurilor și garanții de securitate

Art. 4. – Principii

(1) Măsurile se întemeiază pe legalitate, necesitate, proporționalitate, neutralitate tehnologică, concurență loială, minimizarea datelor și securitate demonstrabilă.

(2) Cetățenia persoanei vizate nu poate constitui, singură, criteriu pentru restrângerea drepturilor acordate de legislația europeană în materia protecției datelor.

Art. 5. – Evaluarea sistemelor critice

(1) Fiecare autoritate publică realizează și actualizează cel puțin o dată la doi ani o evaluare documentată a riscurilor pentru sistemele care prelucrează date personale ori asigură servicii publice esențiale.

(2) Evaluarea are în vedere natura și volumul datelor, categoriile de persoane vizate, continuitatea serviciului, dependența de furnizor, accesul administratorilor și subcontractanților, legislațiile statelor terțe relevante și posibilitățile de migrare.

(3) Clasificarea unui sistem ca fiind critic se motivează individual; nu rezultă automat din simpla apartenență a datelor la o categorie administrativă.

(4) Evaluarea prevăzută de prezentul articol nu înlocuiește evaluarea de impact asupra protecției datelor, atunci când aceasta este obligatorie potrivit art.35 din Regulamentul (UE) 2016/679.

Art. 6. – Cerințe minime pentru contractare

(1) În contractele privind sisteme critice, autoritățile prevăd, proporțional cu riscurile: criptare adecvată, controlul accesului, jurnalizare, copii de siguranță, planuri de continuitate, notificarea incidentelor, drepturi de audit, evidența subcontractanților și plan de ieșire din contract.

(2) Contractele stabilesc în mod explicit regiunile de prelucrare, condițiile accesului de la distanță, responsabilitățile privind cheile criptografice și procedura de returnare sau ștergere verificabilă a datelor.

(3) Cerințele tehnice se formulează prin standarde ori performanțe verificabile, cu acceptarea mijloacelor echivalente de probă, în condițiile legii.

Art. 7. – Localizarea și accesul la date

(1) Nu se instituie prin prezenta lege o obligație generală de stocare exclusivă a datelor pe teritoriul României.

(2) Pentru sistemele critice, autoritatea poate impune, prin documentația de atribuire și cu justificare individuală, măsuri de rezidență a datelor sau de administrare a cheilor în Uniunea Europeană ori în Spațiul Economic European, numai dacă acestea sunt necesare și proporționale cu riscurile identificate și compatibile cu dreptul Uniunii.

(3) O cerință de localizare exclusiv pe teritoriul României se poate stabili numai atunci când un temei legal special și o justificare obiectivă o permit, cu respectarea dreptului Uniunii.

Art. 8. – Solicitările autorităților statelor terțe

(1) Furnizorul informează fără întârziere autoritatea contractantă despre solicitările de acces formulate de autorități ale statelor terțe, în măsura permisă de lege.

(2) Divulgarea datelor cu caracter personal către autorități ale statelor terțe se efectuează numai în condițiile capitolului V din Regulamentul (UE) 2016/679, inclusiv ale art. 48, și ale celorlalte dispoziții aplicabile.

(3) Prezenta lege nu instituie o autorizare generală prealabilă a transferurilor de către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în afara cazurilor prevăzute expres de dreptul aplicabil.

Art. 9. – Incidente și raportare

(1) Entitățile supuse legislației privind securitatea cibernetică și protecția datelor respectă termenele, destinatarii și condițiile de notificare prevăzute de actele aplicabile fiecărui incident.

(2) Contractele trebuie să asigure transmiterea rapidă a informațiilor necesare operatorului pentru îndeplinirea obligațiilor sale legale; prezenta lege nu unifică și nu înlocuiește termenele distincte din regimurile GDPR și NIS2.

CAPITOLUL III – Achiziții, interoperabilitate și drepturile persoanelor

Art. 10. – Certificări și evaluări

(1) Autoritățile pot utiliza certificări europene de securitate cibernetică aplicabile, standarde internaționale și rapoarte independente de audit, cu respectarea normelor de achiziții publice.

(2) Nu se instituie o certificare națională obligatorie paralelă schemelor europene și nici condiții de acces pe piață bazate pe naționalitatea ori sediul furnizorului.

(3) În cazul în care sunt cerute certificate, se acceptă documentele echivalente și alte mijloace de probă admise de lege.

Art. 11. – Interoperabilitate și ieșire din contract

(1) Autoritățile publice includ, după caz, cerințe de interoperabilitate, export în formate documentate și migrare în condiții de securitate.

(2) Schimbarea furnizorilor de servicii de prelucrare a datelor respectă Regulamentul (UE) 2023/2854 și regimurile speciale aplicabile; drepturile de schimbare a furnizorului nu se confundă cu dreptul individual la portabilitatea datelor prevăzut de art. 20 GDPR.

Art. 12. – Informarea persoanelor vizate

(1) Autoritățile publică, într-un limbaj clar și accesibil, informații despre categoriile de furnizori, regiunile principale de prelucrare și măsurile generale de protecție, în măsura în care divulgarea nu afectează securitatea sistemelor ori alte interese protejate de lege.

(2) Cererile persoanelor vizate se soluționează potrivit termenelor și limitelor stabilite de Regulamentul (UE) 2016/679.

(3) Prezenta lege nu creează un drept de a dispune transferul unor registre publice ori dosare administrative către un furnizor ales de persoana vizată.

Art. 13. – Accesul cetățenilor din străinătate

(1) Autoritățile competente facilitează accesul electronic al cetățenilor români aflați în străinătate la serviciile publice disponibile legal la distanță, prin mecanisme de identificare și autentificare compatibile cu cadrul european privind identitatea digitală.

(2) Serviciile consulare digitale se dezvoltă în limitele competențelor Ministerului Afacerilor Externe și ale legislației speciale; prezenta lege nu instituie vot electronic și nu modifică procedurile electorale.

(3) Extinderea serviciilor se realizează prioritar prin interoperabilitatea platformelor existente, fără duplicarea registrelor de date.

Art. 14. – Protecția minorilor

(1) Prelucrarea datelor minorilor în sistemele publice se realizează cu garanții sporite, potrivit legislației privind protecția datelor și drepturile copilului.

(2) Datele personale ale minorilor nu pot fi reutilizate pentru antrenarea modelelor de inteligență artificială în lipsa unui temei legal valabil și a garanțiilor corespunzătoare; anonimizarea trebuie să fie efectivă, nu doar declarată.

CAPITOLUL IV – Inteligența artificială și coordonarea instituțională

Art. 15. – Sisteme de inteligență artificială

(1) Înaintea utilizării unui sistem de inteligență artificială care prelucrează date personale în cadrul unui sistem critic, autoritatea documentează temeiul prelucrării, fluxurile de date, accesul furnizorului, riscurile pentru drepturile fundamentale și măsurile de control uman aplicabile.

(2) Se respectă obligațiile prevăzute de Regulamentul (UE) 2024/1689, potrivit calendarului de aplicare efectiv în vigoare, precum și Regulamentul (UE) 2016/679.

(3) Utilizarea datelor în scop de antrenare, ajustare sau inferență se supune principiilor limitării scopului, minimizării și securității.

Art. 16. – Coordonare

(1) Autoritatea pentru Digitalizarea României coordonează elaborarea unor modele orientative de clauze contractuale și a unui ghid de interoperabilitate, în colaborare cu autoritățile competente, în limitele atribuțiilor legale.

(2) Directoratul Național de Securitate Cibernetică participă în limitele competențelor sale privind securitatea cibernetică.

(3) Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal își exercită independent atribuțiile prevăzute de legislația aplicabilă; prezenta lege nu îi conferă sarcini de certificare a furnizorilor de cloud ori de aprobare a fiecărei cereri de acces.

Art. 17. – Raportare

(1) În termen de 18 luni de la intrarea în vigoare, Guvernul prezintă Parlamentului un raport privind riscurile de dependență tehnologică, nivelul de interoperabilitate și măsurile de securitate ale sistemelor publice critice.

(2) Raportul cuprinde o analiză a costurilor și beneficiilor utilizării infrastructurilor existente, inclusiv a cloudului guvernamental, și recomandări privind investițiile viitoare.

CAPITOLUL V – Dispoziții finale

Art. 18. – Răspundere

Încălcarea obligațiilor stabilite prin prezenta lege atrage răspunderea disciplinară, civilă, contravențională sau penală, după caz, potrivit actelor normative aplicabile.

Nu se instituie prin prezenta lege amenzi care dublează sancțiunile prevăzute pentru aceeași faptă de dreptul Uniunii Europene.

Art. 19. – Norme metodologice

În termen de 180 de zile de la intrarea în vigoare, Guvernul aprobă, prin hotărâre, metodologia de evaluare și documentare a riscurilor prevăzută la art.5, după consultarea autorităților competente și a mediului profesional. Metodologia nu poate introduce restricții suplimentare asupra circulației datelor ori condiții de acces pe piață neprevăzute de lege.

Art. 20. – Aplicarea în timp

(1) Obligațiile privind evaluarea riscurilor se îndeplinesc în termen de 12 luni de la intrarea în vigoare.

(2) Cerințele contractuale prevăzute la art.6 și 11 se aplică procedurilor de achiziție inițiate după expirarea termenului prevăzut la alin.(1).

(3) Contractele aflate în derulare se adaptează la reînnoire sau la modificarea legal permisă, fără încălcarea legislației achizițiilor publice.

Art. 21. – Finanțare

Măsurile prevăzute de prezenta lege se realizează în limita creditelor bugetare aprobate anual, cu posibilitatea utilizării fondurilor europene eligibile, potrivit regulilor fiecărui program.

Art. 22. – Intrarea în vigoare

Prezenta lege intră în vigoare la 90 de zile de la publicarea în Monitorul Oficial al României, Partea I.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art.75 şi ale art.76 alin.(1) din Constituţia României, republicată.

PREŞEDINTE	**PREŞEDINTE**
CAMERA DEPUTAŢILOR	**SENATUL ROMÂNIEI**
GRINDEANU SORIN-MIHAI	**ABRUDEAN MIRCEA**