



Presă și informare

Curtea de Justiție a Uniunii Europene  
**COMUNICAT DE PRESĂ nr. 29/21**  
Luxemburg, 2 martie 2021

Hotărârea în cauza C-746/18  
H. K/Prokuratuur

**Accesul, în scopuri penale, la un ansamblu de date de transfer sau de localizare privind comunicațiile electronice, care permit deducerea unor concluzii precise cu privire la viața privată, nu este autorizat decât în vederea combaterii infracționalității grave sau a prevenirii amenințărilor grave la adresa siguranței publice**

*Dreptul Uniunii se opune de altfel unei reglementări naționale care conferă Ministerului Public competența de a autoriza accesul unei autorități publice la aceste date pentru a desfășura o urmărire penală*

În Estonia s-a inițiat o procedură penală împotriva lui H. K. pentru infracțiunile de furt, de utilizare a cardului bancar al unui terț și de violență față de persoane care participă la o procedură judiciară. H.K. a fost condamnată pentru aceste infracțiuni de un Tribunal de Primă Instanță la o pedeapsă cu închisoarea de doi ani. Ulterior, această decizie a fost confirmată în apel.

Procesele verbale pe care este întemeiată constatarea acestor infracțiuni au fost întocmite, în mod special, pe baza unor date cu caracter personal generate în cadrul furnizării unor servicii de comunicații electronice. Riigikohus (Curtea Supremă, Estonia), în fața căreia H.K a declarat recurs, a exprimat îndoieli cu privire la compatibilitatea cu dreptul Uniunii <sup>1</sup> a condițiilor în care serviciile de investigare au avut acces la aceste date.

Aceste îndoieli privesc în primul rând aspectul dacă întinderea perioadei pentru care serviciile de investigare au avut acces la date constituie un criteriu care permite să se evalueze gravitatea ingerinței constituite de acest acces în drepturile fundamentale ale persoanelor vizate. Astfel, în cazul în care această perioadă este foarte scurtă sau volumul datelor colectate este foarte limitat, instanța de trimitere a ridicat problema stabilirii faptului dacă obiectivul privind combaterea criminalității în general, iar nu numai a criminalității grave, poate justifica o asemenea ingerință. În al doilea rând, instanța de trimitere a avut îndoieli cu privire la posibilitatea de a considera că Ministerul Public estonian, ținând seama de diferitele misiuni care îi sunt încredințate de reglementarea națională, este o autoritate administrativă „independentă” în sensul Hotărârii Tele2 Sverige și Watson și alții <sup>2</sup>, susceptibilă să autorizeze accesul autorităților de investigare la datele vizate.

Prin hotărârea sa, pronunțată în Marea Cameră, Curtea statuează că Directiva asupra confidențialității și comunicațiilor electronice, citită în lumina cartei, se opune unei reglementări naționale care permite accesul autorităților publice la un ansamblu de date de transfer sau de date de localizare, care pot să furnizeze informații cu privire la comunicațiile efectuate de un utilizator al unui mijloc de comunicare electronică sau cu privire la localizarea echipamentelor terminale pe care le utilizează acesta și să permită să se deducă concluzii precise cu privire la viața sa privată,

<sup>1</sup> Mai precis, cu 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 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) (denumită în continuare „Directiva 2002/58”), citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”).

<sup>2</sup> Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții, [C-203/15 și C-698/15](#) punctul 120 ; a se vedea de asemenea Comunicatul de presă nr. [145/16](#).

În scopul prevenirii, investigării, detectării și urmăririi penale a infracțiunilor, fără ca acest acces să fie limitat la proceduri care vizează combaterea infracționalității grave sau prevenirea amenințărilor grave la adresa siguranței publice. Potrivit Curții, întinderea perioadei pentru care se solicită accesul la aceste date și volumul sau natura datelor disponibile pentru o astfel de perioadă nu sunt relevante în această privință. În plus, Curtea consideră că aceeași directivă, citită în lumina cartei, se opune unei reglementări naționale care conferă Ministerului Public competența de a autoriza accesul unei autorități publice la datele de transfer și la datele de localizare în scopul desfășurării unei urmăririi penale.

#### Aprecierea Curții

În ceea ce privește condițiile în care autorităților publice li se poate acorda accesul la datele de transfer și la datele de localizare stocate de furnizorii de servicii de comunicații electronice, în scopul prevenirii, investigării, detectării și urmăririi penale a infracțiunilor, în aplicarea unei măsuri adoptate în temeiul Directivei asupra confidențialității și comunicațiilor electronice<sup>3</sup>, Curtea a amintit ceea ce a statuat în Hotărârea La Quadrature du Net și alții<sup>4</sup>. Astfel, această directivă nu permite statelor membre să adopte, între altele în aceste scopuri, măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute de această directivă, în special obligația de a asigura confidențialitatea comunicațiilor și a datelor de transfer<sup>5</sup>, decât cu respectarea principiilor generale de drept al Uniunii, printre care figurează principiul proporționalității, și a drepturilor fundamentale garantate de cartă<sup>6</sup>. În acest cadru, directiva se opune unor măsuri legislative care impun furnizorilor de servicii de comunicații electronice, cu titlu preventiv, o stocare generalizată și nediferențiată a datelor de transfer și a datelor de localizare.

În ceea ce privește obiectivul de prevenire, investigare, detectare și urmărire penală a infracțiunilor, urmărit prin reglementarea în discuție, în conformitate cu principiul proporționalității, Curtea consideră că numai obiectivele de combatere a infracționalității grave sau de prevenire a amenințărilor grave pentru siguranța publică sunt de natură să justifice accesul autorităților publice la un ansamblu de date de transfer sau de date de localizare, care permit deducerea unor concluzii precise privind viața privată a persoanelor vizate, fără ca alți factori referitori la proporționalitatea unei cereri de acces, precum perioada pentru care se solicită accesul la astfel de date, să poată avea ca efect ca obiectivul de prevenire, investigare, detectare și urmărire penală a infracțiunilor în general să fie susceptibil să justifice un astfel de acces.

În ceea ce privește competența conferită Ministerului Public de a autoriza accesul unei autorități publice la datele de transfer și la datele de localizare pentru a desfășura o urmărire penală, Curtea amintește că revine dreptului național sarcina de a stabili condițiile în care furnizorii de servicii de comunicații electronice trebuie să acorde autorităților naționale competente accesul la datele de care dispun. Pentru a îndeplini cerința proporționalității, o astfel de reglementare trebuie să prevadă însă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz. Această reglementare trebuie să aibă forță juridică obligatorie în dreptul intern și în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date, garantând în acest mod că o ingerință este limitată la strictul necesar.

Potrivit Curții, în scopul de a garanta, în practică, deplina respectare a acestor condiții, este esențial ca accesul autorităților naționale competente la datele stocate să fie condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă și ca decizia acestei instanțe sau a acestei entități să intervină în urma unei cereri motivate formulate de autoritățile respective, printre altele în cadrul unor proceduri de prevenire, de detectare sau de

<sup>3</sup> Articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice.

<sup>4</sup> Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, [C-511/18](#), [C-512/18](#) și [C-520/18](#), punctele 166 - 169 ; a se vedea de asemenea Comunicatul de presă nr. [123/20](#)

<sup>5</sup> Articolul 5 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice.

<sup>6</sup> În special, articolele 7, 8 și 11, precum și articolul 52 alineatul (1) din cartă.

urmărire penală. În caz de urgență justificată corespunzător, controlul trebuie să aibă loc în termene scurte.

În această privință, Curtea precizează că un control prealabil impune, printre altele, ca instanța sau entitatea însărcinată cu efectuarea controlului prealabil menționat să dispună de toate atribuțiile și să prezinte toate garanțiile necesare în vederea asigurării unei concilierii a diferitor interese și drepturi în cauză. În ceea ce privește mai concret o investigație penală, un asemenea control impune ca această instanță sau această entitate să fie în măsură să asigure un just echilibru între, pe de o parte, interesele legate de nevoile investigației în cadrul combaterii infracționalității și, pe de altă parte, drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal ale persoanelor ale căror date sunt vizate prin acces. Atunci când acest control nu este efectuat de o instanță, ci de o entitate administrativă independentă, aceasta trebuie să beneficieze de un statut care să îi permită să acționeze în cadrul exercitării misiunilor sale în mod obiectiv și imparțial și trebuie să fie, în acest scop, protejată de orice influență externă.

În opinia Curții, din acestea rezultă că cerința privind independența pe care trebuie să o îndeplinească autoritatea însărcinată cu exercitarea controlului prealabil impune ca această autoritate să aibă calitatea de terț în raport cu cea care solicită accesul la date, astfel încât prima să fie în măsură să exercite respectivul control în mod obiectiv și imparțial la adăpost de orice influență exterioară. În special, în domeniul penal, cerința privind independența presupune ca autoritatea însărcinată cu acest control prealabil, pe de o parte, să nu fie implicată în desfășurarea investigației penale în cauză și, pe de altă parte, să aibă o poziție de neutralitate față de părțile din procedura penală. Or, această situație nu se regăsește în cazul unui Minister Public precum Ministerul Public estonian care conduce procedura de investigare și exercită, dacă este cazul, acțiunea publică. Rezultă că Ministerul Public nu este în măsură să efectueze controlul prealabil sus-menționat.

---

**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. Este de competența instanței naționale să soluționeze 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 Paiova ☎ (+352) 4303 4293*

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