CONCLUZIILE AVOCATULUI GENERAL
DOMNUL MANUEL CAMPOS SÁNCHEZ-BORDONA
prezentate la 20 aprilie 2023 [1]

Cauza C-548/21

C. G.
împotriva
Bezirkshauptmannschaft Landeck

[cerere de decizie preliminară formulată de Landesverwaltungsgericht Tirol (Tribunalul Administrativ Regional din Tirol, Austria)]

„Trimitere preliminară – Telecomunicații – Protecția datelor cu caracter personal – Directiva (UE) 2016/680 – Procedură penală – Tentativă a autorităților publice de a accesa datele înregistrate pe un telefon mobil fără autorizarea unei instanțe sau a unei autorități administrative independente”

1. Prezenta cerere de decizie preliminară se referă în esență la condițiile pe care trebuie să le respecte autoritățile polițienești pentru a accesa datele stocate pe telefonul mobil al unei persoane care face obiectul unei anchete penale.

2. Astfel cum vom încerca să explicăm, trimiterea preliminară prezintă deficiențe semnificative în ceea ce privește admisibilitatea sa. În cazul în care Curtea va decide, totuși, să analizeze fondul cauzei, va trebui să se pronunțe cu privire la domeniul de aplicare al Directivei 2002/58/CE [2] și, respectiv, al Directivei (UE) 2016/680 [3].

[1] Limba originală: spaniola.

[2] Directiva 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).

[3] Directiva 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 (JO 2016, L 119, p. 89).

I. Cadrul juridic

A. Dreptul Uniunii

1. Regulamentul (UE) 2016/679[4]

3. Articolul 2 („Domeniul de aplicare material”) alineatul (2) prevede:

„Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

[…]

(d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.”

2. Directiva 2016/680

4. În considerentul (2) se arată:

„Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal ar trebui […] 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.”

5. Considerentul (46) are următorul cuprins:

„Orice limitare a drepturilor persoanei vizate trebuie să fie în conformitate cu Carta și cu CEDO, după cum a fost interpretată de jurisprudența Curții de Justiție și, respectiv, a Curții Europene a Drepturilor Omului[5], și, îndeosebi, trebuie să respecte esența drepturilor și libertăților respective.”

6. În considerentul (49) se arată:

„În cazul în care datele cu caracter personal sunt prelucrate în cadrul unei anchete penale și al unor acțiuni în instanță în materie penală, statele membre ar trebui să poată garanta exercitarea drepturilor la informare, acces și de rectificare sau ștergere a datelor cu caracter personal și de restricționare a prelucrării în conformitate cu normele naționale privind procedurile judiciare.”

7. Articolul 1 („Obiect și obiective”) prevede:

„(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 urmăririi penale a infracțiunilor sau al executării

[4] Regulamentul 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). Denumit în continuare „RGPD”.

[5] Denumită în continuare „Curtea EDO”.

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

[…]

(3) Prezenta directivă nu împiedică statele membre să prevadă garanții sporite față de 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."

8. Articolul 2 („Domeniul de aplicare") alineatul (1) prevede:

„Prezenta directivă se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1)."

9. Articolul 3 („Definiții") stabilește:

„În sensul prezentei directive:

[…]

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, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

[…]

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

[…]"

10. Articolul 4 („Principii referitoare la prelucrarea datelor cu caracter personal") alineatul (1) prevede:

„Statele membre garantează că datele cu caracter personal:

(a) sunt prelucrate în mod legal și echitabil;

(b) sunt colectate în scopuri determinate, explicite 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;

[…]

(e) sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;

(f) sunt prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.”

11. Articolul 8 („Legalitatea prelucrării”) stabilește:

„(1) Statele membre garantează legalitatea prelucrării numai dacă și în măsura în care aceasta este necesară pentru îndeplinirea unei sarcini de către o autoritate competentă în scopurile stabilite la articolul 1 alineatul (1) și că aceasta se întemeiază pe dreptul Uniunii sau pe dreptul intern.

(2) Dreptul intern care reglementează prelucrarea care intră sub incidența prezentei directive precizează cel puțin obiectivele prelucrării, datele cu caracter personal care urmează să fie prelucrate și scopurile prelucrării.”

12. Articolul 13 („Informații care se pun la dispoziția persoanei vizate sau se comunică acesteia”) prevede:

„(1) Statele membre garantează că operatorul pune la dispoziția persoanelor vizate cel puțin următoarele informații:

[…]

(d) dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;

[…]

(3) Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a furnizării de informații persoanei vizate în conformitate cu alineatul (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.

[…]”

13. În conformitate cu articolul 15 („Limitarea dreptului de acces”) alineatul (1):

„Statele membre pot adopta măsuri legislative care limitează, integral sau parțial, dreptul de acces al persoanei vizate în măsura în care și atât timp cât o astfel de limitare, parțială sau totală, constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama de drepturile fundamentale și de interesele legitime ale respectivei persoane 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.”

14. În temeiul articolului 27 („Evaluarea impactului asupra protecției datelor”):

„(1) În cazul în care un tip de prelucrare, în special care implică utilizarea de noi tehnologii, și, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibil să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, statele membre garantează că operatorul, înainte de prelucrare, efectuează o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor cu caracter personal.

(2) Evaluarea menționată la alineatul (1) cuprinde cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea abordării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze respectarea prezentei directive, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate.”

15. Articolul 28 („Consultarea prealabilă a autorității de supraveghere”) prevede:

„(1) Statele membre garantează că operatorul sau persoana împuternicită de către operator consultă autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou de evidență a datelor care urmează a fi creat, în cazul în care:

(a) o evaluare a impactului asupra protecției datelor, prevăzută la articolul 27, indică faptul că prelucrarea ar genera un risc ridicat în absența măsurilor luate de operator pentru atenuarea riscului sau

(b) un tip de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor și libertăților persoanelor vizate.

[…]”

16. Articolul 54 („Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau a unei persoane împuternicite de către operator”) prevede:

„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 articolul 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.”

B. Dreptul național

17. Articolul 18 din Strafprozessordnung[6] atribuie poliției judiciare funcții în serviciul administrării justiției penale [alineatul (1)]. Investigațiile efectuate de poliția judiciară revin în sarcina autorităților de securitate [alineatul (2)]. Organele serviciului de securitate publică prestează serviciul executiv al poliției judiciare, care constă în investigarea și în urmărirea penală a infracțiunilor [alineatul (3)].

18. În conformitate cu articolul 99 din StPO, poliția judiciară efectuează investigații din oficiu sau pe baza unei plângeri și trebuie să respecte ordonanțele Ministerului Public și ale instanțelor [alineatul (1)]. Atunci când o măsură de investigare necesită adoptarea unei ordonanțe de către Ministerul Public, poliția judiciară poate exercita competența corespunzătoare, chiar și în lipsa unei astfel de ordonanțe, în cazul unui pericol iminent. Într-o astfel de situație, aceasta trebuie să solicite imediat o autorizație [alineatul (2)].

19. În conformitate cu articolul 111 alineatul (2) din StPO, în cazul în care informațiile stocate pe suporturi de date trebuie să facă obiectul unei colectări de date, orice persoană este obligată să permită accesul la aceste informații și, la cerere, să furnizeze sau să permită crearea unui suport electronic de date într-un format de arhivare utilizat în mod curent. În plus, trebuie să permită realizarea unei copii de siguranță a informațiilor stocate pe suporturile de date.

II. Situația de fapt, litigiul și întrebările preliminare

20. C. G. este un cetățean german care lucrează și locuiește în Austria.

21. La 23 februarie 2021, în timp ce efectuau un control cu privire la stupefiante, funcționarii biroului vamal din Innsbruck (Austria) au interceptat un pachet adresat lui C. G. care conținea 85 de grame de canabis.

[6] Codul de procedură penală, denumit în continuare „StPO”, BGBl nr. 631/1975, în versiunea aplicabilă la momentul faptelor (BGBl I nr. 24/2020).

22. La 6 martie 2021, doi ofițeri de poliție l-au interogat pe C. G. cu privire la expeditorul pachetului și i-au percheziționat locuința. În cursul percheziției, aceștia i-au ridicat telefonul mobil (inclusiv o cartelă SIM și un card SD) și i-au înmânat procesul-verbal de ridicare.

23. Atunci când i s-a solicitat să permită accesul la datele de conexiune ale telefonului său mobil și să dezvăluie codul de acces la acesta, C. G. a refuzat.

24. Comandamentul de poliție al districtului Landeck (Austria) nu a reușit să deblocheze telefonul mobil. Acesta a fost trimis la Bundeskriminalamt (Oficiul Federal al Poliției Judiciare) din Viena (Austria), unde s-a încercat din nou, fără succes, deblocarea sa și citirea datelor stocate în el.

25. La momentul la care au fost dispuse de poliție, aceste măsuri nu aveau acoperire în vreun ordin al Ministerului Public sau într-o hotărâre judecătorească.

26. La 31 martie 2021, C. G. a formulat o acțiune în fața Landesverwaltungsgericht Tirol (Tribunalul Administrativ Regional din Tirol, Austria) împotriva măsurii coercitive care i-a fost impusă, contestând ridicarea telefonului său mobil. Acesta i s-a returnat la 20 aprilie 2021.

27. C. G. nu a fost informat cu privire la încercările de a analiza conținutul telefonului mobil; el a luat cunoștință de acestea deoarece agentul de poliție care a ridicat telefonul și a inițiat ulterior analiza digitală a fost interogat în calitate de martor, fiind supus obligației de a spune adevărul. De asemenea, încercările respective nu au fost documentate în dosarul poliției judiciare.

28. În acest context, Landesverwaltungsgericht Tirol (Tribunalul Administrativ Regional din Tirol, Austria) a adresat Curții următoarele întrebări preliminare:

„1) Articolul 15 alineatul (1) (eventual coroborat cu articolul 5) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136/CE, citit în lumina articolelor 7 și 8 din cart[ă] […], 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, detectării și urmăririi penale a unor infracțiuni, acest acces trebuie limitat la combaterea criminalității grave?

2) Articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136/CE, trebuie interpretat, în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din [cartă], în sensul că se opune unei reglementări naționale precum articolul 18 coroborat cu articolul 99 alineatul (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) Articolul 47 din cart[ă] […] coroborat cu articolele 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 articolul 18 coroborat cu articolul 99 alineatul (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?”

III. Procedura în fața Curții

29. Cererea de decizie preliminară a fost introdusă la grefa Curții la 6 septembrie 2021.

30. La 20 octombrie 2021, Curtea a solicitat instanței de trimitere să precizeze dacă Directiva 2016/680 ar putea fi relevantă în speță.

31. La 11 noiembrie 2021, instanța de trimitere a răspuns că Directiva 2016/680 trebuie să fie aplicată în litigiul principal.

32. Au formulat observații scrise guvernele german, austriac, cipriot, danez, estonian, francez, maghiar, irlandez, neerlandez, norvegian, polonez și suedez, precum și Comisia Europeană.

33. La ședința publică desfășurată la 16 ianuarie 2023, s-au prezentat, pe lângă guvernul finlandez, toate guvernele care au formulat observații scrise, cu excepția guvernelor german, maghiar și polonez. Toate acestea au fost invitate de Curte să își concentreze argumentele pe Directiva 2016/680 și să răspundă oral la anumite întrebări referitoare la aceasta.

IV. Analiză

A. Inadmisibilitate

34. Instanța de trimitere și-a formulat inițial întrebările solicitând doar interpretarea Directivei 2002/58. Cu toate acestea, aproape toate intervenientele în procedură sunt de acord că directiva menționată nu se aplică în prezenta cauză și că, în consecință, interpretarea sa nu este necesară pentru soluționarea litigiului.

35. În conformitate cu articolul 3, Directiva 2002/58 se aplică „[…] prelucrării de date cu caracter personal legate de furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații din cadrul [Uniunii], inclusiv al rețelelor publice de comunicații care presupun colectarea de date și dispozitive de identificare”.

36. Curtea a statuat că „atunci când statele membre pun în aplicare în mod direct măsuri care derogă de la confidențialitatea comunicațiilor electronice, fără a impune obligații de prelucrare furnizorilor de servicii de astfel de comunicații, protecția datelor persoanelor în cauză nu intră sub incidența Directivei 2002/58, ci exclusiv a dreptului național, sub rezerva aplicării [Directivei 2016/680]”[7].

37. În prezenta cauză, tentativa de a accesa datele a fost făcută direct de autoritățile polițienești în cadrul unei anchete penale. Nu a existat nicio intervenție a furnizorilor de servicii de comunicații electronice, cărora nu li s-a solicitat să comunice date cu caracter personal. Prin urmare, Directiva 2002/58 nu este aplicabilă.

38. Norma de drept al Uniunii care reglementează situația descrisă este Directiva 2016/680, care, conform articolului 2 alineatul (1) din aceasta, se aplică prelucrării datelor cu caracter personal de către autoritățile competente în „scopul […] investigării […] infracțiunilor”.

[7] 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, denumită în continuare „Hotărârea La Quadrature du Net”, punctul 103).

39. Considerațiile anterioare ar fi suficiente pentru a se constata că cererea de decizie preliminară este inadmisibilă așa cum a fost formulată de instanța de trimitere, deoarece norma de drept al Uniunii a cărei interpretare se solicită nu este aplicabilă în speță.

40. Cu toate acestea, este adevărat că articolul 267 TFUE permite Curții să reformuleze întrebările preliminare sau să indice existența altor norme de drept al Uniunii care ar putea fi relevante, pentru a oferi un răspuns util instanței naționale [8].

41. Curtea a solicitat instanței de trimitere să se pronunțe cu privire la eventuala relevanță a Directivei 2016/680. Prin urmare, aceasta i-a oferit posibilitatea să completeze sau să reformuleze ea însăși întrebările. În loc să procedeze astfel, instanța de trimitere s-a limitat să arate că „în prezenta cauză, trebuie să se respecte, în orice caz, dispozițiile Directivei 2016/680", fără a le identifica însă pe cele în privința cărora avea îndoieli și fără a face alte aprecieri pe fond [9].

42. Potrivit unei jurisprudențe constante a Curții, „este indispensabil, după cum prevede articolul 94 litera (c) din Regulamentul de procedură, ca decizia de trimitere să conțină expunerea motivelor care au condus instanța de trimitere să reflecteze asupra interpretării sau a validității anumitor dispoziții ale dreptului Uniunii, precum și legătura pe care o stabilește între aceste dispoziții și legislația națională aplicabilă litigiului principal" [10].

43. Or, având în vedere considerațiile anterioare, nerespectarea cerințelor prevăzute la articolul 94 din Regulamentul de procedură este evidentă în prezenta cauză. Chiar dacă Curtea dă dovadă de o anumită flexibilitate în această privință, cooperarea cu instanța de trimitere trebuie să fie reciprocă: în lipsa nejustificată a cooperării sale în vederea expunerii îndoielilor cu privire la interpretarea dreptului Uniunii pe care îl consideră aplicabil (în speță, Directiva 2016/680), ni se pare logic ca cererea de decizie preliminară să fie respinsă ca inadmisibilă [11].

44. În plus, instanța de trimitere:

– nu a precizat natura prelucrării pe care au încercat să o efectueze autoritățile polițienești și nici a datelor cu caracter personal căutate în mod concret. Inițial, pare să indice că aceasta se limita la datele de conexiune (cu alte cuvinte, datele de transfer și de localizare), însă ulterior nu exclude faptul că deblocarea telefonului ar permite accesul la „toate datele digitale stocate" [12] și chiar la conținutul comunicațiilor și al mesajelor electronice schimbate prin intermediul său [13];

– se referă atât la ridicarea telefonului, cât și la accesul sau tentativa de acces la datele conținute în acesta și la „exploatarea" (*Auswertung*) lor ulterioară, cu alte cuvinte la examinarea și la citirea lor. Aceasta din urmă, adaugă el, „implică accesul complet necontrolat la ansamblul comunicațiilor digitale ale persoanei vizate", ceea ce permite „reconstituirea unei imagini foarte detaliate și profunde a aproape tuturor domeniilor vieții private".

8 A se vedea în special Hotărârea din 28 aprilie 2016, Oniors Bio (C-233/15, EU:C:2016:305, punctul 30).

9 Curtea a fost nevoită să invite părțile să indice „care sunt, în opinia lor, dispozițiile relevante ale Directivei 2016/680 în lumina cărora Curtea ar trebui, dacă este cazul, să reformuleze cele trei întrebări preliminare adresate de instanța de trimitere" (a patra întrebare dintre cele de la care se aștepta un răspuns oral în ședință).

10 Hotărârea din 6 octombrie 2021, Consorzio Italian Management și Catania Multiservizi (C-561/19, EU:C:2021:799, punctul 69).

11 Suntem de acord cu guvernul francez în ceea ce privește această apreciere (punctele 36-41 din observațiile sale scrise).

12 Astfel în a doua întrebare preliminară.

13 Instanța de trimitere precizează că „în ceea ce privește datele de conexiune, aproape toate contactele pot fi reconstituite în funcție de frecvența, timpul și durata comunicațiilor, în ceea ce privește comunicațiile efectuate prin SMS și alte servicii de mesagerie și, de asemenea, în ceea ce privește conținutul; de asemenea, prin evaluarea fotografiilor și a istoricului de navigare pe internet se realizează o cunoaștere foarte intimă a vieții private a persoanei vizate".

45. În aceste condiții, mai degrabă decât să *reformuleze* întrebările instanței de trimitere, Curtea ar proceda la o adevărată *reconstituire* a cererii de decizie preliminară, care, în plus, s-ar baza parțial pe considerații ipotetice, iar nu pe fapte stabilite. Astfel cum am menționat, Curtea ar fi nevoită să facă toate aceste lucruri în condițiile în care i-a oferit instanței posibilitatea de a-și completa sau reformula întrebările.

46. Prin urmare, propunem ca cererea de decizie preliminară să fie declarată inadmisibilă, astfel cum au solicitat mai multe state interveniente.

47. Faptul – subliniat în ședință – că în fața instanței de trimitere nu mai există un litigiu real care să necesite interpretarea unor norme de drept al Uniunii ar trebui să conducă de asemenea la constatarea inadmisibilității cererii.

48. Astfel, guvernul austriac (care este responsabil pentru autoritățile polițienești care au intervenit în anchetă) recunoaște că acțiunile acestora au fost ilegale și au încălcat drepturile persoanei vizate. Având în vedere că, potrivit deciziei de trimitere, cererea reclamantului în fața instanței de contencios administrativ era îndreptată tocmai împotriva măsurilor adoptate de poliție, pe care administrația pârâtă le consideră nelegale, nu mai există litigiul supus analizei instanței de trimitere.

49. În orice caz, în cazul în care Curtea nu împărtășește opinia noastră, vom aborda în cele ce urmează, cu caracter subsidiar, aspectele de fond care stau la baza întrebărilor preliminare.

50. Totuși, considerăm că este necesar mai întâi să excludem existența unui alt motiv de inadmisibilitate invocat de anumiți intervenienți în procedură [14]. În opinia lor, întrucât Directiva 2016/680 se referă la protecția persoanelor fizice în ceea ce privește *prelucrarea* datelor lor, aceasta nu s-ar aplica în situații precum cea în discuție în prezenta cauză, în care nu ar fi existat o prelucrare, ci doar o simplă *tentativă de accesare* a datelor care, în cele din urmă, nu au putut fi obținute.

51. Pe de altă parte, potrivit Comisiei, efectul util al Directivei 2016/680 ar trebui să favorizeze o interpretare a scopului său care să nu se limiteze la prelucrarea datelor în sens strict, ci să includă și chestiuni care sunt direct legate de ea. Una dintre acestea din urmă ar fi tentativa de accesare a datelor a căror prelucrare se solicită [15].

52. În opinia noastră, fără a fi necesar să forțăm limitele domeniului de aplicare al Directivei 2016/680 [16], aplicarea sa în prezenta cauză este justificată nu ca urmare a ridicării telefonului mobil [17], ci din cauza acțiunii subsecvente a autorităților polițienești cu scopul de a obține din el anumite date cu caracter personal ale persoanei vizate, scop în care au încercat să îl deblocheze și să permită accesul la conținutul său.

[14] Facem referire concret la guvernele austriac, francez, neerlandez și norvegian.

[15] Potrivit Comisiei, „este irelevant dacă tentativele au avut succes sau nu. Apariția unor dificultăți tehnice care împiedică succesul tentativelor este o împrejurare care nu poate fi cunoscută în prealabil și care nu afectează riscurile pentru protecția datelor cu caracter personal”.

[16] Ni se pare în special că nu este necesar să se recurgă la articolele 27 și 28 din Directiva 2016/680, așa cum propune Comisia în observațiile sale scrise. „Evaluarea impactului asupra protecției datelor” prevăzută la articolul 27 se referă, în mod generic, la „un tip de prelucrare”, iar nu la operațiuni de prelucrare specifice sau particulare. Acest lucru reiese clar din considerentul (58) al Directivei 2016/680: „[e]valuările impactului ar trebui să acopere sistemele și procesele relevante aferente operațiunilor de prelucrare, și *nu cazuri individuale*” (sublinierea noastră). În ședință, Comisia și-a nuanțat invocarea celor două dispoziții, pe care le-ar fi citat doar pentru a evidenția modul în care Directiva 2016/680 acoperă și situațiile anterioare prelucrării efective a datelor.

[17] Directiva 2016/680 nu reglementează ridicarea telefonului ca mijloc de probă în contextul unei anchete penale.

53. Printre operațiunile definite drept „prelucrare” la articolul 3 punctul 2 din Directiva 2016/680 figurează „punerea la dispoziție în orice alt mod” a datelor cu caracter personal, realizată în cadrul unei anchete penale. Considerăm că, atunci când autoritatea polițienească ridică un telefon în care sunt stocate astfel de date și îl manipulează pentru a extrage datele din el, aceasta inițiază o „operațiune” de prelucrare, chiar dacă nu reușește din motive tehnice privind securitatea criptografică.

54. O tentativă nereușită de a accesa datele cu caracter personal stocate pe un telefon mobil în cadrul unei anchete penale este reglementată de Directiva 2016/680 pentru motive similare celor care au determinat Curtea să statueze că Directiva 2002/58 este aplicabilă *încercării* (de asemenea nereușite) de a obține o autorizație judiciară pentru a accesa anumite date ale persoanei anchetate, deținute de un operator de comunicații electronice [18].

55. În acest context, în cazul în care instanța de trimitere ar trebui să se pronunțe cu privire la nelegalitatea comportamentului autorităților polițienești (recunoscută de guvernul austriac, astfel cum am arătat anterior), aprecierea sa ar putea depinde de legalitatea scopului urmărit prin el, atât dacă măsura a avut succes, cât și dacă doar s-a început, fără succes, punerea sa în aplicare.

B. Cu privire la fond

1. Prima întrebare preliminară

56. Instanța de trimitere solicită să se stabilească dacă, în conformitate cu articolul 15 alineatul (1) din Directiva 2002/58 (coroborat, dacă este cazul, cu articolul 5 din aceasta) și în lumina articolelor 7 și 8 din cartă, „accesul autorităților publice la datele stocate pe telefoanele mobile constituie o ingerință în drepturile fundamentale consacrate de aceste articole din cartă suficient de gravă pentru ca acest acces, în contextul prevenirii, cercetării, descoperirii și urmăririi penale a infracțiunilor, să fie limitat la lupta împotriva criminalității grave”.

57. În cazul în care trimiterea preliminară ar fi admisibilă, inaplicabilitatea Directivei 2002/58 ar impune reformularea primei întrebări, astfel încât Curtea să interpreteze Directiva 2016/680 în răspunsul dat.

58. Acest răspuns ar trebui să clarifice, la rândul său, dacă, în situații precum cea în discuție în prezenta cauză, poate fi vorba despre o ingerință și, în cazul în care există, dacă Directiva 2016/680 impune ca accesul la date să fie limitat la cazurile de combatere a infracționalității grave.

59. Operațiunile de prelucrare a datelor pot, prin definiție, să aducă atingere drepturilor la respectarea vieții private (articolul 7 din cartă) și la protecția datelor cu caracter personal (articolul 8 din cartă). Prin urmare, autoritățile publice trebuie să respecte condițiile prevăzute la articolul 52 alineatul (1) din cartă pentru a justifica ingerința lor în exercitarea acestor drepturi fundamentale.

60. Ingerința în drepturile protejate de articolele 7 și 8 din cartă va fi cu atât mai mare cu cât prin aceasta: a) se urmărește accesul la date sensibile înregistrate de obicei pe telefoanele mobile, a căror cunoaștere poate dezvălui aspecte ale vieții proprietarilor care nu ar trebui să fie cunoscute de terți, și b) se permite accesul la conținutul comunicațiilor.

[18] Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

61. Totuși, dintr-o perspectivă generală și având în vedere conținutul său, Directiva 2016/680 nu poate fi interpretată în sensul că operațiunile de prelucrare a datelor la care se referă se limitează doar la cazurile de combatere a infracționalității grave.

62. Directiva 2016/680 se referă la orice operațiune de prelucrare [19] a datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a *tuturor categoriilor* de infracțiuni.

63. Din principiile pe care le stabilește Directiva 2016/680 în ceea ce privește prelucrarea datelor cu caracter personal în astfel de scopuri (articolul 4) sau din condițiile de legalitate privind efectuarea prelucrării (articolul 8), nu rezultă că, de regulă, prelucrarea datelor este posibilă doar în cazuri de infracționalitate gravă.

64. De asemenea, o limitare la cazurile de combatere a infracționalității grave nu ar putea fi justificată prin simpla extrapolare a jurisprudenței cu privire la Directiva 2002/58 [20] la situații precum cea în discuție în prezenta cauză.

65. În opinia noastră, acest lucru nu este posibil, deoarece, fără a aduce atingere considerațiilor prezentate în continuare, jurisprudența respectivă se referă la stocarea generalizată și nediscriminatorie a datelor cu caracter personal ale unui grup generic și nedeterminat, efectuată în mod sistematic de furnizorii de servicii de comunicații electronice. Amploarea ingerinței pe care acest tip de stocare o implică pentru întreaga societate explică de ce Curtea a fost deosebit de riguroasă în interzicerea sa și în stabilirea de excepții în ceea ce privește interdicția respectivă.

66. Această situație nu există în cazul în care accesul solicitat nu afectează întreaga populație sau grupuri mari de populație (cu alte cuvinte, datele cu caracter personal ale unui grup generic și nedeterminat), ci informațiile stocate pe un telefon mobil individual, în contextul unei proceduri de urmărire penală care este de asemenea unică, în privința căreia este aplicabilă în mod specific Directiva 2016/680.

67. Obiectul Directivei 2016/680 nu este altul decât prelucrarea datelor de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor – a tuturor tipurilor de infracțiuni, iar nu doar a celor grave.

68. În rest, astfel cum au subliniat anumiți intervenienți în procedura preliminară, în lipsa oricărei indicații privind gravitatea infracțiunilor în Directiva 2016/680, aceasta nu poate fi aplicată în mod uniform în statele membre, deoarece aprecierile fiecărui drept național cu privire la gravitatea mai mare sau mai mică a comportamentului sancționabil diferă considerabil [21].

69. În concluzie, Directiva 2016/680 nu impune drept condiție de legalitate ca prelucrarea datelor cu caracter personal pe care o reglementează să fie posibilă numai în scopul combaterii infracționalității grave.

[19] Tipologia „tranzacțiilor” de la articolul 3 punctul 2 din Directiva 2016/680 este foarte largă. A se vedea transcrierea lor de la punctul 9 din prezentele concluzii.

[20] Hotărârea La Quadrature du Net, Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, denumită în continuare „Hotărârea Tele2 Sverige și Watson”), Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), Hotărârea din 6 octombrie 2020, Privacy International (C-623/17, EU:C:2020:790), și Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, EU:C:2021:152, denumită în continuare „Hotărârea Prokuratuur”).

[21] Guvernul francez oferă drept exemplu infracțiunile de posesie și de trafic de droguri, a căror gravitate diferă în dreptul penal austriac și francez. Guvernul suedez are o opinie similară.

70. Acest lucru nu aduce atingere faptului că, în aplicarea principiului proporționalității și de la caz la caz, prelucrarea datelor pe care autoritățile competente intenționează să o efectueze în temeiul Directivei 2016/680 trebuie să fie proporțională cu: a) natura infracțiunilor care fac obiectul urmăririi penale și b) calitatea datelor cu caracter personal care fac obiectul prelucrării respective.

71. În această privință, suntem de acord cu unele declarații ale guvernului german privind limitarea accesului la datele din telefoanele ridicate, atunci când permit stabilirea unui profil complet al personalității proprietarilor acestora, având în vedere conținutul digital al telefoanelor. Potrivit guvernului german, un astfel de acces ar trebui să fie limitat la datele care sunt necesare ca mijloace de probă într-un caz concret și ar putea să nu fie adecvat având în vedere factori precum „caracterul minor al infracțiunii care face obiectul anchetei sau valoarea probatorie redusă a datelor care urmează să fie obținute” [22].

72. Prin urmare, în *abstract*, Directiva 2016/680 nu consideră din start ca fiind nelegal accesul la datele cu caracter personal stocate pe un telefon mobil cu scopul de a facilita investigarea unor comportamente care pot intra în sfera infracționalității generale sau comune. Dacă, *în concret*, accesul respectiv este sau nu este posibil va fi o chestiune pe care autoritatea relevantă va trebui să o aprecieze de la caz la caz, ținând seama de necesitatea sa și de criteriul proporționalității la care tocmai ne-am referit.

73. Acest lucru rezultă, în opinia noastră, din dispozițiile Directivei 2016/680 care stabilesc condițiile de validitate a prelucrării datelor cu caracter personal în contextul combaterii criminalității:

– articolul 4 alineatul (1) litera (a), conform căruia datele trebuie „prelucrate în mod legal”;

– articolul 8 alineatul (1), care subliniază că prelucrarea trebuie să fie *necesară* și să se întemeieze pe dreptul Uniunii sau al unui stat membru.

2. A doua întrebare preliminară

74. Prin intermediul celei de a doua întrebări, instanța de trimitere solicită să se stabilească dacă articolul 15 alineatul (1) din Directiva 2002/58 coroborat cu articolele 7, 8, 11 și cu articolul 52 alineatul (1) din cartă, „se opune unei reglementări naționale precum articolul 18 coroborat cu articolul 99 alineatul (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”.

75. Formularea întrebării este oarecum ambiguă. Instanța de trimitere:

– recunoaște că, în conformitate cu articolul 110 alineatul (2) din StPO, ridicarea sau confiscarea bunurilor necesită, în principiu, autorizarea Ministerului Public. Autoritatea polițienească poate efectua aceste confiscări fără o astfel de autorizație numai în circumstanțele excepționale prevăzute la alineatul (3) al articolului respectiv (care nu par să existe în prezenta cauză);

[22] Observațiile scrise ale guvernului german, punctul 20.

– aceasta adaugă, totuși, că analiza informațiilor stocate pe telefoanele mobile „nu este reglementată fără echivoc [de StPO]” și că ar putea fi efectuată de autoritățile de securitate din proprie inițiativă, fără autorizație prealabilă.

76. Guvernul austriac furnizează o versiune a legislației naționale care nu este conformă cu cea prezentată în decizia de trimitere. În special, acesta susține că, în temeiul dreptului național, atât ridicarea telefonului (cu excepția situațiilor de urgență), cât și analiza datelor stocate pe acesta nu sunt posibile decât cu autorizarea Ministerului Public [23]. În lipsa unui ordin emis de acesta, exploatarea de către poliție a datelor stocate pe telefonul respectiv este nelegală.

77. Revine în sarcina instanței de trimitere să verifice termenii legislației interne. În cadrul procedurii prevăzute la articolul 267 TFUE, Curtea nu este competentă să interpreteze dreptul național și revine numai instanței naționale sarcina să determine domeniul de aplicare exact al actelor cu putere de lege și al actelor administrative naționale [24].

78. Fără a dori să ne implicăm în controversa privind interpretarea dreptului austriac, ni se pare dificil de dedus doar din dispozițiile identificate de instanța de trimitere [articolul 18 din StPO coroborat cu articolul 99 alineatul (1) din aceeași lege] consecința pe care ea însăși o deduce. Totuși, astfel cum am menționat, acesta este un aspect pe care doar instanța respectivă îl poate soluționa.

79. În orice caz, instanța de trimitere consideră că jurisprudența stabilită în Hotărârea Prokuratuur [25] cu privire la controlul prealabil, de către o instanță sau o autoritate independentă, al accesului la datele păstrate, ar putea fi extrapolată la o situație precum cea în discuție în prezenta cauză.

80. Pentru guvernul neerlandez, dimpotrivă, această jurisprudență trebuie înțeleasă în contextul unei legislații naționale care permitea autorităților competente accesul *general* la *toate* datele de transfer și de localizare stocate. Astfel s-ar explica cerința unei autorizații judiciare prealabile, care ar putea totuși să nu fie justificată în cazul accesului la datele unui singur telefon mobil.

81. În același sens, guvernul norvegian susține că, printre numeroasele garanții prevăzute de Directiva 2016/680 [26], nu este menționată în mod explicit necesitatea unei autorizații prealabile din partea unei autorități judiciare sau administrative independente.

82. Comisia, bazându-se pe faptul că dispozițiile Directivei 2016/680 trebuie interpretate în lumina cartei, susține că obligația impusă statelor membre prin articolul 8 alineatul (1) din directiva respectivă (condițiile de legalitate a prelucrării) implică necesitatea de a respecta drepturile fundamentale garantate de articolele 7 și 8 din cartă.

[23] Punctul 19 din observațiile guvernului austriac. Acesta citează decizia Oberster Gerichtshof (Curtea Supremă, Austria) din 13 octombrie 2020 (cauza 11 Os 56/20z), care califică drept nelegal, ca urmare a faptului că încalcă drepturile subiective ale persoanei vizate, accesul poliției judiciare la datele dintr-un telefon mobil fără autorizația Ministerului Public.

[24] Hotărârea din 28 aprilie 2022, SeGEC și alții (C-277/21, EU:C:2022:318, punctul 21).

[25] Hotărârea Prokuratuur, punctul 51: „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 urmărire penală”.

[26] În plus față de cele cuprinse la articolele 4 și 8, cele conținute în capitolele III („Drepturile persoanei vizate”), IV („Operatorul și persoana împuternicită de către operator”), VI („Autorități de supraveghere independente”) și VIII („Căi de atac, răspundere și sancțiuni”).

83. Împărtășim opinia Comisiei potrivit căreia legiuitorii naționali sunt obligați să definească normele necesare pentru a asigura că accesul la date este justificat în fiecare caz și este limitat la ceea ce este strict necesar și proporțional, respectând totodată dispozițiile cartei.

84. Totuși, aceste norme naționale nu trebuie să fie neapărat specifice accesului la datele cu caracter personal conținute, precum în speță, într-un telefon mobil, ci pot fi cele prevăzute de dreptul național, în general, în materia obținerii de probe.

85. În acest sens, am transcris deja punctul 103 din Hotărârea La Quadrature du Net în ceea ce privește măsurile statelor membre care afectează confidențialitatea comunicațiilor electronice, fără a impune obligații de prelucrare furnizorilor acestor servicii de comunicații [27].

86. Prin urmare, fără a fi necesar să se deducă din Directiva 2016/680 norme *specifice* de natură procedurală pentru a asigura legalitatea accesului la datele stocate pe un telefon mobil [28], se vor aplica normele naționale care reglementează exercitarea competențelor de percheziție și de sechestru în cadrul anchetelor penale [29].

87. Trimiterea la dispozițiile de drept intern pentru a asigura legalitatea accesului în temeiul Directivei 2016/680 este, în rest, conformă cu jurisprudența Curții EDO. Într-o cauză referitoare la Republica Austria în legătură cu articolul 8 din CEDO (dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței), Curtea EDO a constatat că legislația austriacă privind ridicarea bunurilor și în special a documentelor se aplică percheziționării și confiscării datelor stocate pe suporturi informatice [30].

88. În cazul în care, după cum susține guvernul austriac, citând jurisprudența Oberster Gerichtshof (Curtea Supremă, Austria), autoritățile polițienești nu au dreptul să acceseze datele stocate pe un anumit telefon mobil fără autorizația Ministerului Public, a doua întrebare preliminară își pierde o mare parte din sens.

89. În orice caz, răspunsul la această întrebare nu poate exclude posibilitatea ca accesul la datele cu caracter personal din telefonul ridicat să conducă la „reconstituirea unei imagini foarte detaliate și profunde a aproape tuturor domeniilor vieții private” ale persoanei vizate [31]. În această ipoteză, autoritățile polițienești nu ar putea să facă abstracție de autorizația prealabilă menționată în Hotărârea Prokuratuur.

90. La prima vedere, această afirmație ar fi incompatibilă cu neaplicarea în prezenta cauză a Directivei 2002/58 (pe care o interpretează Hotărârea Prokuratuur), așa cum am argumentat anterior. Totuși, apreciem că *ratio* a acestei hotărâri susține aceeași soluție.

[27] A se vedea punctul 36 din prezentele concluzii.

[28] Eforturile Comisiei – care se reflectă la punctele 34-39 din observațiile sale scrise – de a contribui la definirea unor norme clare și precise pentru stabilirea unor limite și a unor garanții adecvate în ceea ce privește accesul la datele din telefoanele mobile ilustrează bine dificultatea acestui demers.

[29] Norme care, după cum subliniază, de exemplu, guvernele danez și irlandez, nu intră în domeniul de aplicare al dreptului Uniunii, însă care pot contribui la îndeplinirea unei cerințe care rezultă din dreptul respectiv.

[30] Hotărârea Curții EDO din 16 octombrie 2007, Wieser și Bicos Beteiligungen împotriva Austriei (CE:ECHR:2007:1016JUD007433601), § 54: „the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data” [„Codul de procedură penală austriac nu conține prevederi specifice referitoare la percheziționarea și confiscarea datelor electronice. Totuși, codul conține prevederi detaliate referitoare la confiscarea obiectelor și, adițional, reguli specifice pentru confiscarea documentelor. Este deja stabilit în jurisprudența instanțelor de judecată naționale că aceste prevederi se aplică și percheziționării și confiscării datelor electronice”].

[31] A se vedea constatările instanței de trimitere transcrise la punctul 44 din prezentele concluzii.

91. În litigiul care a condus la pronunțarea Hotărârii Prokuratuur, deși accesul a fost efectuat prin obținerea de date (metadate) de la furnizorii de servicii de comunicații electronice, era în joc – la fel ca în speță – o anchetă penală singulară, îndreptată împotriva unei anumite persoane. Scopul era de a colecta „datele referitoare la mai multe numere de telefon […] și diferite identități internaționale de echipament mobil ale acesteia” [32].

92. În Hotărârea Prokuratuur, în opinia noastră, se pot distinge două planuri: a) cel în care se pun în discuție normele generale ale unui stat membru privind stocarea generalizată și nediferențiată și accesul ulterior la datele deținute de furnizorii de servicii și b) cel al controlului prealabil, pentru un caz specific, al accesului la acele metadate, atunci când acestea permit stabilirea unui profil precis al vieții private a unei persoane.

93. În opinia noastră, împrejurarea că, în prezenta cauză, datele care dezvăluie viața privată nu se află în posesia furnizorilor de servicii și sunt obținute (sau se încearcă obținerea lor) dintr-un singur telefon confiscat este de importanță secundară în raport cu *ratio* a cerinței privind controlul prealabil, la care face trimitere Hotărârea Prokuratuur.

94. Acest control prealabil se bazează, în ultimă instanță, pe protecția garantată de articolele 7 și 8 din cartă. Autoritatea însărcinată cu efectuarea controlului prealabil trebuie 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” [33].

3. A treia întrebare preliminară

95. Prin intermediul celei de a treia întrebări, instanța de trimitere solicită să se stabilească dacă articolul 47 din cartă (coroborat, dacă este cazul, cu articolele 41 și 52) se opune unei reglementări precum cea austriacă [34], ce „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”.

96. Considerăm că întrebarea formulată în acești termeni ar putea să se dovedească inutilă pentru soluționarea litigiului, deoarece persoana în cauză ar fi putut să își exercite dreptul consacrat la articolul 47 din cartă, solicitând instanței de trimitere să declare nulitatea acțiunii poliției asupra telefonului ridicat, care includea exploatarea ulterioară (și forțată) a datelor stocate pe el.

97. În ceea ce privește aceste două momente de intervenție a poliției, trebuie să se efectueze o distincție:

– în ceea ce privește ridicarea telefonului în sine, din informațiile depuse la dosar rezultă că persoana în cauză avea cunoștință despre aceasta și că a refuzat să furnizeze codul de deblocare autorităților polițienești la momentul confiscării;

– în ceea ce privește încercarea de a analiza datele, totul pare să indice că operatorul nu a informat persoana vizată cu privire la această operațiune, deși guvernul austriac susține că

[32] Hotărârea Prokuratuur, punctul 17.

[33] Hotărârea Prokuratuur, punctul 52.

[34] Din nou, se face referire la articolul 18 din StPO coroborat cu articolul 99 din StPO.

persoana respectivă a luat cunoștință de un raport în care se făcea referire la acțiunile poliției judiciare asupra telefonului [35].

98. Rămân, așadar, anumite neclarități în ceea ce privește utilizarea datelor și informarea în acest sens a persoanei vizate, care, așa cum am arătat anterior, ar fi trebuit să fie clarificate de instanța *a quo* în decizia de trimitere și care împiedică oferirea unui răspuns util la a treia întrebare preliminară.

99. În orice caz, în cazul în care Curtea nu consideră această întrebare inadmisibilă, ne vom exprima opinia în ceea ce o privește. În această ipoteză și având în vedere inaplicabilitatea Directivei 2002/58, întrebarea ar trebui să fie reformulată în lumina Directivei 2016/680, care, la articolele 13, 15 și 54, oferă indiciile necesare pentru a răspunde la aceasta.

100. În conformitate cu Directiva 2016/680, informațiile privind prelucrarea datelor care trebuie furnizate persoanei vizate sunt cele necesare printre altele pentru: a) depunerea unei plângeri în fața autorității de supraveghere [articolul 13 alineatul (1) litera (d)] și b) obținerea dreptului la o cale de atac judiciară efectivă în cazul încălcării drepturilor garantate de Directiva 2016/680, fără a aduce atingere vreunei căi de atac administrative sau extrajudiciare disponibile (articolul 54).

101. Cu toate acestea, nu trebuie ignorat faptul că atât articolul 13 alineatul (3), cât și articolul 15 alineatul (1) din Directiva 2016/680 autorizează statele membre să adopte măsuri legislative care:

– amână, restricționează sau omit furnizarea de informații persoanei vizate în conformitate cu articolul 13 alineatul (2);

– limitează, integral sau parțial, dreptul de acces al persoanei vizate la datele prelucrate în măsura în care și atât timp cât o astfel de limitare constituie o măsură necesară și proporțională, *inter alia*, pentru evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice și pentru a nu prejudicia investigarea infracțiunilor [36].

102. În orice caz, legalitatea prelucrării datelor nu depinde de respectarea de către autoritățile competente a obligațiilor (ulterioare) care le sunt impuse la articolul 13 din Directiva 2016/680, ci de legalitatea scopului cu care a fost efectuată, cu alte cuvinte de aspectul dacă autoritățile administrative respective aveau dreptul să prelucreze datele cu caracter personal.

103. Din această perspectivă, faptul că persoana vizată a fost informată cu privire la tentativele de accesare a datelor stocate pe telefonul ridicat de la aceasta nu are în sine nicio legătură cu legalitatea pe motive de fond a acțiunii poliției. Comportamentul operatorului care poate fi contrar obligațiilor impuse la articolul 13 din Directiva 2016/680 poate avea alte consecințe, însă, astfel cum am arătat, nu afectează ca atare legalitatea sau nelegalitatea prelucrării respective.

104. Instanța de trimitere este cea care trebuie să stabilească dacă legislația națională permite exercitarea efectivă a acelor drepturi de către persoana vizată.

[35] Punctul 37 din observațiile sale scrise.

[36] A se vedea în acest sens Hotărârea Tele2 Sverige și Watson, punctul 121. Jurisprudența stabilită în aceasta în legătură cu Directiva 2002/58 poate fi extrapolată la Directiva 2016/680 în contextul asigurării protecției jurisdicționale a drepturilor titularilor datelor prelucrate.

V. Concluzie

105. În lumina considerațiilor care precedă, propunem Curții să declare inadmisibilă cererea de decizie preliminară formulată de Landesverwaltungsgericht Tirol (Tribunalul Administrativ Regional din Tirol, Austria).

Cu titlu subsidiar, sugerăm să se răspundă la prezenta cerere după cum urmează:

„1) Articolul 4 alineatul (1) litera (a) și articolul 8 alineatul (1) din Directiva (UE) 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 coroborat cu articolele 7, 8 și 52 din Carta drepturilor fundamentale a Uniunii Europene

trebuie interpretat în sensul că,

în cadrul unei anchete penale, accesul autorităților publice la datele cu caracter personal stocate pe un telefon mobil, în scopul prelucrării lor, nu este limitat la cazurile de combatere a infracționalității grave.

Un astfel de acces trebuie să fie justificat în fiecare caz și trebuie să fie limitat la ceea ce este strict necesar și proporțional, în funcție de natura infracțiunilor urmărite penal și de datele cu caracter personal la care se solicită accesul.

Autoritățile polițienești nu pot, de sine stătător și fără autorizarea prealabilă a unei instanțe, în cadrul unei anchete penale, să obțină acces complet și necontrolat la toate datele stocate pe un telefon mobil, atunci când din acestea se poate obține o imagine precisă a vieții private a unei persoane.

2) Articolele 13, 15 și 54 din Directiva 2016/680 coroborate cu articolele 47 și 52 din cartă

trebuie interpretate în sensul că,

fără a aduce atingere limitărilor autorizate la articolul 15 alineatul (1) din Directiva 2016/680 sau altor căi de atac administrative sau extrajudiciare disponibile, persoana care deține telefonul mobil trebuie să fie informată cu privire la prelucrarea datelor cu caracter personal stocate în acesta de către autoritățile relevante, la momentul și în condițiile necesare pentru a asigura exercitarea efectivă a dreptului său de a obține protecție jurisdicțională împotriva unei posibile încălcări a drepturilor recunoscute de Directiva 2016/680.”