



Presă și informare

Curtea de Justiție a Uniunii Europene
COMUNICAT DE PRESĂ nr. 145/16

Luxemburg, 21 decembrie 2016

Hotărârea în cauzele conexe C-203/15
Tele2 Sverige AB/Post-och telestyrelsen și C-698/15 Secretary of State for
the Home Department/Tom Watson și alții

Statele membre nu pot impune furnizorilor de servicii de comunicații electronice o obligație generală de păstrare a datelor

Dreptul Uniunii se opune unei păstrări generalizate și nediferențiate a datelor privind traficul și a datelor de localizare, însă statele membre pot prevedea, cu titlu preventiv, o păstrare direcționată a acestor date doar în scopul combaterii infracționalității grave, cu condiția ca o astfel de păstrare să fie, în ceea ce privește categoriile de date care trebuie păstrate, mijloacele de comunicare vizate, persoanele în cauză, precum și durata de păstrare reținută, limitată la strictul necesar. Accesul autorităților naționale la datele păstrate trebuie supus unor condiții, printre care existența unui control prealabil din partea unei autorități independente și păstrarea datelor pe teritoriul Uniunii

Prin Hotărârea Digital Rights Ireland din 2014¹, Curtea de Justiție a declarat nevalidă directiva privind păstrarea datelor² pentru motivul că ingerința în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal pe care o presupune obligația generală de păstrare a datelor privind traficul și a datelor de localizare impuse de aceasta nu era limitată la strictul necesar.

În urma acestei hotărâri, Curtea a fost sesizată cu două cauze privind obligația generală impusă furnizorilor de servicii de comunicații electronice, în Suedia și în Regatul Unit, de a păstra datele referitoare la aceste comunicații, a căror păstrare era prevăzută de directiva declarată nevalidă.

În ziua următoare pronunțării Hotărârii Digital Rights Ireland, societatea de telecomunicații Tele2 Sverige a notificat autoritățile suedeze pentru monitorizarea serviciilor poștale și a telecomunicațiilor decizia sa de a înceta păstrarea datelor, precum și intenția sa de a șterge datele deja înregistrate (cauza C-203/15). Astfel, dreptul suedez îi obligă pe furnizorii de servicii de comunicații electronice să păstreze în mod sistematic și continuu, fără nicio excepție, ansamblul datelor privind traficul și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați ai acestora, în ceea ce privește toate mijloacele de comunicare electronică.

În cauza C-698/15, domnii Tom Watson, Peter Brice și Geoffrey Lewis au formulat acțiuni împotriva sistemului britanic de păstrare a datelor care permite ministrului de interne să oblige operatorii de telecomunicații publice să păstreze toate datele referitoare la comunicații pentru o durată maximă de 12 luni, subînțelegându-se că este exclusă păstrarea conținutului acestor comunicații.

Sesizată de Kammarrätten i Stockholm (Curtea Administrativă de Apel din Stockholm, Suedia) și de Court of Appeal (England and Wales) (Civil Division) (Secția civilă a Curții de Apel din Anglia și Țara Galilor, Regatul Unit), Curtea trebuie să stabilească dacă sistemele naționale care impun furnizorilor o obligație generală de păstrare a datelor și care prevăd accesul autorităților naționale competente la datele păstrate, printre altele fără a limita acest acces doar la scopul combaterii infracționalității grave și fără a supune accesul respectiv unui control prealabil din partea unei instanțe sau a unei autorități administrative independente, sunt compatibile cu dreptul Uniunii (în

¹ Hotărârea Curții din 8 aprilie 2014, *Digital Rights Ireland și Seitlinger și alții* (cauzele conexe [C-293/12](#) și [C-594/12](#), a se vedea și comunicatul de presă [nr. 54/14](#)).

² Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO 2006, L 105, p. 54, Ediție specială, 13/vol. 53, p. 51).

speță cu Directiva „viața privată și comunicațiile electronice”³ interpretată în lumina Cartei drepturilor fundamentale a UE⁴).

În hotărârea pronunțată astăzi, **Curtea răspunde că dreptul Uniunii se opune unei reglementări naționale care prevede o păstrare generalizată și nediferențiată a datelor.**

Curtea confirmă mai întâi că **măsurile naționale în cauză intră în domeniul de aplicare al directivei.** Astfel, protecția confidențialității comunicațiilor electronice și a datelor de transfer, garantată de directivă, se aplică măsurilor adoptate de orice alte persoane decât utilizatorii, indiferent că este vorba despre persoane sau entități private ori despre entități statale.

Curtea constată în continuare că, deși această directivă permite statelor membre să restrângă sfera de aplicare a obligației de principiu de a asigura confidențialitatea comunicațiilor și a datelor de transfer aferente acestora, ea nu poate să justifice ca derogarea de la această obligație de principiu și, în special, de la interdicția de a stoca aceste date, prevăzută de directiva menționată, să devină regula.

În plus, Curtea amintește jurisprudența sa constantă potrivit căreia protecția dreptului fundamental la respectarea vieții private impune ca **derogările** de la protecția datelor cu caracter personal **să fie efectuate în limitele strictului necesar.** Curtea aplică această jurisprudență la normele care reglementează păstrarea datelor și la cele care reglementează accesul la datele păstrate.

Curtea constată, **în ceea ce privește păstrarea**, că datele păstrate considerate în ansamblul lor **pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor** ale căror date au fost păstrate.

Ingerința care rezultă dintr-o reglementare națională care prevede păstrarea datelor privind traficul și a datelor de localizare trebuie considerată deosebit de gravă. Faptul că păstrarea datelor este efectuată fără ca utilizatorii serviciilor de comunicații electronice să fie informați cu privire la aceasta este susceptibil să genereze, în mintea persoanelor vizate, sentimentul că viața lor privată face obiectul unei supravegheri constante. Prin urmare, **numai combaterea infracționalității grave poate justifica o asemenea ingerință.**

Curtea arată că **o reglementare care prevede o păstrare generalizată și nediferențiată a datelor nu impune o relație între datele a căror păstrare este prevăzută și o amenințare pentru securitatea publică** și nu se limitează printre altele să prevadă o păstrare a datelor aferente unei perioade și/sau unei zone geografice și/sau unui cerc de persoane care pot fi implicate într-o infracțiune gravă. **O asemenea reglementare națională depășește, așadar, limitele strictului necesar și nu poate fi considerată justificată, într-o societate democratică, astfel cum impune directiva interpretată în lumina cartei.**

Curtea explică în schimb că **directiva nu se opune unei reglementări naționale care impune o păstrare direcționată a datelor**, în scopul combaterii infracționalității grave, **cu condiția ca o asemenea păstrare să fie**, în ceea ce privește categoriile de date care trebuie păstrate, mijloacele de comunicare vizate, persoanele în cauză, precum și durata de păstrare reținută, **limitată la strictul necesar.** Potrivit Curții, **orice reglementare națională care conține dispoziții în acest sens trebuie să fie clară și precisă și să prevadă garanții suficiente** pentru a proteja datele împotriva riscurilor de abuz. Aceasta trebuie să indice împrejurările și condițiile în care o măsură de păstrare a datelor poate fi luată, cu titlu preventiv, astfel încât să garanteze ca amplexarea acestei măsuri să fie limitată efectiv, în practică, la strictul necesar. Printre altele, o asemenea reglementare trebuie **să se întemeieze pe elemente obiective** care să permită să fie vizate persoanele ale căror date pot prezenta o legătură cu acte de infracționalitate gravă, care să

³ 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) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11, rectificare în JO 2013, L 241, p. 9).

⁴ Articolul 7, articolul 8 și articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene.

contribuie la combaterea infracționalității grave sau care să prevină un risc grav pentru securitatea publică.

În ceea ce privește **accesul autorităților naționale competente la datele păstrate**, Curtea confirmă că reglementarea națională în cauză nu se poate limita la a impune ca accesul să răspundă unuia dintre obiectivele vizate de directivă, chiar dacă acesta constă în combaterea infracționalității grave, ci trebuie să prevadă și condițiile materiale și procedurale care guvernează accesul autorităților naționale competente la datele păstrate. Respectiva reglementare trebuie să se întemeieze pe **criterii obiective pentru a defini împrejurările și condițiile în care trebuie să se permită autorităților naționale competente accesul la date**. În principiu, accesul nu poate fi permis, în raport cu obiectivul de combatere a infracționalității, decât la datele persoanelor bănuite de a pregăti, de a săvârși sau de a fi săvârșit o infracțiune gravă sau de a fi implicate în orice mod într-o astfel de infracțiune. Cu toate acestea, în situații speciale, precum cele în care interese vitale privind securitatea națională, apărarea sau securitatea publică sunt amenințate de activități teroriste, ar putea de asemenea să fie permis accesul la datele altor persoane, în cazul în care există elemente obiective care permit să se considere că aceste date ar putea aduce, într-un caz concret, o contribuție efectivă la combaterea unor asemenea activități.

În plus, Curtea consideră că **este esențial ca accesul la datele păstrate să fie condiționat, cu excepția unor situații de urgență, de un control prealabil** efectuat de o instanță sau de o entitate independentă. De asemenea, autoritățile naționale competente cărora le-a fost acordat accesul la datele păstrate trebuie să informeze persoanele în cauză în privința acestui aspect.

Ținând seama de cantitatea datelor păstrate, de caracterul sensibil al respectivelor date, precum și de riscul de acces ilicit la acestea, **reglementarea națională trebuie să prevadă ca datele să fie păstrate pe teritoriul Uniunii** și ca ele să fie distruse iremediabil la finalul duratei de păstrare a acestora.

MENȚIUNE: Trimiterea preliminară permite instanțelor din statele membre ca, în cadrul unui litigiu cu care sunt sesizate, să adreseze Curții întrebări cu privire la interpretarea dreptului Uniunii sau la validitatea unui act al Uniunii. Curtea nu soluționează litigiul național. Instanța națională are obligația de a soluționa cauza conform deciziei Curții. Această decizie este obligatorie, în egală măsură, pentru celelalte instanțe naționale care sunt sesizate cu o problemă similară.

Document neoficial, destinat presei, care nu angajează răspunderea Curții de Justiție.

[Textul integral](#) al hotărârii se publică pe site-ul CURIA în ziua pronunțării.

Persoana de contact pentru presă: Iliana Paliova ☎ (+352) 4303 3708

Imagini de la pronunțarea hotărârii sunt disponibile pe „[Europe by Satellite](#)” ☎ (+32) 2 2964106