



Repertoriul jurisprudenței

Cauzele conexate C-793/19 și C-794/19

Bundesrepublik Deutschland
împotriva
SpaceNet AG
și
Telekom Deutschland GmbH

(cereri de decizie preliminară formulate de Bundesverwaltungsgericht)

Hotărârea Curții (Marea Cameră) din 20 septembrie 2022

„Trimitere preliminară – Prelucrarea datelor personale în sectorul comunicațiilor electronice – Confidențialitatea comunicațiilor – Furnizori de servicii de comunicații electronice – Păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare – Directiva 2002/58/CE – Articolul 15 alineatul (1) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 6, 7, 8 și 11, precum și articolul 52 alineatul (1) – Articolul 4 alineatul (2) TUE”

1. *Apropierea legislațiilor – Sectorul telecomunicațiilor – Prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice – Directiva 2002/58 – Domeniu de aplicare – Reglementare națională care impune furnizorilor de servicii de comunicații electronice să păstreze date de transfer și date de localizare – Obiective de protecție a securității naționale și de combatere a criminalității – Includere [art. 4 alin. (2) TUE; Directiva 2002/58 a Parlamentului European și a Consiliului, astfel cum a fost modificată prin Directiva 2009/136, art. 1 alin. (1) și (3), art. 3 și art. 15 alin. (1)]*

(a se vedea punctul 48)

2. *Apropierea legislațiilor – Sectorul telecomunicațiilor – Prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice – Directiva 2002/58 – Posibilitatea statelor membre de a limita întinderea anumitor drepturi și obligații – Măsuri naționale care impun furnizorilor de servicii de comunicații electronice păstrarea generalizată și nediferențiată a datelor de transfer și de localizare – Obiectiv de combatere a criminalității grave și de prevenire a amenințărilor grave la adresa siguranței publice – Inadmisibilitate – Durata perioadei de păstrare generalizată și nediferențiată a acestor date – Lipsa incidenței – Măsuri naționale referitoare la păstrarea anumitor categorii de date – Obiective de protecție a securității naționale, de combatere a criminalității grave și de prevenire a amenințărilor grave la adresa siguranței publice – Admisibilitate – Condiții [Carta drepturilor fundamentale a Uniunii Europene, art. 7, 8 și 11 și art. 52 alin. (1); Directiva 2002/58 a Parlamentului European și a Consiliului, astfel cum a fost modificată prin Directiva 2009/136, art. 15 alin. (1)]*

(a se vedea punctele 49-75, 77-81, 83-85, 87-94, 97-99, 110, 113, 116-121 și 127-131 și dispozitivul)

Rezumat

În ultimii ani, Curtea s-a pronunțat, în mai multe hotărâri, cu privire la păstrarea datelor cu caracter personal și la accesul la acestea în domeniul comunicațiilor electronice¹.

Mai recent, prin Hotărârea La Quadrature du net și alții², pronunțată în Marea Cameră la 6 octombrie 2020, Curtea și-a confirmat jurisprudența rezultată din Hotărârea Tele2 Sverige și Watson și alții³ cu privire la caracterul disproporționat al unei păstrări generalizate și nediferențiate a datelor de transfer și a datelor de localizare aferente comunicațiilor electronice. Ea a adus totodată precizări, în special în ceea ce privește întinderea competențelor pe care Directiva asupra confidențialității și comunicațiilor electronice le recunoaște statelor membre în materia păstrării unor asemenea date în vederea protecției securității naționale, a combaterii criminalității și a protecției siguranței publice.

În prezentele cauze conexe, două cereri de decizie preliminară au fost formulate de Bundesverwaltungsgericht (Curtea Administrativă Federală, Germania), care a fost sesizată cu un recurs declarat de Republica Federală Germania împotriva a două hotărâri prin care fuseseră admise acțiunile formulate de două societăți, SpaceNet AG (cauza C-793/19) și Telekom Deutschland GmbH (cauza C-794/19), care furnizează servicii de acces la internet. Prin aceste acțiuni, societățile menționate contestau obligația pe care le-o impune reglementarea germană⁴ de a păstra date de transfer și date de localizare aferente comunicațiilor electronice ale clienților lor.

Îndoielile exprimate de instanța de trimitere priveau în special compatibilitatea cu Directiva asupra confidențialității și comunicațiilor electronice⁵, citită în lumina Cartei drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”)⁶ și a articolului 4 alineatul (2) TUE, a unei reglementări naționale care impune furnizorilor de servicii publice de comunicații electronice – în special în scopul urmăririi infracțiunilor grave sau al prevenirii unui risc concret pentru securitatea națională – păstrarea generalizată și nediferențiată a celei mai mari părți a datelor de transfer și a datelor de localizare ale utilizatorilor acestor servicii, prevăzând o perioadă de păstrare de mai multe săptămâni și norme prin care se urmărește garantarea unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz, precum și împotriva oricărui acces ilicit la aceste date.

¹ Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238), Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970), și Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

² Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții (C-511/18, C-512/18 și C-520/18, EU:C:2020:791). A se vedea de asemenea Hotărârea Privacy International, pronunțată în aceeași zi (C-623/17, EU:C:2020:790), referitoare la transmiterea generalizată și nediferențiată a datelor de transfer și a datelor de localizare.

³ În această hotărâre, Curtea a statuat că articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor [electronice] (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63, denumită în continuare Directiva asupra confidențialității și comunicațiilor electronice), 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), se opune unei reglementări naționale care prevede păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare în vederea combaterii criminalității.

⁴ Dispozițiile articolului 113a alineatul (1) coroborate cu cele ale articolului 113b din Telekommunikationsgesetz (Legea privind telecomunicațiile) din 22 iunie 2004 (BGBl. 2004 I, p. 1190), în versiunea aplicabilă litigiului principal.

⁵ Mai precis, articolul 15 alineatul (1) din Directiva 2002/58.

⁶ Articolele 6-8 și 11 și articolul 52 alineatul (1) din cartă.

Prin hotărârea sa, Curtea, reunită în Marea Cameră, confirmă, precizându-i totodată domeniul de aplicare, jurisprudența rezultată din Hotărârea La Quadrature du Net și alții și, mai recent, din Hotărârea Commissioner of An Garda Síochána și alții⁷. Ea amintește în special că păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare aferente comunicațiilor electronice nu este autorizată, cu titlu preventiv, în scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice.

Aprecierea Curții

Curtea începe prin a confirma aplicabilitatea Directivei asupra confidențialității și comunicațiilor electronice în privința reglementării naționale în discuție, după care face o evocare didactică a principiilor rezultate din jurisprudența sa, înainte de a efectua o examinare detaliată a caracteristicilor reglementării naționale în cauză, evidențiate de instanța de trimitere.

În ceea ce privește, mai întâi, conținutul datelor păstrate, Curtea arată că obligația de păstrare prevăzută de reglementarea națională în discuție se extinde la un ansamblu foarte larg de date de transfer și de date de localizare și că ea privește cvasitotalitatea persoanelor care compun populația, fără ca acestea să se regăsească, fie și în mod indirect, într-o situație care poate da naștere urmării penale. Ea arată de asemenea că această reglementare impune păstrarea, fără motiv, generalizată și nediferențiată din punct de vedere personal, temporal și geografic, a celei mai mari părți a datelor de transfer și a datelor de localizare a căror întindere corespunde în esență celei a datelor păstrate în cauzele care au condus la pronunțarea Hotărârii La Quadrature du net și alții. Prin urmare, având în vedere această jurisprudență, Curtea consideră că o obligație de păstrare a datelor precum cea în discuție în litigiile principale nu poate fi considerată ca fiind o păstrare selectivă a datelor.

În continuare, în ceea ce privește perioada de păstrare a datelor, Curtea amintește că, din Directiva asupra confidențialității și comunicațiilor electronice⁸ rezultă că perioada de păstrare prevăzută de o măsură națională care impune o obligație de păstrare generalizată și nediferențiată este, desigur, un factor pertinent, printre alții, pentru a stabili dacă dreptul Uniunii se opune unei asemenea măsuri, directiva impunând ca această perioadă să fie „limitată”. Cu toate acestea, gravitatea ingerinței decurge din riscul, în special având în vedere numărul și varietatea lor, ca datele păstrate, considerate în ansamblul lor, să permită să se deducă concluzii foarte precise cu privire la viața privată a persoanei sau a persoanelor ale căror date au fost păstrate și mai ales să furnizeze mijloacele de a stabili profilul persoanei sau al persoanelor vizate, care este o informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al comunicațiilor. Prin urmare, păstrarea datelor de transfer sau a datelor de localizare prezintă în orice caz un caracter grav, independent de durata perioadei de păstrare, de volumul sau de natura datelor păstrate, atunci când ansamblul de date păstrate este susceptibil să permită să se deducă asemenea concluzii⁹.

În sfârșit, în ceea ce privește garanțiile prin care se urmărește protejarea datelor păstrate împotriva riscurilor de abuz și împotriva oricărui acces ilicit, Curtea arată, întemeindu-se pe jurisprudența anterioară, că păstrarea datelor și accesul la acestea constituie ingerințe distincte în drepturile fundamentale ale persoanelor vizate, care necesită o justificare distinctă. Reiese că o legislație

⁷ Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258).

⁸ Mai precis, din articolul 15 alineatul (1) a doua teză din Directiva 2002/58.

⁹ A se vedea, în ceea ce privește accesul la astfel de date, Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, EU:C:2021:152, punctul 39).

națională care asigură respectarea deplină a condițiilor rezultate din jurisprudența în materie de acces la datele păstrate nu poate fi susceptibilă, prin natura sa, nici să limiteze și nici măcar să remedieze ingerința gravă în drepturile persoanelor vizate care ar rezulta din păstrarea generalizată a acestor date.

Pe de altă parte, pentru a răspunde la argumentele prezentate în fața sa, Curtea arată, în primul rând, că o amenințare la adresa securității naționale trebuie să fie reală și actuală sau cel puțin previzibilă, ceea ce presupune apariția unor împrejurări suficient de concrete pentru a putea justifica o măsură de păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare pe o perioadă limitată. O asemenea amenințare se distinge, așadar, prin natura sa, prin gravitatea sa și prin caracterul specific al împrejurărilor care o constituie, de riscul general și permanent care este cel de apariție a unor tensiuni sau a unor tulburări, chiar grave, ale siguranței publice sau cel de infracțiuni grave. Prin urmare, criminalitatea, fie și deosebit de gravă, nu poate fi asimilată unei amenințări la adresa securității naționale.

În al doilea rând, ea arată că faptul de a autoriza, în scopul combaterii criminalității grave, accesul la date de transfer și la date de localizare păstrate în mod generalizat și nediferențiat pentru a face față unei amenințări grave la adresa securității naționale ar contraveni ierarhiei obiectivelor de interes general care pot justifica o măsură luată în temeiul Directivei asupra confidențialității și comunicațiilor electronice¹⁰. Astfel, aceasta ar însemna ca accesul să poată fi justificat de un obiectiv de o importanță mai redusă decât acela care a justificat păstrarea, și anume protecția securității naționale, ceea ce ar risca să priveze de orice efect util interdicția de a se efectua o păstrare generalizată și nediferențiată în scopul combaterii criminalității grave.

Curtea concluzionează, confirmându-și jurisprudența anterioară, că Directiva asupra confidențialității și comunicațiilor electronice, citită în lumina cartei, se opune unor măsuri legislative naționale care prevăd, cu titlu preventiv, în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare.

În schimb, ea nu se opune unor măsuri legislative naționale care permit, în scopul protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice de a efectua o păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare în situații în care statul membru în cauză se confruntă cu o amenințare gravă la adresa securității naționale care se dovedește reală și actuală sau previzibilă. În această privință, Curtea precizează că decizia care prevede această obligație poate face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie are efect obligatoriu, prin care se urmărește să se verifice existența uneia dintre aceste situații, precum și respectarea condițiilor și a garanțiilor care trebuie să fie prevăzute, iar obligația menționată nu poate fi impusă decât pentru o perioadă limitată la strictul necesar, dar care poate fi reînnoită în cazul menținerii acestei amenințări.

Această directivă, citită în lumina cartei, nu se opune nici unor măsuri legislative naționale care prevăd, în scopul protecției securității naționale, al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare selectivă a datelor de transfer și a datelor de localizare care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic, pentru o perioadă limitată la strictul necesar, dar care poate fi reînnoită.

¹⁰ Această ierarhie este consacrată în jurisprudența Curții, în special în Hotărârea La Quadrature du Net și alții, la punctele 135 și 136. În temeiul acestei ierarhii, combaterea criminalității grave prezintă o importanță mai redusă decât protecția securității naționale.

Situația este aceeași în ceea ce privește măsurile legislative naționale care prevăd, în scopul protecției securității naționale, al combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, o păstrare generalizată și nediferențiată a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată la strictul necesar, precum și a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice, cu privire la care este cert că păstrarea poate contribui la combaterea criminalității grave, în măsura în care aceste date permit identificarea persoanelor care au utilizat asemenea mijloace în contextul pregătirii sau al săvârșirii unui act care ține de criminalitatea gravă.

Situația nu este diferită în ceea ce privește măsurile legislative naționale care permit, în scopul combaterii criminalității grave și, *a fortiori*, al protecției securității naționale, impunerea unei obligații furnizorilor de servicii de comunicații electronice prin intermediul unei decizii a autorității competente, supusă unui control jurisdicțional efectiv, de a efectua, pentru o perioadă determinată, păstrarea rapidă a datelor de transfer și a datelor de localizare de care dispun acești furnizori de servicii.

Curtea indică însă că toate măsurile menționate mai sus trebuie să garanteze, prin norme clare și precise, că păstrarea datelor în discuție este subordonată respectării condițiilor de drept material și de drept procedural aferente acestora și că persoanele în cauză dispun de garanții efective împotriva riscurilor de abuz. Aceste diferite măsuri pot să fie aplicate împreună, potrivit alegerii legiuitorului național și cu respectarea limitelor strictului necesar.