

Declarație



Declarația 02/2021 privind noul proiect de dispoziții ale celui de al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta)

Adoptată pe 2 februarie 2021

Comitetul european pentru protecția datelor a adoptat următoarea declarație:

Observații preliminare și contextul declarației CEPD

Comitetul european pentru protecția datelor (CEPD) și autoritățile de protecție a datelor din UE urmăresc îndeaproape elaborarea celui de al doilea protocol adițional la Convenția de la Budapesta și au contribuit în mod regulat la procesul de consultare organizat de Consiliul Europei, de exemplu în cadrul conferinței anuale „Octopus”. În noiembrie 2019, CEPD a publicat, de asemenea, cea mai recentă contribuție a sa la acest proces de consultare cu privire la un al doilea protocol adițional¹, indicând că rămâne „disponibil pentru contribuții suplimentare” și a solicitat „o implicare timpurie și mai proactivă a autorităților pentru protecție a datelor în pregătirea acestor dispoziții specifice, pentru a asigura o înțelegere și o luare în considerare optime ale garanțiilor privind protecția datelor”².

Ca urmare a publicării noului proiect de dispoziții ale celui de al doilea protocol adițional la Convenția de la Budapesta³, CEPD dorește, încă o dată, să ofere o contribuție de specialitate și constructivă, pentru a se asigura că aspectele legate de protecția datelor sunt luate în considerare

¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf

² CEPD susține pozițiile și recomandările exprimate în această contribuție anterioară și consideră relevantă reafirmarea principiilor-cheie în lumina celor mai recente evoluții și a noilor proiecte de dispoziții publicate.

³ <https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations>

în mod corespunzător în procesul general de redactare a protocolului adițional, având în vedere faptul că reuniunile consacrate pregătirii protocolului adițional se desfășoară în sesiuni închise și că implicarea directă a autorităților pentru protecția datelor în procesul de redactare nu a fost prevăzută în mandatul T-CY⁴.

În plus, CEPD consideră că este probabil ca dispozițiile menționate anterior să afecteze condițiile de fond și procedurile pentru accesul la datele cu caracter personal în UE, inclusiv ca urmare a unor solicitări din partea autorităților din țări terțe, fiind astfel în consonanță cu dezbaterile aflate în derulare la nivelul UE și cu inițiativele legislative conexe care sunt în curs de examinare de către colegiuitorii⁵. Prin urmare, CEPD solicită Comisiei Europene și Parlamentului European, precum și statelor membre ale UE și parlamentelor naționale să se asigure că negocierile în curs fac obiectul unei examinări atente, pentru a garanta coerența deplină cu acquis-ul UE a celui de al doilea protocol adițional preconizat, în special în domeniul protecției datelor cu caracter personal.

Accesul la datele cu caracter personal din toate jurisdicțiile a fost deja abordat în trecut, în diverse poziții și avize, de către autoritățile pentru protecția datelor din UE, iar CEPD dorește să reamintească încă o dată în special observațiile Grupului de lucru „articolul 29” cu privire la chestiunea accesului direct al autorităților de aplicare a legii din țările terțe la datele stocate într-o altă jurisdicție, așa cum se propune în proiectul de elemente pentru un protocol adițional la Convenția de la Budapesta privind criminalitatea informatică⁶, precum și declarația sa privind aspectele legate de protecția datelor și a vieții private în ceea ce privește accesul transfrontalier la probele electronice⁷. Autoritatea Europeană pentru Protecția Datelor a emis Avizul 03/2019 privind mandatul pentru participarea Comisiei la negocieri⁸, precum și Avizul 7/2019 privind propunerile referitoare la ordinele europene de divulgare și de păstrare a probelor electronice în materie penală⁹. Aceste contribuții se bazează, de asemenea, pe Avizul 23/2018 al CEPD referitor la propunerile Comisiei privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală¹⁰.

CEPD este pe deplin conștient de faptul că situațiile în care autoritățile judiciare și de aplicare a legii se confruntă cu o „situație transfrontalieră” în ceea ce privește accesul la datele cu caracter personal în cadrul investigațiilor lor pot fi o realitate dificilă și recunoaște obiectivul legitim de consolidare a cooperării internaționale în materie de criminalitate informatică și a accesului la informații. În

⁴ Mandat pentru elaborarea unui al doilea proiect adițional la Convenția de la Budapesta privind criminalitatea informatică, aprobat de cea de a 17-a sesiune plenară a T-CY din 8 iunie 2017, T-CY (2017) 3.

⁵ În special, dar nu exclusiv, cu discuțiile referitoare la propunerile Comisiei privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală.

⁶ Observațiile Grupului de lucru „articolul 29” cu privire la chestiunea accesului direct al autorităților de aplicare a legii din țările terțe la datele stocate în alte jurisdicții, astfel cum se propune în proiectul de elemente pentru un protocol adițional la Convenția de la Budapesta privind criminalitatea informatică, 05/12/2013.

⁷ Declarația Grupului de lucru „Articolul 29” privind aspectele legate de protecția datelor și de viața privată ale accesului transfrontalier la probele electronice, 29 noiembrie 2017.

⁸ Avizul AEPD 3/2019 privind participarea la negocieri în vederea adoptării unui al doilea protocol adițional la Convenția de la Budapesta privind criminalitatea informatică.

⁹ Avizul 7/2019 privind propunerile referitoare la ordinele europene de divulgare și de păstrare a probelor electronice în materie penală.

¹⁰ Avizul 23/2018 al CEPD, adoptat la data de 26 septembrie 2018, referitor la propunerile Comisiei privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală.

paralel, CEPD reiterează faptul că trebuie garantate protecția datelor cu caracter personal și securitatea juridică, contribuind astfel la îndeplinirea obiectivului creării unor mecanisme durabile pentru schimbul de date cu caracter personal cu țările terțe în scopul aplicării legii care să fie pe deplin compatibile cu tratatele UE și cu Carta drepturilor fundamentale a UE. În plus, CEPD consideră că este esențial ca pregătirea protocolului adițional să fie delimitată de cadrul valorilor și principiilor fundamentale ale Consiliului Europei, în special în ceea ce privește drepturile omului și statul de drept.

În ceea ce privește „accesul transfrontalier direct la datele stocate pe calculator”, în conformitate cu articolul 32 litera (b) din Convenția de la Budapesta, CEPD reafirmă, în special, că un operator de date poate, în mod normal, să divulge date numai după prezentarea prealabilă, de către de o autoritate națională de aplicare a legii în conformitate cu legislația sa națională, a unei autorizații ori a unui mandat judiciar sau a oricărui document care justifică necesitatea de a accesa datele și care face trimitere la temeiul juridic relevant pentru acest acces, în care va fi specificat scopul pentru care sunt necesare datele.

Întrucât Convenția de la Budapesta, precum și oricare dintre protocoalele sale adiționale sunt instrumente internaționale obligatorii, CEPD subliniază că, în conformitate cu jurisprudența CJUE, „obligațiile impuse de un acord internațional nu pot avea ca efect prejudicierea principiilor constituționale ale Tratatului CE, care includ principiul conform căruia toate actele comunitare trebuie să respecte drepturile fundamentale, respectarea acestora constituind o condiție a legalității acestora”¹¹. Prin urmare, este esențial ca părțile la negociere din cadrul UE să se asigure că dispozițiile prevăzute în protocolul adițional respectă acquis-ul UE în domeniul protecției datelor, pentru a asigura compatibilitatea acestuia cu legislația primară și secundară a UE.

Având în vedere calendarul procesului de consultare, prezenta contribuție a CEPD se va concentra pe o evaluare preliminară a noului proiect de dispoziții ale celui de al doilea protocol adițional la Convenția de la Budapesta, care nu a făcut obiectul unor consultări anterioare cu părțile interesate:

- Echipe comune de anchetă și anchete comune
- Divulgarea accelerată în situații de urgență a datelor informatice stocate
- Cerere de informații referitoare la înregistrarea numelor de domeniu

Încă o dată, CEPD înțelege că dispozițiile specifice privind protecția datelor cu caracter personal sunt încă în curs de dezbateri. CEPD rămâne disponibil pentru contribuții suplimentare și face apel la o implicare timpurie și mai proactivă a autorităților pentru protecția datelor în pregătirea acestor dispoziții specifice, pentru a asigura o înțelegere și o luare în considerare optime ale garanțiilor privind protecția datelor.

Proiect provizoriu de dispoziții privind echipele comune de anchetă și anchetele comune (JIT) (articolul 3), privind cererea de informații referitoare la înregistrarea numelor de domeniu

¹¹ A se vedea cauzele conexe C-402/05 P și C-415/05 P, Kadi/Consiliul, ECLI:EU:C:2008:461, punctul 285.

(articolul 6) și privind divulgarea accelerată în situații de urgență a datelor informatice stocate (articolul 7)

Pe baza evaluării sale preliminare, CEPD recomandă examinarea în continuare a proiectului provizoriu de dispoziții în ceea ce privește elementele de mai jos.

CEPD constată că atât cererile de informații privind înregistrarea numelor de domeniu, cât și cererile de divulgare accelerată a datelor informatice stocate în cazuri de urgență sunt cereri fără caracter obligatoriu, iar motivele refuzului de a se conforma cererii nu sunt clar definite, în timp ce posibilitatea de a se baza pe legislația statului parte solicitat pentru a refuza o astfel de cooperare, inclusiv motivele de refuz prevăzute în tratatele pentru asistența juridică reciprocă, este, de asemenea, neclară¹². CEPD reamintește, în acest sens, că este necesar ca legea să prevadă condițiile în care furnizorii de servicii de comunicare electronice sau entitatea care furnizează servicii de nume de domeniu acordă acest acces, astfel încât să se asigure că prelucrarea se bazează pe un temei juridic clar.

CEPD face referire, de asemenea, la contribuția sa anterioară pentru a reafirma faptul că, cu excepția cazurilor de urgență stabilite în mod valabil¹³ și având în vedere jurisprudența CJUE¹⁴, CEPD consideră că tipul de autorități solicitante care pot emite o astfel de cerere ar trebui să se limiteze la un procuror, la o autoritate judiciară sau la o altă autoritate independentă. CEPD consideră, de asemenea, că implicarea sistematică a autorităților judiciare în demersurile părților solicitate este esențială pentru a asigura un control eficace al conformității cererilor cu Convenția și pentru a menține aplicarea principiului dublei incriminări în domeniul cooperării judiciare.

CEPD reamintește în această privință că principiul dublei incriminări urmărește să ofere o garanție suplimentară pentru a se asigura că o parte nu poate recurge la asistența unei alte părți pentru a aplica o sancțiune penală care nu există în dreptul acestei alte părți. Pe lângă asigurarea respectării drepturilor persoanelor și a garanțiilor procedurale în cadrul mecanismului preconizat de cooperare judiciară, o astfel de garanție asigură, de asemenea, o garanție esențială legată de condițiile procedurale de acces la datele cu caracter personal ale respectivelor persoane. După cum s-a menționat deja în contribuția sa anterioară, în ceea ce privește securitatea prelucrării datelor, CEPD invită T-CY să ia în considerare, ca o garanție specifică de protecție a datelor, un mecanism de notificare fără întârziere a încălcărilor securității datelor care ar putea afecta grav drepturile și libertățile persoanelor vizate. Încălcările securității datelor cu caracter personal ar putea efectiv produce o serie de efecte negative semnificative pentru persoanele vizate.

În ceea ce privește proiectul provizoriu de dispoziții privind cererea de informații referitoare la înregistrarea numelor de domenii, CEPD subliniază că aceste informații includ date cu caracter personal și că, prin urmare, orice instrument internațional care stabilește condițiile de fond și procedurale pentru accesarea acestor date trebuie să fie, în cazul părților care sunt state membre ale Uniunii Europene, conform cu legislația primară și secundară a UE.

¹² Proiectul de articol 6 alineatul (2) se referă, de exemplu, la „condiții rezonabile prevăzute de dreptul intern”.

¹³ CEPD ia act de faptul că noțiunea de urgență este menționată în sensul alineatului (1) din proiectul de dispoziție privind asistența reciprocă de urgență și consideră că domeniul de aplicare al unei astfel de situații poate fi clarificat și încadrat în continuare.

¹⁴ A se vedea cauzele conexe CJUE C-203/15 și C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, punctul 120.

În ceea ce privește proiectul provizoriu de dispoziții privind „divulgarea accelerată în situații de urgență a datelor informatice stocate” (articolul 7), CEPD observă că, în funcție de modul în care este aplicată de către fiecare parte, această nouă dispoziție poate implica divulgarea directă a datelor referitoare la conținut. CEPD ia act, de asemenea, de faptul că statul parte solicitat poate solicita, după divulgarea datelor, să se furnizeze o cerere adecvată de asistență reciprocă [articolul 7 alineatul (5)]. Cu toate acestea, în acest din urmă caz, nu există, din partea părților la protocolul avut în vedere, niciun angajament de a șterge datele sau de a nu le utiliza ca elemente de probă în cazul în care, pe baza informațiilor suplimentare obținute în cadrul cererii corespunzătoare de asistență reciprocă, autoritățile solicitate concluzionează că nu au fost îndeplinite condițiile pentru divulgarea datelor. Prin urmare, consecințele juridice pentru datele divulgate, odată ce acestea au ajuns în țara solicitantă, par să fie lăsate pe deplin la latitudinea autorităților de aplicare a legislației naționale a țării respective. Lipsa unui angajament la nivelul protocolului implică, prin urmare, riscul de a priva această dispoziție de orice efect de protecție în ceea ce privește prelucrarea datelor cu caracter personal deja divulgate.

În fine, CEPD subliniază cerința prevăzută la articolul 52 alineatul (1) din Carta drepturilor fundamentale a UE¹⁵, conform căreia orice restrângere a exercițiului drepturilor și libertăților recunoscute de Cartă trebuie să respecte principiul proporționalității și poate fi impusă numai dacă este necesară. Prin urmare, pentru a fi legal în temeiul dreptului Uniunii, proiectul de dispoziții ale protocolului avut în vedere trebuie să îndeplinească această cerință. Aceasta se referă atât la datele cu caracter personal conținute în cerere, cât și la răspunsul la o astfel de cerere. **Prin urmare, Comitetul european pentru protecția datelor este deosebit de preocupat de formularea articolului 6 alineatul (3) litera (c) din proiect și de cea a alineatului (13) din proiectul de raport explicativ, în ceea ce privește această dispoziție, întrucât aceste formulări par să implice faptul că țările terțe solicitante care sunt părți la protocolul avut în vedere pot să nu fie obligate să respecte principiul proporționalității atunci când adresează cereri unui stat membru al UE.** În plus, nu există o claritate deplină în ceea ce privește posibilitatea de a invoca, în temeiul acestor dispoziții, principiul proporționalității ca motiv de refuz.

De asemenea, nu este clar dacă părțile ar fi obligate să respecte obligațiile de a asigura, în contextul protocolului avut în vedere, condițiile și garanțiile prevăzute la articolul 15 din Convenția de la Budapesta¹⁶. **CEPD recomandă clarificarea faptului că obligațiile prevăzute la articolul 15 din Convenția de la Budapesta se aplică pe deplin și în contextul acestei cooperări transfrontaliere.**

Dispoziții privind garanțiile în materie de protecție a datelor

CEPD consideră că este esențial ca textul provizoriu făcut public să fie completat de dispoziții specifice privind garanțiile în materie de protecție a datelor, care trebuie ulterior să fie evaluate împreună cu alte dispoziții, pentru a se asigura că proiectul de protocol adițional se traduce într-un acord durabil pentru schimbul de date cu caracter personal cu țările terțe în scopul aplicării legii, care să fie pe deplin compatibil cu tratatele UE și cu Carta drepturilor fundamentale.

Datorită faptului că stabilește condițiile procedurale pentru accesul la datele cu caracter personal, proiectul provizoriu de dispoziții privind cererea de informații referitoare la înregistrarea numelor de

¹⁵ A se vedea și Articolul 8 alineatul (2) din Convenția europeană a drepturilor omului.

¹⁶ A se vedea în special articolul 6 alineatul (4) între paranteze.

domeniu și divulgarea accelerată în situații de urgență a datelor informatice stocate poate avea deja un impact asupra nivelului de protecție a datelor cu caracter personal și, de asemenea, poate necesita modificări pentru a asigura aplicarea operațională a garanțiilor adecvate în materie de protecție a datelor. **În acest sens, CEPD ar dori să sublinieze din nou necesitatea ca garanțiile privind protecția datelor să se aplice oricărui schimb de date cu caracter personal efectuat în contextul protocolului avut în vedere¹⁷, inclusiv în ceea ce privește transferul de date cu caracter personal¹⁸.**

CEPD consideră că dispozițiile specifice privind garanțiile în materie de protecție a datelor trebuie să reflecte principii-cheie, în special legalitatea, echitatea și transparența, limitarea scopului, reducerea la minimum a datelor, acuratețea, limitarea stocării, integritatea și confidențialitatea. De asemenea, CEPD ar dori să sublinieze importanța asigurării unor drepturi individuale de bază (de acces, rectificare și ștergere), orice restricții trebuind să fie limitate de principiul proporționalității, precum și a unor căi de atac judiciare eficiente pentru persoanele vizate, în cazul încălcării garanțiilor privind protecția datelor. Exercițarea acestor drepturi necesită, de asemenea, notificarea persoanei vizate, cel puțin odată ce această notificare nu mai pune în pericol ancheta. Aceste principii, drepturi și obligații sunt, de asemenea, în conformitate cu Convenția modernizată a Consiliului Europei pentru protejarea persoanelor față de prelucrarea datelor cu caracter personal (Convenția 108+), la care sunt, de asemenea, părți multe dintre părțile la Convenția de la Budapesta privind criminalitatea informatică. În conformitate cu Convenția 108+, acestea ar trebui să se aplice tuturor autorităților care prelucrează datele la nivelul părții solicitante, pentru a asigura continuitatea protecției. **CEPD face trimitere la contribuția sa la consultarea publică din 2019 pentru detalii suplimentare cu privire la cerințele UE în această privință¹⁹.**

CEPD reiterează importanța implicării autorităților pentru protecția datelor în procesul de elaborare a protocolului adițional și este pregătit să contribuie și să asiste T-CY la pregătirea textului provizoriu al dispozițiilor privind garanțiile în materie de protecție a datelor.

Pentru Comitetul european pentru protecția datelor

Președinta

(Andrea Jelinek)

¹⁷ Articolul 6 alineatul (4) pare să limiteze aplicarea garanțiilor, precum și a articolului 15 din convenție doar la informațiile divulgate, nefiind vizate și datele cu caracter personal incluse în cerere.

¹⁸ În conformitate cu punctul 9 din proiectul de raport explicativ, această dispoziție poate/ar trebui să se aplice numai transferului de date cu caracter personal efectuat de echipele comune de anchetă.

¹⁹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf.