LOVITURA CJUE – Hotarare istorica a Curtii de Justitie a Uniunii Europene care limiteaza ingerinta autoritatilor in viata privata: „Accesul, in scopuri penale, la un ansamblu de date de transfer sau de localizare privind comunicatiile electronice, care permit deducerea unor concluzii precise cu privire la viata privata, nu este autorizat decat in vederea combaterii infractionalitatii grave sau a prevenirii amenintarilor grave la adresa sigurantei publice”

Scris de Valentin BUSUIOC | Data: 02.03.2021 16:49

Autoritatile nu trebuie sa se inghesuie a-si supraveghea in masa propriii cetateni, ci trebuie sa se asigure ca ingerintele intreprinse in viata privata a oamenilor sunt proportionale cu gravitatea infractiunilor prevenite. Altfel spus: masurile de tip Big Brother nu trebuie luate decat pentru combaterea infractionalitatii grave sau pentru prevenirea unor amenintari grave la adresa sigurantei publice.

Este principala idee exprimata de catre Curtea de Justitie a Uniunii Europene (CJUE) marti, 2 martie 2021, in cauza C-746/18, in care H.K., o femeie din Estonia, a fost condamnata pentru furt, utilizare a cardului bancar al unui tert si violenta fata de persoane care participa la o procedura judiciara. Problema este ca aceste infractiuni au fost constatate, in mod special, pe baza unor date cu caracter personal generate in cadrul furnizarii unor servicii de comunicatii electronice. Or, ***„accesul, in scopuri penale, la un ansamblu de date de transfer sau de localizare privind comunicatiile electronice, care permit deducerea unor concluzii precise cu privire la viata privata, nu este autorizat decat in vederea combaterii infractionalitatii grave sau a prevenirii amenintarilor grave la adresa sigurantei publice”***, subliniaza CJUE.

„*Dreptul Uniunii se opune de altfel unei reglementari nationale care confera Ministerului Public competenta de a autoriza accesul unei autoritati publice la aceste date pentru a desfasura o urmarire penala*”, adauga judecatorii Curtii de Justitie a UE, evidentiind **necesitatea unui control din partea unei instante sau a unei entitati independente cu privire la respectarea dreptului la viata privata**.

Prezentam comunicatul CJUE (vezi facsimil):

„Accesul, in scopuri penale, la un ansamblu de date de transfer sau de localizare privind comunicatiile electronice, care permit deducerea unor concluzii precise cu privire la viata privata, nu este autorizat decat in vederea combaterii infractionalitatii grave sau a prevenirii amenintarilor grave la adresa sigurantei publice

Dreptul Uniunii se opune de altfel unei reglementari nationale care confera Ministerului Public competenta de a autoriza accesul unei autoritati publice la aceste date pentru a desfasura o urmarire penala

In Estonia s-a initiat o procedura penala impotriva lui H. K. pentru infractiunile de furt, de utilizare a cardului bancar al unui tert si de violenta fata de persoane care participa la o procedura judiciara. H.K. a fost condamnata pentru aceste infractiuni de un Tribunal de Prima Instanta la o pedeapsa cu inchisoarea de doi ani. Ulterior, aceasta

decizie a fost confirmata in apel.

Procesele verbale pe care este intemeiata constatarea acestor infractiuni au fost intocmite, in mod special, pe baza unor date cu caracter personal generate in cadrul furnizarii unor servicii de comunicatii electronice. Riigikohus (Curtea Suprema, Estonia), in fata careia H.K a declarat recurs, a exprimat indoieli cu privire la compatibilitatea cu dreptul Uniunii a conditiilor in care serviciile de investigare au avut acces la aceste date.

Aceste indoieli privesc in primul rand aspectul daca intinderea perioadei pentru care serviciile de investigare au avut acces la date constituie un criteriu care permite sa se evalueze gravitatea ingerintei constituite de acest acces in drepturile fundamentale ale persoanelor vizate. Astfel, in cazul in care aceasta perioada este foarte scurta sau volumul datelor colectate este foarte limitat, instanta de trimitere a ridicat problema stabilirii faptului daca obiectivul privind combaterea criminalitatii in general, iar nu numai a criminalitatii grave, poate justifica o asemenea ingerinta. In al doilea rand, instanta de trimitere a avut indoieli cu privire la posibilitatea de a considera ca Ministerul Public estonian, tinand seama de diferitele misiuni care ii sunt incredintate de reglementarea nationala, este o autoritate administrativa „independenta" in sensul Hotararii Tele2 Sverige si Watson si altii, susceptibila sa autorizeze accesul autoritatii de investigare la datele vizate.

Prin hotararea sa, pronuntata in Marea Camera, Curtea statueaza ca Directiva asupra confidentialitatii si comunicatiilor electronice, citita in lumina cartei, se opune unei reglementari nationale care permite accesul autoritatilor publice la un ansamblu de date de transfer sau de date de localizare, care pot sa furnizeze informatii cu privire la comunicatiile efectuate de un utilizator al unui mijloc de comunicare electronica sau cu privire la localizarea echipamentelor terminale pe care le utilizeaza acesta si sa permita sa se deduca concluzii precise cu privire la viata sa privata, in scopul prevenirii, investigarii, detectarii si urmaririi penale a infractiunilor, fara ca acest acces sa fie limitat la proceduri care vizeaza combaterea infractionalitatii grave sau prevenirea amenintarilor grave la adresa sigurantei publice. Potrivit Curtii, intinderea perioadei pentru care se solicita accesul la aceste date si volumul sau natura datelor disponibile pentru o astfel de perioada nu sunt relevante in aceasta privinta. In plus, Curtea considera ca aceeasi directiva, citita in lumina cartei, se opune unei reglementari nationale care confera Ministerului Public competenta de a autoriza accesul unei autoritati publice la datele de transfer si la datele de localizare in scopul desfasurarii unei urmariri penale.

Aprecierea Curtii

In ceea ce priveste conditiile in care autoritatilor publice li se poate acorda accesul la datele de transfer si la datele de localizare stocate de furnizorii de servicii de comunicatii electronice, in scopul prevenirii, investigarii, detectarii si urmaririi penale a infractiunilor, in aplicarea unei masuri adoptate in temeiul Directivei asupra confidentialitatii si comunicatiilor electronice, Curtea a amintit ceea ce a statuat in Hotararea La Quadrature du Net si altii. Astfel, aceasta directiva nu permite statelor membre sa adopte, intre altele in aceste scopuri, masuri legislative pentru a restrange sfera de aplicare a drepturilor si obligatiilor prevazute de aceasta directiva, in special obligatia de a asigura confidentialitatea comunicatiilor si a datelor de transfer, decat cu respectarea principiilor generale de drept al Uniunii, printre care figureaza principiul proportionalitatii, si a drepturilor fundamentale garantate de carta. In acest cadru, directiva se opune unor masuri legislative care impun furnizorilor de servicii de comunicatii electronice, cu titlu preventiv, o stocare generalizata si nediferentiata a datelor de transfer si a datelor de localizare.

In ceea ce priveste obiectivul de prevenire, investigare, detectare si urmarire penala a infractiunilor, urmarit prin reglementarea in discutie, in conformitate cu principiul proportionalitatii, Curtea considera ca numai obiectivele de combatere a infractionalitatii grave sau de prevenire a amenintarilor grave pentru siguranta publica sunt de natura sa justifice accesul autoritatilor publice la un ansamblu de date de transfer sau de date de localizare, care permit deducerea unor concluzii precise privind viata privata a persoanelor vizate, fara ca alti factori referitori la proportionalitatea unei cereri de acces, precum perioada pentru care se solicita accesul la astfel de date, sa poata avea ca efect ca obiectivul de prevenire, investigare, detectare si urmarire penala a infractiunilor in general sa fie susceptibil sa justifice un astfel de acces.

In ceea ce priveste competenta conferita Ministerului Public de a autoriza accesul unei autoritati publice la datele de transfer si la datele de localizare pentru a desfasura o urmarire penala, Curtea aminteste ca revine dreptului national sarcina de a stabili conditiile in care furnizorii de servicii de comunicatii electronice trebuie sa acorde autoritatilor nationale competente accesul la datele de care dispun. Pentru a indeplini cerinta proportionalitatii, o astfel de reglementare trebuie sa prevada insa norme clare si precise care sa reglementeze continutul si aplicarea masurii respective si sa impuna o serie de cerinte minime

astfel incat persoanele ale caror date cu caracter personal sunt vizate sa dispuna de garantii suficiente care sa permita protejarea in mod eficient a acestor date impotriva riscurilor de abuz. Aceasta reglementare trebuie sa aiba forta juridica obligatorie in dreptul intern si in special sa indice in ce imprejurari si in ce conditii poate fi luata o masura care prevede prelucrarea unor asemenea date, garantand in acest mod ca o ingerinta este limitata la strictul necesar.

Potrivit Curtii, in scopul de a garanta, in practica, deplina respectare a acestor conditii, este esential ca accesul autoritatilor nationale competente la datele stocate sa fie conditionat de un control prealabil efectuat fie de o instanta, fie de o entitate administrativa independenta si ca decizia acestei instante sau a acestei entitati sa intervina in urma unei cereri motivate formulate de autoritatile respective, printre altele in cadrul unor proceduri de prevenire, de detectare sau de urmarire penala. In caz de urgenta justificata corespunzator, controlul trebuie sa aiba loc in termene scurte.

In aceasta privinta, Curtea precizeaza ca un control prealabil impune, printre altele, ca instanta sau entitatea insarcinata cu efectuarea controlului prealabil mentionat sa dispuna de toate atributiile si sa prezinte toate garantiile necesare in vederea asigurarii unei concilieri a diferitor interese si drepturi in cauza. In ceea ce priveste mai concret o investigatie penala, un asemenea control impune ca aceasta instanta sau aceasta entitate sa fie in masura sa asigure un just echilibru intre, pe de o parte, interesele legate de nevoile investigatiei in cadrul combaterii infractionalitatii si, pe de alta parte, drepturile fundamentale la respectarea vietii private si la protectia datelor cu caracter personal ale persoanelor ale caror date sunt vizate prin acces. Atunci cand acest control nu este efectuat de o instanta, ci de o entitate administrativa independenta, aceasta trebuie sa beneficieze de un statut care sa ii permita sa actioneze in cadrul exercitarii misiunilor sale in mod obiectiv si impartial si trebuie sa fie, in acest scop, protejata de orice influenta externa.

In opinia Curtii, din acestea rezulta ca cerinta privind independenta pe care trebuie sa o indeplineasca autoritatea insarcinata cu exercitarea controlului prealabil impune ca aceasta autoritate sa aiba calitatea de tert in raport cu cea care solicita accesul la date, astfel incat prima sa fie in masura sa exercite respectivul control in mod obiectiv si impartial la adapost de orice influenta exterioara. In special, in domeniul penal, cerinta privind independenta presupune ca autoritatea insarcinata cu acest control prealabil, pe de o parte, sa nu fie implicata in desfasurarea investigatiei penale in cauza si, pe de alta parte, sa aiba o pozitie de neutralitate fata de partile din procedura penala. Or, aceasta situatie nu se regaseste in cazul unui Minister Public precum Ministerul Public estonian care conduce procedura de investigare si exercita, daca este cazul, actiunea publica. Rezulta ca Ministerul Public nu este in masura sa efectueze controlul prealabil sus-mentionat”.

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

Presă și informare

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 [1] 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 [2], susceptibilă să autorizeze accesul autorității 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,

[1] 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").

[2] 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 urmăriri 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[3], Curtea a amintit ceea ce a statuat în Hotărârea La Quadrature du Net și alții [4]. 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 [5], decât cu respectarea principiilor generale de drept al Uniunii, printre care figurează principiul proporționalității, și a drepturilor fundamentale garantate de cartă[6]. 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

[3] Articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice.
[4] 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
[5] Articolul 5 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice.
[6] 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 concilieri 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.

---

sursa foto: LSCV.ch