



PROTECȚIA DATELOR CU CARACTER PERSONAL

Protecția datelor cu caracter personal și respectarea vieții private constituie drepturi fundamentale europene. Parlamentul European a insistat întotdeauna asupra necesității de a menține un echilibru între îmbunătățirea securității și protejarea drepturilor omului, inclusiv în ceea ce privește protecția datelor și viața privată. În mai 2018 au intrat în vigoare noi norme ale UE în materie de protecție a datelor, care consolidează drepturile cetățenilor și simplifică normele aplicabile întreprinderilor în era digitală. Cercetările pregătite pentru Parlamentul European indică faptul că legislația UE referitoare la reglementarea fluxurilor de date contribuie anual cu 51,6 miliarde EUR la PIB-ul Uniunii Europene. Cercetările pregătite pentru Comisia de anchetă a Parlamentului European în vederea investigării utilizării Pegasus și a unor programe spion de supraveghere echivalente (Comisia PEGA) confirmă importanța protecției datelor pentru apărarea democrației și a libertăților individuale în UE.

TEMEI JURIDIC

Articolul 16 din Tratatul privind funcționarea Uniunii Europene (TFUE)

Articolele 7 și 8 din Carta drepturilor fundamentale a UE.

OBIECTIVE

Uniunea trebuie să asigure aplicarea consecventă a dreptului fundamental la protecția datelor, care este consacrat în Carta drepturilor fundamentale a UE. Având în vedere creșterea exponențială a volumului transferurilor de date – UE, SUA și Canada reprezentând cea mai mare parte a acestei creșteri – poziția UE privind protecția datelor cu caracter personal trebuie consolidată în contextul tuturor politicilor UE.

REALIZĂRI

A. Cadrul instituțional

1. Tratatul de la Lisabona

Înainte de intrarea în vigoare a Tratatului de la Lisabona, legislația privind protecția datelor în spațiul de libertate, securitate și justiție (SLSJ) a fost împărțită între primul pilon (protecția datelor în scopuri private și comerciale, pentru care era utilizată metoda comunitară) și cel de al treilea pilon (protecția datelor în scopul aplicării legii, la nivel interguvernamental). În consecință, procesele decizionale din cele două domenii au urmat reguli diferite. Structura pe bază de piloni a dispărut odată cu Tratatul de la Lisabona, care consolidează temeiul juridic necesar pentru dezvoltarea unui sistem



mai clar și mai eficace de protecție a datelor și prevede totodată noi competențe pentru Parlament, care devine colegislator. Articolul 16 din TFUE prevede că Parlamentul și Consiliul stabilesc normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organismele, oficiile și agențiile Uniunii, precum și de către statele membre, în exercitarea activităților care fac parte din domeniul de aplicare al dreptului Uniunii.

2. Orientările strategice pentru spațiul de libertate, securitate și justiție

În urma programelor de la Tampere și Haga (din octombrie 1999 și, respectiv, noiembrie 2004), Consiliul European a aprobat, în decembrie 2009, programul multianual privind spațiul de libertate, securitate și justiție (SLSJ) pentru perioada 2010-2014, cunoscut sub numele de „Programul de la Stockholm”. În concluziile sale din iunie 2014, Consiliul European a definit orientările strategice pentru planificarea legislativă și operațională pentru următorii ani în cadrul SLSJ în conformitate cu articolul 68 din TFUE. Unul dintre obiectivele esențiale este o mai bună protecție a datelor personale în UE.

B. Principalele instrumente legislative în materie de protecție a datelor

1. Carta drepturilor fundamentale a UE

Articolele 7 și 8 din Carta drepturilor fundamentale a UE recunosc că respectarea vieții private și protecția datelor cu caracter personal sunt drepturi fundamentale strâns legate, dar separate.

2. Consiliul European

a. Convenția 108 din 1981

Convenția 108 din 28 ianuarie 1981 a Consiliului European pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal a fost primul instrument internațional cu forță juridică obligatorie adoptat în domeniul protecției datelor. Scopul său este de a garanta tuturor persoanelor fizice respectarea drepturilor și libertăților lor fundamentale, și, în special, a dreptului la viața privată, în legătură cu prelucrarea automatizată a datelor cu caracter personal. Protocolul de modificare a convenției urmărește să extindă domeniul său de aplicare, să crească nivelul de protecție a datelor și să-i îmbunătățească eficacitatea.

b. Convenția europeană a drepturilor omului (CEDO)

Articolul 8 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale din 4 noiembrie 1950 stabilește dreptul la respectarea vieții private și a vieții de familie, a căminului și a corespondenței tuturor persoanelor.

3. Actualele instrumente legislative ale UE în vigoare în materie de protecție a datelor

a. Regulamentul general privind protecția datelor (RGPD)

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) a devenit aplicabil în mai 2018. Normele au scopul de a proteja toți cetățenii Uniunii de încălcarea vieții private și a datelor într-o lume care se bazează din ce în ce mai mult pe date, creând



În același timp un cadru mai clar și mai coerent pentru întreprinderi. Noile drepturi de care se bucură cetățenii includ consimțământul clar și afirmativ ca datele lor să fie prelucrate, precum și dreptul de a primi informații clare și ușor de înțeles cu privire la aceasta; dreptul de a fi uitat: un cetățean poate solicita ca datele sale să fie șterse; dreptul de a transfera date către un alt furnizor de servicii (de exemplu atunci când se mută de la o rețea socială la alta); precum și dreptul de a fi înștiințat când datele au fost piratate. Noile norme se aplică tuturor întreprinderilor care își desfășoară activitatea în UE, chiar dacă își au sediul în afara ei. În plus, se pot impune măsuri de remediere, cum ar fi avertismente și ordine, precum și amenzi operatorilor care încalcă normele. La 24 iunie 2020, Comisia Europeană a prezentat un [raport privind evaluarea și revizuirea regulamentului](#)^[1].

b. Directiva privind protecția datelor în materie de asigurare a respectării legii

Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului a devenit aplicabilă în mai 2018. Directiva protejează dreptul fundamental al cetățenilor la protecția datelor în toate cazurile în care autoritățile de aplicare a legii folosesc date cu caracter personal. Directiva garantează că datele cu caracter personal ale victimelor, ale martorilor și ale suspectilor sunt protejate în mod corespunzător și facilitează cooperarea transfrontalieră în domeniul combaterii criminalității și a terorismului. La 25 iulie 2022, Comisia Europeană și-a publicat cu întârziere [raportul referitor la aplicarea și funcționarea Directivei privind protecția datelor în materie de asigurare a respectării legii](#). Aceasta a fost urmată de un [studiu de evaluare](#) comandat de Comisia pentru libertăți civile, justiție și afaceri interne (LIBE) conținând o evaluare critică a punerii în aplicare a Directivei privind protecția datelor în materie de asigurare a respectării legii^[2].

c. Directiva asupra confidențialității și comunicațiilor electronice

[Directiva 2002/58/CE](#) a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) a fost modificată prin [Directiva 2009/136/CE](#) din 25 noiembrie 2009. Aceasta ridică problema delicată a păstrării datelor, care a fost adusă în mod repetat în fața CJUE și care a condus la o serie de hotărâri, cel mai recent în [2020](#), în care se afirmă că dreptul UE se opune păstrării generale și nediferențiate a datelor de transfer și de localizare.

Noua [propunere de regulament](#) din 2017 al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice) se află de multă vreme în discuții. Experții

[1]Comunicarea Comisiei din 24 iunie 2020 intitulată „Protecția datelor ca pilon al capacității cetățenilor și al abordării UE privind tranziția digitală – doi ani de aplicare a Regulamentului general privind protecția datelor” (SWD(2020)0115).

[2]Vogiatzoglou, P. *et al.*, [Assessment of the implementation of the Law Enforcement Directive](#) (Evaluarea punerii în aplicare a Directivei privind asigurarea respectării legii), Parlamentul European, Direcția Generală Politici Interne ale Uniunii, Departamentul tematic pentru drepturile cetățenilor și afaceri constituționale, 7 decembrie 2022.



Parlamentului European au indicat că Parlamentul ar trebui să se opună încercărilor Consiliului de a exclude aplicabilitatea principiilor europene de protecție a datelor^[3].

d. Regulamentul privind prelucrarea datelor cu caracter personal de către instituțiile și organele Uniunii

[Regulamentul \(UE\) 2018/1725](#) al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE a intrat în vigoare la 11 decembrie 2018.

e. Articole privind protecția datelor în acte legislative sectoriale

Pe lângă principalele acte legislative privind protecția datelor menționate mai sus, se stabilesc dispoziții specifice privind protecția datelor și în acte legislative sectoriale, cum ar fi:

- articolul 13 (referitor la protecția datelor personale) din Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave;
- articolul 6 (privind prelucrarea datelor) din [Directiva 2004/82/CE a Consiliului](#) din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii (API);
- la 13 decembrie 2022, Comisia a adoptat [două propuneri legislative](#) privind colectarea și transferul datelor API care vor înlocui API^[4];
- capitolul VI (referitor la garanțiile privind protecția datelor) din Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol);
- capitolul VIII (referitor la protecția datelor) din Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO).

4. Principalele acorduri internaționale ale UE privind transferurile de date

a. Transferuri de date comerciale: decizii privind caracterul adecvat al nivelului de protecție

În temeiul articolului 45 din RGPD, Comisia are competența de a stabili dacă o țară din afara UE oferă un nivel adecvat de protecție a datelor, fie pe baza legislației sale naționale, fie pe baza angajamentelor internaționale pe care și le-a asumat.

[3] Sartor G *et al.*, [The impact of Pegasus on fundamental rights and democratic processes](#) (Impactul Pegasus asupra drepturilor fundamentale și a proceselor democratice), Parlamentul European, Direcția Generală Politici Interne ale Uniunii, Departamentul tematic pentru drepturile cetățenilor și afaceri constituționale, ianuarie 2023, p 56-57.

[4] Vavoula, N. *et al.*, [Advance Passenger Information \(API\) – An analysis of the European Commission's proposals to reform the API legal framework \[Informații prealabile referitoare la pasageri \(API\) - O analiză a propunerilor Comisiei Europene de reformare a cadrului juridic referitor la API\]](#), Parlamentul European, Direcția Generală Politici Interne ale Uniunii, Departamentul tematic pentru drepturile cetățenilor și afaceri constituționale, 8 iunie 2023.



În timp ce transferurile de date între UE și America de Nord au crescut exponențial, SUA dominând publicitatea și supravegherea privată online^[5], Parlamentul a adoptat numeroase rezoluții care ridică semne de întrebare cu privire la fluxurile transatlantice de date. În special, acesta a considerat că Scutul de confidențialitate UE-SUA nu oferă nivelul adecvat de protecție impus de legislația UE, în timp ce CJUE a anulat în mod repetat deciziile privind caracterul adecvat al nivelului de protecție în ceea ce privește SUA (a se vedea hotărârile sale din 2015 privind sfera de siguranță în cauza [Schrems](#) și din 2020 privind Scutul de confidențialitate UE-SUA în cauza [Schrems II](#)).

În pofida lipsei unei reforme a regimului de protecție a datelor în SUA, Comisia Europeană a ajuns la un alt acord cu SUA și a prezentat [o propunere](#) pentru încă un cadru UE-SUA privind confidențialitatea datelor. În urma prezentării unei propuneri a Comisiei LIBE la 11 mai 2023, Parlamentul a adoptat [o rezoluție](#) referitoare la caracterul adecvat al protecției oferite de Cadru UE-SUA privind confidențialitatea datelor, concluzionând că cadrul UE-SUA privind confidențialitatea datelor nu creează echivalența esențială a nivelului de protecție și solicitând Comisiei să continue negocierile cu omologii săi din SUA, dar să se abțină de la adoptarea constatării caracterului adecvat până la punerea în aplicare deplină a tuturor recomandărilor formulate în rezoluția Parlamentului și în avizul Comitetului european pentru protecția datelor (CEPD).

Comisia a adoptat cel de al treilea [Cadru UE-SUA privind confidențialitatea datelor](#) la 10 iulie 2023.

b. Acordul-cadru UE-SUA

În cadrul procedurii de aprobare, Parlamentul a fost implicat în aprobarea acordului dintre SUA și UE privind protecția informațiilor cu caracter personal în ceea ce privește prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor, cunoscut și sub denumirea de „acordul-cadru”. Obiectivul acordului îl constituie asigurarea unui înalt nivel de protecție a informațiilor personale transferate în cadrul cooperării transatlantice în scopul aplicării legii, și anume pentru combaterea terorismului și a criminalității organizate.

c. Acordurile UE-SUA, UE-Australia și UE-Canada privind registrul cu numele pasagerilor (PNR)

Uniunea Europeană a semnat acorduri bilaterale privind registrul cu numele pasagerilor (PNR) cu Statele Unite ale Americii, Australia și Canada. Datele PNR includ informații furnizate de pasageri în momentul rezervării biletelor sau al înregistrării pasagerilor și a bagajelor pentru zbor, precum și datele colectate de transportatorii aerieni în scopuri comerciale proprii. Datele PNR pot fi utilizate de autoritățile de aplicare a legii pentru combaterea formelor grave de criminalitate și a terorismului.

[5]Maciejewski, M., [Metaverse](#), Parlamentul European, Direcția Generală Politici Interne ale Uniunii, Departamentul tematic pentru drepturile cetățenilor și afaceri constituționale, 26 iunie 2023.



d. Programul UE-SUA de urmărire a finanțărilor în scopuri teroriste (TFTP)

Uniunea Europeană a semnat un acord bilateral cu SUA privind prelucrarea și transferul datelor de mesagerie financiară din UE către SUA în scopul programului de urmărire a finanțărilor în scopuri teroriste.

5. Abordarea aspectelor legate de protecția datelor în rezoluții sectoriale specifice
Mai multe rezoluții ale Parlamentului referitoare la diferite domenii de politică abordează, de asemenea, protecția datelor cu caracter personal, pentru a se asigura coerența cu legislația generală a UE privind protecția datelor și protecția vieții private în aceste sectoare specifice.

6. Autoritățile Uniunii de supraveghere în materie de protecție a datelor

[Autoritatea Europeană pentru Protecția Datelor \(AEPD\)](#) este o autoritate de supraveghere independentă care garantează că instituțiile și organele UE își respectă obligațiile în materie de protecție a datelor. Principalele atribuții ale AEPD sunt supravegherea, consultarea și cooperarea.

[Comitetul european pentru protecția datelor \(CEPD\)](#), fostul Grup de lucru „Articolul 29”, are statutul unui organism al Uniunii Europene cu personalitate juridică și dispune de un secretariat independent. CEPD reunește autoritățile naționale de supraveghere ale Uniunii, AEPD și Comisia. CEPD are competențe extinse de a soluționa litigiile dintre autoritățile naționale de supraveghere și de a oferi recomandări și îndrumări cu privire la conceptele cheie din RGPD și din Directiva privind protecția datelor în materie de aplicare a legii.

ROLUL PARLAMENTULUI EUROPEAN

Parlamentul a jucat un rol-cheie în elaborarea legislației Uniunii în domeniul protecției datelor cu caracter personal, introducând protecția vieții private ca o nouă prioritate politică. De asemenea, în cadrul procedurii legislative ordinare, continuă să lucreze la reforma protecției datelor, pe picior de egalitate cu Consiliul. Parlamentul și-a încheiat, în 2017, activitatea legată de ultima piesă importantă din puzzle, și anume noul regulament privind viața privată și comunicațiile electronice, și așteaptă cu interes ca Consiliul să își încheie în sfârșit lucrările pentru a putea începe negocierile.

În numeroase rezoluții, Parlamentul și-a exprimat îndoielile cu privire la caracterul adecvat al protecției acordate cetățenilor UE în contextul Cadrului privind sfera de siguranță UE-SUA și, ulterior, al „Scutului de confidențialitate” UE-SUA. După ce cauza Schrems II a condus la invalidarea [Deciziei de punere în aplicare \(UE\) 2016/1250](#) a Comisiei Europene privind caracterul adecvat al protecției oferite de „Scutul de confidențialitate” UE-SUA, pe baza preocupărilor legate de faptul că competențele de supraveghere ale guvernului SUA nu sunt limitate, astfel cum prevede legislația UE, și de faptul că cetățenii UE nu dispun de căi de atac efective, Parlamentul European a adoptat o rezoluție în care a deplâns faptul că Comisia a plasat relațiile cu SUA înaintea intereselor cetățenilor UE^[6].

[6] [Rezoluția Parlamentului European din 20 mai 2021 referitoare la hotărârea CJUE din 16 iulie 2020 - Comisarul pentru protecția datelor/Facebook Ireland Limited și Maximilian Schrems \(„Schrems II”\), Cauza C-311/18, punctul 28.](#)



În urma prezentării [propunerii](#) Comisiei LIBE la 11 mai 2023, Parlamentul [a adoptat](#) o rezoluție referitoare la caracterul adecvat al protecției oferite de Cadrul UE-SUA privind confidențialitatea datelor, concluzionând că cadrul UE-SUA privind confidențialitatea datelor nu creează echivalența esențială a nivelului de protecție și solicitând Comisiei să continue negocierile cu omologii săi din SUA, dar să se abțină de la adoptarea constatării caracterului adecvat până la punerea în aplicare deplină a tuturor recomandărilor formulate în rezoluție și în avizul CEPD. Comisia și-a adoptat decizia privind [Cadrul UE-SUA privind confidențialitatea datelor](#) la 10 iulie 2023.

Parlamentul a înființat o [comisie de anchetă pentru a investiga utilizarea Pegasus și a programelor spion de supraveghere echivalente](#) în statele membre ale UE (PEGA). Prezidată de [Jeroen Lenaers, deputat în Parlamentul European](#), Comisia PEGA a investigat în detaliu practicile de utilizare a programelor spion pentru a investiga membrii opoziției, jurnaliștii, avocații și activiștii societății civile, precum și modul în care astfel de practici afectează procesele democratice și drepturile individuale în UE. În cursul anchetei sale, Comisia PEGA a consultat [cadre universitare de prim rang](#), practicieni și autorități din UE și din întreaga lume. Departamentul tematic al Parlamentului a pregătit rapoarte pentru misiunile PEGA în [Polonia](#), [Grecia](#) și [Cipru](#). Comisia PEGA a votat la 8 mai 2023 aprobarea [raportului său final](#) extrem de critic conținând recomandări privind investigarea presupuselor încălcări și cazuri de administrare defectuoasă în aplicarea dreptului UE în ceea ce privește utilizarea Pegasus și a programelor spion de supraveghere echivalente, și incluzând, printre multe alte puncte, o recomandare de înființare a unui laborator tehnologic al UE pentru cercetarea și monitorizarea utilizării programelor spion împotriva cetățenilor UE. Recomandarea Parlamentului adresată Consiliului și Comisiei în urma raportului PEGA a fost adoptată în plen la 15 iunie 2023. Cu toate acestea, Comisia nu a oferit un răspuns în timp util la recomandare și a blocat proiectul-pilot de laborator tehnologic al UE, propus de deputații în Parlamentul European.

Parlamentul a comandat o serie de studii, pentru a dispune de o bază științifică pentru activitățile sale legislative în prima linie a evoluțiilor tehnologice și a protecției datelor, inclusiv un studiu privind [impactul Regulamentului general privind protecția datelor \(RGPD\) asupra inteligenței artificiale](#), un studiu [privind recunoașterea biometrică și detectarea comportamentală](#) și un studiu [privind Metaverse](#).

Această fișă informativă a fost pregătită de Departamentul tematic pentru drepturile cetățenilor și afaceri constituționale al Parlamentului European.

[Mariusz Maciejewski](#)

11/2023

