

HOTĂRÂREA C.J.U.E. C-548/21 DIN 4 OCTOMBRIE 2024

Necesitatea existenței unei autorizații prealabile emise de o instanță sau de o entitate administrativă independentă în ipoteza tentativei de accesare de către poliție a datelor conținute într-un telefon mobil. Accesarea de către poliție a respectivelor date nu este limitată în mod necesar la combaterea criminalității grave. Necesitatea informării, în prealabil, a titularului telefonului despre motivele care stau la baza respectivei accesări



Av. Răzvan-Gabriel DALU

Abstract: *An austrian court has decided to refer three preliminary questions to the Court of Justice of the European Union regarding the interpretation of European legal provisions on the protection of personal data contained in a mobile phone and processed in criminal proceedings. On this occasion, the Court of Justice of the European Union clarified a multitude of aspects regarding the interpretation and application of the relevant legal provisions.*

Keywords: *Court of Justice of the European Union, Charter of fundamental rights, protection of personal data, the principle of proportionality*

I. ASPECTE INTRODUCTIVE ȘI CADRUL LEGAL ÎN MATERIE

Cauza C-548/21 a avut ca obiect o cerere de decizie preliminară formulată de Tribunalul Administrativ Regional din Tirol (Austria), în temeiul articolului 267 TFUE, în cadrul unui litigiu între numitul CG și autoritatea administrativă a districtului Landeck (Austria), în legătură cu ridicarea telefonului mobil al lui CG de către autoritățile de poliție și cu încercările acestora de a debloca telefonul pentru a accesa datele conținute în acesta, în cadrul unei anchete desfășurate în materie de trafic de stupefiante.

Cererea a privit interpretarea art. 5 și a art. 15 alin. (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), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 [denumită în continuare „Directiva 2002/58”], citite în

coroborare cu art. 7, 8, 11, 41 și 47 din Carta drepturilor fundamentale a Uniunii Europene [denumită în continuare „Carta”], precum și a art. 52 alin. (1) din Cartă.

Art. 1 din Directiva 2002/58 prevede următoarele: „(1) Prezenta directivă prevede armonizarea dispozițiilor naționale, lucru necesar în vederea asigurării unui nivel echivalent de protecție a drepturilor și a libertăților fundamentale, în special a dreptului la confidențialitate și la respectarea vieții private, în domeniul prelucrării de date cu caracter personal în sectorul comunicațiilor electronice și a asigurării liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Comunității. (...) (3) Prezenta directivă nu se aplică activităților care nu sunt cuprinse în domeniul de aplicare al [Tratatului FUE], cum sunt cele menționate la titlurile V și VI ale Tratatului [UE], și în orice caz activităților legate de siguranța publică, de apărare, de siguranța statului (inclusiv de bunăstarea economică a acestuia, dacă activitățile respective sunt legate de chestiuni de siguranță a statului), și activităților statului în domeniul legii penale”.

Art. 5 din aceeași directivă prevede următoarele: „Statele membre trebuie să asigure confidențialitatea comunicațiilor și a datelor de transfer aferente transmise prin intermediul unei rețele de comunicații publice sau unor servicii publice de comunicații electronice, prin legislația internă. Acestea interzic astfel în special ascultarea, înregistrarea, stocarea sau alte tipuri de interceptare sau supraveghere a comunicațiilor și a datelor de transfer aferente de către persoane altele decât utilizatorul, fără acordul utilizatorului în cauză, cu excepția cazurilor în care acest lucru este permis în temeiul articolului 15 alineatul (1). Prezentul alineat nu interzice stocarea tehnică necesară pentru transmisia comunicației care nu aduce atingere principiului confidențialității”.

Art. 15 alin. (1) din directiva menționată prevede următoarele: „Statele membre pot adopta măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 ale prezentei directive, în cazul în care restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46/CE (...). În acest scop, statele membre pot adopta, inter alia, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat. Toate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale ale legislației comunitare, inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [TUE]”.

Considerentele (2), (4), (7), (10), (11), (15), (26), (44), (46) și (104) ale Directivei 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului [denumită în continuare „Directiva 2016/680”] au următorul cuprins:

➤ „(2) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, să respecte drepturile și libertățile fundamentale ale acestora, în special dreptul la protecția datelor cu caracter personal. Prezenta directivă urmărește să contribuie la realizarea unui spațiu de libertate, securitate și justiție”.

➤ „(4) Libera circulație a datelor cu caracter personal între autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora în cadrul Uniunii, și transferul de astfel de date cu caracter personal către țări terțe și organizații internaționale ar trebui facilitate asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal. (...)”.

➤ „(7) Asigurarea unui nivel omogen și ridicat de protecție a datelor cu caracter personal ale persoanelor fizice și facilitarea schimbului de date cu caracter personal între autoritățile competente ale statelor membre sunt esențiale pentru a se garanta eficacitatea cooperării judiciare în materie penală și a cooperării polițienești. În acest scop, nivelul de protecție a drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, ar trebui să fie echivalent în toate statele membre. Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea drepturilor persoanelor vizate și a obligațiilor celor care prelucrează date cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele în materie de protecție a datelor cu caracter personal în statele membre”.

➤ „(10) În Declarația nr. 21 cu privire la protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, anexată la actul final al Conferinței interguvernamentale care a adoptat Tratatul de la Lisabona, conferința a recunoscut că s-ar putea dovedi necesare norme specifice privind protecția datelor cu caracter personal și libera circulație a datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești în temeiul art. 16 TFUE, având în vedere natura specifică a acestor domenii”.

➤ „(11) Prin urmare, domeniile menționate ar trebui să fie reglementate printr-o directivă care să stabilească norme specifice privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, cu respectarea naturii speciale a activităților în cauză. Pot reprezenta astfel de autorități competente nu numai autoritățile publice, precum autoritățile judiciare, poliția sau alte autorități de aplicare a legii, ci și orice alt organism sau altă entitate însărcinată prin dreptul intern să exercite autoritatea publică și competențe publice în sensul prezentei directive. În cazul în care un astfel de organism sau de entitate prelucrează date cu caracter personal în alte scopuri decât cele urmărite de prezenta directivă, se aplică Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind

protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1)]. (...)”.

➤ „(15) (...) Armonizarea drepturilor statelor membre nu ar trebui să aibă ca rezultat diminuarea nivelului de protecție a datelor cu caracter personal pe care îl oferă statele respective, ci ar trebui, dimpotrivă, să urmărească să asigure un înalt nivel de protecție în cadrul Uniunii. Statele membre nu ar trebui să fie împiedicate să prevadă garanții mai mari decât cele stabilite în prezenta directivă pentru protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente”.

➤ „(26) (...) Datele cu caracter personal ar trebui să fie adecvate și relevante pentru scopurile în care sunt prelucrate. În special, ar trebui să se asigure faptul că datele cu caracter personal colectate nu sunt excesive și că nu sunt stocate mai mult timp decât este necesar pentru îndeplinirea scopului în care sunt prelucrate. Datele cu caracter personal ar trebui prelucrate doar în cazul în care scopul prelucrării nu poate fi îndeplinit, în mod rezonabil, prin alte mijloace. (...)”.

➤ „(44) Statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării sau a omiterii informării persoanelor vizate sau în vederea restricționării, integrale sau parțiale, a accesului la datele lor cu caracter personal, în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, pentru a se apăra securitatea publică sau securitatea națională ori pentru a se apăra drepturile și libertățile altor persoane. Operatorul ar trebui să evalueze, prin intermediul unei examinări concrete și individuale a fiecărui caz în parte, dacă dreptul de acces ar trebui să fie limitat parțial sau complet”.

➤ „(46) Orice limitare a drepturilor persoanei vizate trebuie să fie în conformitate cu carta și cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950, după cum a fost interpretată de jurisprudența Curții de Justiție a Uniunii Europene și, respectiv, a Curții Europene a Drepturilor Omului și, îndeosebi, trebuie să respecte esența drepturilor și libertăților respective”.

➤ „(104) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de cartă, astfel cum sunt consacrate în TFUE, în special dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la o cale de atac eficientă și la un proces echitabil. Limitările aduse acestor drepturi sunt în conformitate cu art. 52 alin. (1) din cartă întrucât sunt necesare pentru atingerea obiectivelor de interes general recunoscute de Uniune sau pentru a proteja drepturile și libertățile celorlalți”.

Art. 1 din Directiva 2016/680 prevăd următoarele: „(1) Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării

sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. (2) În conformitate cu prezenta directivă, statele membre: (a) protejează drepturile și libertățile fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal și (b) se asigură că schimbul de date cu caracter personal de către autoritățile competente în cadrul Uniunii, în cazul în care schimbul respectiv de informații este impus de dreptul Uniunii sau de dreptul intern, nu este limitat sau interzis din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal”.

Art. 2 din Directiva 2016/680 prevede la alin. (1) că aceasta „se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la art. 1 alin. (1)”, iar alin. (3) lit. a) din același articol prevede că „prezenta directivă nu se aplică prelucrării datelor cu caracter personal în cadrul unei activități care nu intră sub incidența dreptului Uniunii”.

Potrivit art. 3 din Directiva 2016/680 prevede că, „în sensul prezentei directive:

➤ Pct. 1: „date cu caracter personal» înseamnă orice informație privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identifiant online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale”;

➤ Pct. 2: „prelucrare» înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvoltarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea”;

➤ Pct. 7: „autoritate competentă» înseamnă: (a) orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora, sau (b) orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora”.

Art. 4 din Directiva 2016/680 prevede la alin. (1) că „statele membre garantează că datele cu caracter personal: (a) sunt prelucrate în mod legal și echitabil; (b) sunt colectate în scopuri determinate, explicate și legitime și nu sunt prelucrate într-un mod incompatibil cu aceste scopuri; (c) sunt adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate; (...)”.

Art. 6 din Directiva 2016/680 prevede că „statele membre garantează că, după caz și în măsura posibilului, operatorul face distincție clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, precum: (a) persoane în privința cărora există motive

serioase să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune; (b) persoane condamnate pentru săvârșirea unei infracțiuni; (c) victime ale unei infracțiuni sau persoane în privința cărora, în baza anumitor fapte, există motive să se creadă că persoanele respective ar putea fi victimele unei infracțiuni și (d) alte părți care au legătură cu infracțiunea, ca de exemplu persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracțiuni sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informații cu privire la infracțiuni sau persoane care sunt în legătură sau asociate cu persoanele menționate la literale (a) și (b)”.

Art. 10 din Directiva 2016/680, intitulat „Prelucrarea de categorii speciale de date cu caracter personal”, are următorul cuprins: „Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice este autorizată numai atunci când este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate și numai atunci când: (a) este autorizată de dreptul Uniunii sau de dreptul intern; (b) este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice sau (c) prelucrarea respectivă se referă la date care sunt făcute publice în mod manifest de persoana vizată”.

Art. 13 din Directiva 2016/680, intitulat „Informații care se pun la dispoziția persoanei vizate sau se comunică acesteia”, prevede următoarele:

➤ Alin. (1): „Statele membre garantează că operatorul pune la dispoziția persoanelor vizate cel puțin următoarele informații: (a) identitatea și datele de contact ale operatorului; (b) dacă este cazul, datele de contact ale responsabilului cu protecția datelor; (c) scopurile în care sunt prelucrate datele cu caracter personal; (d) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere; (e) existența dreptului de a solicita operatorului acces la datele cu caracter personal referitoare la persoana vizată ori rectificarea sau ștergerea acestor date sau restricționarea prelucrării lor”.

➤ Alin. (2): „În plus față de informațiile menționate la alineatul (1), statele membre garantează prin lege că operatorul comunică persoanei vizate, în anumite cazuri, următoarele informații suplimentare, pentru a permite acesteia exercitarea drepturilor sale: (a) temeiul juridic al prelucrării; (b) perioada pentru care vor fi stocate datele cu caracter personal sau, în cazul în care nu este posibil, criteriile utilizate pentru a stabili respectiva perioadă; (c) dacă este cazul, categoriile de destinatari ai datelor cu caracter personal, inclusiv în țări terțe sau organizații internaționale; (d) în cazul în care este necesar, informații suplimentare, în special atunci când datele cu caracter personal sunt colectate fără știrea persoanei vizate.”

➤ Alin. (3): „Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a furnizării de informații persoanei vizate în conformitate cu alin. (2) în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de drepturile fundamentale și de interesele legitime ale persoanei fizice, pentru: (a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice; (b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea

penală a infracțiunilor sau executarea pedepselor; (c) protejarea securității publice; (d) protejarea securității naționale; (e) protejarea drepturilor și libertăților celorlalți”.

Art. 54 din Directiva 2016/680, intitulat „Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau a unei persoane împuternicite de către operator”, prevede că, „fără a aduce atingere vreunei căi de atac administrative sau extrajudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în conformitate cu art. 52, statele membre garantează persoanei vizate dreptul la exercitarea unei căi de atac judiciare eficiente în cazul în care aceasta consideră că, prin prelucrarea datelor sale cu caracter personal cu nerespectarea dispozițiilor adoptate în temeiul prezentei directive, au fost încălcate drepturile care îi revin în conformitate cu dispozițiile respective”.

II. ASPECTELE ÎNVEDERATE DE TRIBUNALUL ADMINISTRATIV REGIONAL DIN TIROL

În anul 2021, în timpul unui control cu privire la stupefiante, vameșii din Innsbruck au interceptat un pachet adresat lui CG care conținea 85 de grame de canabis, pachet ce a fost transmis spre examinare la Comisariatul central de poliție din St. Anton am Arlberg.

Ulterior, doi agenți de poliție ai acestui comisariat au efectuat o percheziție la domiciliul lui CG, în cursul căreia l-au interogată cu privire la expeditorul pachetului menționat și i-au percheziționat locuința. În timpul percheziției, polițiștii au solicitat accesul la datele de conexiune ale telefonului mobil al lui CG. Ca urmare a refuzului exprimat de acesta din urmă, aceștia au procedat la ridicarea telefonului mobil respectiv, inclusiv o cartelă SIM și un card SD, și i-au înmănat lui CG procesul-verbal de ridicare.

Ulterior, telefonul mobil a fost predat, în vederea deblocării, unui expert al postului de poliție din districtul Landeck. Având în vedere că acesta nu a reușit să deblocheze telefonul, acesta a fost trimis la Oficiul Federal al Poliției Judiciare din Viena, unde s-a încercat din nou deblocarea lui.

Deosebit de important de menționat este că ridicarea telefonului mobil, precum și încercările ulterioare de deblocare a acestui telefon au fost efectuate din proprie inițiativă de ofițerii de poliție vizați, fără ca ei să fi fost autorizați în acest sens de Ministerul Public sau de o instanță.

Având în vedere cele prezentate, numitul CG a introdus o acțiune la Tribunalul Administrativ Regional din Tirol, care este și instanța de trimitere din prezenta cauză, acțiune ce are ca obiect contestarea legalității ridicării telefonului său mobil. Ulterior, telefonul i-a fost returnat la 20 aprilie 2021.

Instanța de trimitere reține că persoana în cauză nu a fost informată imediat cu privire la tentativele de deblocare a telefonului său mobil, CG luând cunoștință de acestea abia atunci când agentul de poliție care a ridicat telefonul și a inițiat ulterior

analiza digitală a fost interogat în calitate de martor în cadrul procedurii din fața instanței de trimitere.

De asemenea, tentativele de deblocare a telefonului nu au fost documentate în dosarul poliției judiciare.

Având în vedere cele prezentate, instanța de trimitere ridică, în primul rând, problema dacă art. 15 alin. (1) din Directiva 2002/58, citit în lumina art. 7 și 8 din cartă, trebuie interpretat în sensul că un acces complet și necontrolat la toate datele conținute într-un telefon mobil, și anume datele de conexiune, conținutul comunicațiilor, fotografiile și istoricul navigării, care pot oferi o imagine foarte detaliată și aprofundată a aproape tuturor domeniilor vieții private a persoanei vizate, constituie o ingerință atât de gravă în drepturile fundamentale consacrate la art. 7 și 8 încât, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, acest acces trebuie să fie limitat la combaterea infracțiunilor grave.

Sub acest aspect, instanța de trimitere precizează că fapta pentru care este acuzat CG este prevăzută la art. 27 alin. (1) din Legea privind stupefiantele, care se pedepsește cu o pedeapsă cu închisoarea de cel mult un an și nu constituie, în raport cu clasificarea de la art. 17 din StGB, decât o contravenție.

În al doilea rând, instanța de trimitere ridică problema dacă art. 15 alin. (1) din Directiva 2002/58 se opune unei reglementări naționale precum cea care rezultă din art. 18 coroborat cu art. 99 alin. (1) din StPO, în temeiul cărora, în cursul unei proceduri de urmărire penală, poliția judiciară poate obține, fără autorizarea unei instanțe sau a unei entități administrative independente, un acces complet și necontrolat la toate datele digitale conținute într-un telefon mobil.

În al treilea rând, după ce precizează că art. 18 din StPO coroborat cu art. 99 alin. (1) din StPO nu prevede nicio obligație a autorităților polițienești de a documenta măsurile de examinare digitală a unui telefon mobil sau chiar de a informa proprietarul acestuia cu privire la existența unor asemenea măsuri, astfel încât acesta să poată formula opoziție, dacă este cazul, printr-o cale de atac jurisdicțională preventivă sau a posteriori, instanța de trimitere ridică problema compatibilității acestor dispoziții din StPO cu principiul egalității armelor și cu dreptul la o cale de atac jurisdicțională efectivă, în sensul articolului 47 din cartă.

III. ÎNTREBĂRILE PRELIMINARE ADRESATE DE TRIBUNALUL ADMINISTRATIV REGIONAL DIN TIROL

În aceste condiții, Tribunalul Administrativ Regional din Tirol a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

➤ „1) Art. 15 alin. (1) din Directiva 2002/58, eventual coroborat cu art. 5 din aceasta, citit în lumina art. 7 și 8 din cartă, trebuie interpretat în sensul că accesul autorităților publice la datele stocate în telefoanele mobile constituie o atingere suficient de gravă adusă principiilor fundamentale consacrate la aceste articole din

cartă încât, în domeniul prevenirii, investigării, depistării și urmăririi penale a unor infracțiuni, acest acces trebuie limitat la combaterea criminalității grave?”

➤ „2) Art. 15 alin. (1) din Directiva 2002/58 trebuie interpretat, în lumina art. 7, 8 și 11, precum și a art. 52 alin. (1) din cartă, în sensul că se opune unei reglementări naționale precum art. 18 coroborat cu art. 99 alin. (1) din StPO, potrivit căruia, în cursul unei proceduri de urmărire penală, autoritățile de securitate își obțin ele însele, fără autorizarea unei instanțe sau a unui organism independent, un acces complet și necontrolat la toate datele digitale stocate într-un telefon mobil?”

➤ „3) Art. 47 din cartă coroborat cu art. 41 și 52 din aceasta trebuie interpretat, din punctul de vedere al egalității armelor și al unei căi de atac efective, în sensul că se opune unei reglementări a unui stat membru, precum art. 18 coroborat cu art. 99 alin. (1) din StPO, care permite examinarea datelor digitale dintr-un telefon mobil fără ca persoana vizată să fie informată cu privire la aceasta înainte sau măcar după adoptarea măsurii?”

IV. ASPECTELE REȚINUTE DE CURTEA DE JUSTIȚIE A UNIUNII EUROPENE

4.1. Aspecte reținute de C.J.U.E. cu privire la aplicarea în cauză a Directivei 2016/680

După o analiză aprofundată a mai multor dispoziții procedurale referitoare la admisibilitatea sesizării formulate de instanța de trimitere, cu precădere efectuată asupra modalității de formulare a întrebărilor, respectiv trimiterea expresă la Directiva 2002/58, iar nu la Directiva 2016/680, Curtea de Justiție a Uniunii Europene, în baza unei jurisprudențe deja consolidate, a considerat admisibile întrebările formulate și a procedat la analiza pe fond a acestora.

În ceea ce privește incidența Directivei 2016/680 în cazul unei tentative de accesare a datelor conținute într-un telefon mobil, Curtea a reținut că din însuși modul de redactare a art. 3 pct. 2 din directivă anterior citat și în special din utilizarea expresiilor „orice operațiune”, „orice set de operațiuni” și „punerea la dispoziție în orice alt mod”, rezultă că legiuitorul Uniunii a intenționat să confere o sferă largă noțiunii de „prelucrare” și, prin urmare, domeniului de aplicare material al directivei.

Astfel, Curtea a statuat că această interpretare este confirmată de caracterul neexhaustiv, exprimat prin locuțiunea „cum ar fi”, al operațiunilor menționate în articolul menționat¹.

Prin urmare, atunci când autoritățile polițienești ridică un telefon și îl manipulează în scopul extragerii și al consultării datelor cu caracter personal

¹ A se vedea, prin analogie, Hotărârea din 24 februarie 2022, Valsts ieņēmumu dienests (Prelucrarea datelor cu caracter personal în scopuri fiscale), C-175/20, EU:C:2022:124, punctul 35.

conținute în telefon, acestea efectuează o prelucrare, în sensul art. 3 pct. 2 din Directiva 2016/680, chiar dacă acestea nu reușesc, din motive tehnice, să acceseze datele.

În final, Curtea reține că o asemenea interpretare este conformă cu principiul securității juridice, care impune ca aplicarea normelor de drept să fie previzibilă pentru justițiabili, mai ales atunci când ele pot produce consecințe defavorabile². Prin urmare, o interpretare potrivit căreia aplicabilitatea Directivei 2016/680 ar depinde de succesul tentativei de accesare a datelor cu caracter personal conținute într-un telefon mobil ar crea atât pentru autoritățile naționale competente, cât și pentru justițiabili o incertitudine incompatibilă cu acest principiu.

4.2. Aspecte reținute de C.J.U.E. cu privire la primele două întrebări

Cu titlu prealabil, Curtea precizează că trebuie să se considere că, prin intermediul primei și al celei de a doua întrebări, care trebuie analizate împreună, instanța de trimitere solicită în esență să se stabilească dacă art. 4 alin. (1) lit. (c) din Directiva 2016/680, interpretat în lumina art. 7 și 8, precum și a art. 52 alin. (1) din cartă, se opune unei reglementări naționale care acordă autorităților competente posibilitatea de a accesa datele conținute într-un telefon mobil în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor în general și care nu supune exercitarea acestei posibilități unui control prealabil de către o instanță sau de către o entitate administrativă independentă.

Potrivit art. 4 alin. (1) litera (c) din Directiva 2016/680, statele membre trebuie să garanteze că datele cu caracter personal sunt adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate, astfel că această dispoziție impune respectarea de către statele membre a principiului „reducerii la minimum a datelor”³.

În această privință, trebuie precizat că astfel cum prevede considerentul (104) din directivă, limitările ce nu sunt permise să fie aduse dreptului la protecția datelor cu caracter personal, prevăzut la art. 8 din cartă, precum și dreptului la respectarea vieții private și de familie, protejat de art. 7 din această cartă, trebuie interpretate în conformitate cu cerințele art. 52 alin. (1) din aceasta, care includ respectarea principiului proporționalității⁴.

Prin urmare, aceste drepturi fundamentale nu sunt absolute, astfel că orice restrângere a exercițiului acestora trebuie, în conformitate cu art. 52 alin. (1) din cartă, să fie prevăzută de lege și să respecte substanța aceluiași drepturi fundamentale, precum și principiul proporționalității.

² Hotărârea din 27 iunie 2024, Gestore dei Servizi Energetici, C-148/23, EU:C:2024:555, punctul 42 și jurisprudența citată.

³ Hotărârea din 30 ianuarie 2024, Direktor na Glavna direktsia „Natsionalna politisia” pri MVR – Sofia, C-118/22, EU:C:2024:97, punctul 41 și jurisprudența citată.

⁴ *Ibidem*, pct. 33.

În acest context, precum și în aplicarea principiului proporționalității, Curtea reține că pot fi impuse limitări numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și a libertăților celorlalți, astfel că acestea trebuie să fie efectuate în limitele strictului necesar, iar reglementarea care cuprinde limitările trebuie să prevadă norme clare și precise care să guverneze conținutul și aplicarea acestor limitări⁵.

În ceea ce privește, în primul rând, obiectivul de interes general care poate justifica o restrângere a exercițiului drepturilor fundamentale consacrate la art. 7 și 8 din cartă, trebuie precizat că o prelucrare de date cu caracter personal în cadrul unei anchete polițienești privind sancționarea unei infracțiuni, cum ar fi o tentativă de accesare a datelor conținute într-un telefon mobil, trebuie considerată în principiu ca răspunzând efectiv unui obiectiv de interes general recunoscut de Uniune, în sensul art. 52 alin. (1) din cartă.

În ceea ce privește, în al doilea rând, cerința caracterului necesar al unei asemenea restrângeri, astfel cu subliniază și considerentul (26) al directivei, această cerință nu este îndeplinită atunci când obiectivul de interes general vizat poate fi atins în mod rezonabil la fel de eficient prin alte mijloace, care să afecteze mai puțin drepturile fundamentale ale persoanelor vizate⁶.

În schimb, cerința necesității este îndeplinită atunci când obiectivul urmărit de prelucrarea datelor în cauză nu poate fi atins în mod rezonabil la fel de eficient prin alte mijloace care să afecteze mai puțin drepturile fundamentale ale persoanelor vizate, în special dreptul la respectarea vieții private și de familie, precum și dreptul la protecția datelor cu caracter personal garantate la art. 7 și 8 din cartă⁷.

În ceea ce privește, în al treilea rând, caracterul proporțional al restrângerii exercițiului drepturilor fundamentale garantate la art. 7 și 8 din cartă, Curtea precizează că acesta implică o ponderare a tuturor elementelor relevante ale speței⁸.

4.2.1. Criteriile avute în vedere de Curte cu ocazia analizării respectării principiului proporționalității

Reține Curtea că printre aceste elemente relevante ale speței fac parte, printre altele:

➤ gravitatea restrângerii aduse astfel exercițiului drepturilor fundamentale în cauză, care depinde de natura și de sensibilitatea datelor la care autoritățile polițienești competente pot avea acces;

⁵ *Ibidem*, pct. 39.

⁶ *Ibidem*, pct. 40.

⁷ Hotărârea din 26 ianuarie 2023, *Ministerstvo na vatreshnite raboti* (Înregistrarea de date biometrice și genetice de către poliție), C-205/21, EU:C:2023:49, punctul 126 și jurisprudența citată.

⁸ A se vedea în acest sens Hotărârea din 30 ianuarie 2024, *Direktor na Glavna direktsia „Natsionalna politسيا” pri MVR – Sofia*, C-118/22, EU:C:2024:97, punctele 62 și 63 și jurisprudența citată.

- importanța obiectivului de interes general urmărit prin această restrângere;
- legătura existentă între titularul telefonului mobil și infracțiunea în cauză sau relevanța datelor în cauză pentru constatarea faptelor.

4.2.1.1. Criteriul referitor la gravitatea restrângerii aduse exercițiului drepturilor fundamentale în cauză

Din decizia de trimitere reiese că reglementarea austriacă permite autorităților polițienești competente să acceseze, fără o autorizație prealabilă, datele conținute într-un telefon mobil.

Un asemenea acces poate privi, în funcție de conținutul telefonului mobil în cauză și de alegerile efectuate de polițiști, nu numai datele de transfer și de localizare, ci și fotografiile și istoricul de navigare pe internet sau chiar o parte a conținutului comunicațiilor efectuate cu telefonul respectiv.

Astfel, Curtea subliniază că accesul la un astfel de ansamblu de date poate permite deducerea unor concluzii foarte precise privind viața privată a persoanei vizate, precum obiceiurile sale din viața cotidiană, locurile de reședință permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestei persoane și mediile sociale frecventate de ea.

Prin urmare, în ceea ce privește primul criteriu, respectiv gravitatea restrângerii drepturilor fundamentale care rezultă dintr-o reglementare, Curtea conchide că ingerința în drepturile fundamentale garantate la art. 7 și 8 din cartă la care poate conduce aplicarea unei reglementări precum cea în discuție trebuie, prin urmare, să fie considerată gravă sau chiar deosebit de gravă.

4.2.1.2. Criteriul referitor la importanța obiectivului urmărit

În ceea ce privește al doilea criteriu, respectiv **importanța obiectivului urmărit**, Curtea subliniază că gravitatea infracțiunii care face obiectul anchetei constituie unul dintre parametrii centrali în cadrul examinării proporționalității ingerinței grave.

Cu toate acestea, Curtea precizează că a se considera că numai combaterea infracționalității grave poate justifica accesul la datele conținute într-un telefon mobil ar limita competențele de investigare ale autorităților competente, în sensul Directivei 2016/680, în privința infracțiunilor în general, considerându-se că ar rezulta o creștere a riscului de impunitate pentru asemenea infracțiuni, ținând seama de importanța pe care o pot avea asemenea date pentru anchetele penale.

În aceste condiții, Curtea conchide că aspectele precizate anterior nu aduc atingere cerinței care decurge din art. 52 alin. (1) din cartă, potrivit căreia orice restrângere a exercițiului unui drept fundamental trebuie să fie „prevăzută de lege”,

revenind legiuitorului național sarcina de a defini în mod suficient de precis elementele, printre altele natura sau categoriile de infracțiuni în cauză, care trebuie luate în considerare.

4.2.1.3. Criteriul referitor la legătura existentă între titularul telefonului mobil cu infracțiunea în cauză, precum și relevanța datelor în cauză pentru constatarea faptelor

În ceea ce privește al treilea criteriu, respectiv legătura existentă între titularul telefonului mobil cu infracțiunea în cauză, precum și relevanța datelor în cauză pentru constatarea faptelor, Curtea menționează că din art. 6 din Directiva 2016/680 reiese că noțiunea de „persoană vizată” acoperă diferite categorii de persoane, și anume, în esență:

➤ persoanele suspectate, pentru motive serioase, că au săvârșit sau că urmează să săvârșească o infracțiune,

➤ persoanele care au fost condamnate pentru săvârșirea unei infracțiuni,

➤ victimele sau victimele potențiale ale unor astfel de infracțiuni, precum și

➤ alte părți care au legătură cu o infracțiune care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracțiuni sau în cadrul procedurilor penale ulterioare.

Astfel, în ceea ce privește accesul la datele conținute în telefonul mobil al persoanei care face obiectul unei anchete penale, precum în cauza principală, existența unor suspiciuni rezonabile în privința acesteia în sensul că a săvârșit, săvârșește sau intenționează să săvârșească o infracțiune ori că este implicată într-un mod sau altul într-o asemenea infracțiune trebuie să fie susținută de elemente obiective și suficiente.

Prin urmare, Curtea conchide că este esențial, în special pentru a asigura că principiul proporționalității este respectat în fiecare caz concret prin efectuarea unei ponderări a tuturor elementelor relevante, ca, atunci când accesul autorităților naționale competente la datele cu caracter personal implică riscul unei ingerințe grave sau chiar deosebit de grave în drepturile fundamentale ale persoanei vizate, acest acces să fie condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă.

În ceea ce privește o anchetă penală, un asemenea control impune ca această instanță sau entitate să fie în măsură să asigure un just echilibru între, pe de o parte, interesele legitime legate de nevoile anchetei 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 de acces.

Acest control independent trebuie să intervină înaintea oricărei tentative de accesare a datelor vizate, cu excepția cazurilor de urgență justificate corespunzător, caz în care controlul menționat trebuie să intervină în termen scurt. Astfel, un control

ulterior nu ar permite îndeplinirea obiectivului controlului prealabil, care constă în împiedicarea autorizării unui acces la datele în cauză care depășește limitele strictului necesar.

Prin urmare, instanța sau entitatea administrativă independentă care intervine în cadrul unui control prealabil efectuat în urma unei cereri de acces motivate care intră în domeniul de aplicare al Directivei 2016/680 trebuie să fie abilitată să refuze sau să restrângă acest acces atunci când constată că ingerința în drepturile fundamentale pe care ar constitui-o accesul menționat ar fi disproporționată ținând seama de ansamblul elementelor relevante.

4.2.2. Soluția pronunțată de C.J.U.E. la primele două întrebări

Sintetizând cele de mai sus, Curtea de Justiție a Uniunii Europene a formulat următorul răspuns la primele două întrebări preliminare:

➤ Art. 4 alin. (1) lit. (c) din Directiva 2016/680, citit în lumina art. 7 și 8, precum și a art. 52 alin. (1) din cartă, trebuie interpretat în sensul că nu se opune unei reglementări naționale care acordă autorităților competente posibilitatea de a accesa datele conținute într-un telefon mobil în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor în general, dacă această reglementare:

- definește într-un mod suficient de precis natura sau categoriile de infracțiuni vizate;
- garantează respectarea principiului proporționalității și
- supune exercitarea acestei posibilități, cu excepția cazurilor de urgență justificate în mod corespunzător, unui control prealabil din partea unei instanțe sau a unei entități administrative independente.

4.3. Aspecte reținute de C.J.U.E. cu privire la a treia întrebare

Reformulând întrebarea adresată de instanța de trimitere, Curtea precizează că trebuie să se considere că se solicită în esență să se stabilească dacă art. 13 și 54 din Directiva 2016/680, citite în lumina art. 47 și a art. 52 alin. (1) din cartă, trebuie interpretate în sensul că se opun unei reglementări naționale care permite autorităților competente în materie penală să încerce să acceseze datele conținute într-un telefon mobil fără a informa persoana în cauză cu privire la aceasta.

Din jurisprudența⁹ Curții reiese că dreptul la o cale de atac judiciară efectivă, garantat la art. 47 din cartă, impune în principiu ca persoana interesată să poată cunoaște motivele pe care se întemeiază decizia luată în privința sa pentru a-i permite să își apere drepturile în cele mai bune condiții posibile și să decidă în

⁹ Hotărârea din 16 noiembrie 2023, Ligue des droits humains (Verificarea prelucrării datelor de către autoritatea de supraveghere), C-333/22, EU:C:2023:874, punctul 58.

deplină cunoștință de cauză dacă este util să sesizeze instanța competentă, precum și pentru a-i permite pe deplin acesteia din urmă să exercite controlul legalității acestei decizii.

Deși acest drept nu constituie o prerogativă absolută și, în conformitate cu art. 52 alin. (1) din cartă, pot fi impuse restrângeri, există condiția ca aceste restrângeri să fie prevăzute de lege, să respecte substanța drepturilor și libertăților în cauză și, cu respectarea principiului proporționalității, să fie necesare și să răspundă efectiv obiectivelor de interes general recunoscute de Uniune sau necesități protejării drepturilor și libertăților celorlalți¹⁰.

Astfel, Curtea reține că revine autorităților naționale competente care au fost autorizate de o instanță sau de o entitate administrativă independentă să acceseze datele stocate sarcina de a informa persoanele vizate, în cadrul procedurilor naționale aplicabile, cu privire la motivele pe care se întemeiază această autorizație, din momentul în care acest lucru nu poate compromite investigațiile desfășurate de aceste autorități, și de a le pune la dispoziție toate informațiile prevăzute la art. 13 alin. (1) din Directiva 2016/680, aceste informații fiind necesare pentru a permite persoanei să își exercite, printre altele, dreptul la o cale de atac, prevăzut în mod explicit la art. 54 din Directiva 2016/680¹¹.

În schimb, o reglementare națională care ar exclude în general orice drept de a obține astfel de informații nu ar fi conformă cu dreptul Uniunii¹².

Astfel, Curtea de Justiție a Uniunii Europene a formulat următorul răspuns la a treia întrebare:

➤ Art. 13 și 54 din Directiva 2016/680, citite în lumina art. 47 și a art. 52 alin. (1) din cartă, trebuie interpretate în sensul că se opun unei reglementări naționale care permite autorităților competente să încerce să acceseze date conținute într-un telefon mobil fără a informa persoana în cauză, în cadrul procedurilor naționale aplicabile, cu privire la motivele pe care se întemeiază autorizația de a accesa astfel de date, emisă de o instanță sau de o entitate administrativă independentă, începând din momentul în care comunicarea acestei informații nu mai este susceptibilă să compromită misiunile care revin acestor autorități în temeiul directivei menționate.

V. CONCLUZII

Din cele prezentate, rezultă modalitatea de aplicare de către Curtea de Justiție a Uniunii Europene a dispozițiilor existente la nivel unional în materia protecției

¹⁰ *Ibidem*, pct. 59.

¹¹ A se vedea în acest sens Hotărârea din 17 noiembrie 2022, *Spetsializirana prokuratura* (Conserarea datelor de trafic și localizare), C-350/21, EU:C:2022:896, punctul 70 și jurisprudența citată.

¹² *Ibidem*, pct. 71.

datelor cu caracter personal prelucrate în cadrul procedurilor penale, aceasta efectuând o amplă analiză a dreptului unional, stabilind noi linii directoare în această materie.

Totodată, Curtea a confirmat și dezvoltat jurisprudența acumulată pe parcursul anilor cu privire la aplicarea concretă a principiului proporționalității, iar unde s-a impus, a adus noi clarificări cu privire la aplicabilitatea prin analogie a unor soluții pronunțate în situații similare.

Având în vedere toate aspectele prezentate, considerăm salutară hotărârea instanței europene, aceasta aducând claritate, previzibilitate și predictibilitate în interpretarea și aplicarea dreptului unional în materia protecției datelor cu caracter personal prelucrate în cadrul procedurilor penale.