Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
DOMNUL ANTHONY COLLINS
prezentate la 8 iunie 2023[1]

Cauza C-178/22

Autori necunoscuți
intervenient:
Procura della Repubblica presso il Tribunale di Bolzano

[cerere de decizie preliminară formulată de Tribunale di Bolzano (Tribunalul din Bolzano, Italia)]

„Trimitere preliminară – Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice – Confidențialitatea comunicațiilor – Furnizori de servicii de comunicații electronice – Directiva 2002/58/CE – Articolul 1 alineatul (3) și articolul 15 alineatul (1) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8, 11 și articolul 52 alineatul (1) – Cerere din partea unui parchet de acces la date în scopul cercetării și al urmăririi penale a infracțiunii de furt calificat al unui telefon mobil – Noțiunea de «infracțiune gravă» de natură să justifice o ingerință gravă în drepturile fundamentale – Întinderea controlului prealabil în vederea asigurării respectării cerinței legate de săvârșirea unei infracțiuni grave – Principiul proporționalității”

I. Introducere

1. Procura della Repubblica presso il Tribunale di Bolzano (Parchetul de pe lângă Tribunalul din Bolzano, denumit în continuare „Parchetul Bolzano”) solicită Tribunale di Bolzano (Tribunalul din Bolzano, Italia) să autorizeze accesul la datele păstrate de furnizorii de servicii de comunicații electronice în temeiul dreptului național, care fac posibilă printre altele urmărirea și identificarea sursei și a destinației comunicărilor efectuate prin intermediul telefoanelor mobile.

2. În contextul acestei cereri, Tribunale di Bolzano (Tribunalul din Bolzano) solicită Curții de Justiție interpretarea articolului 15 alineatul (1) din Directiva 2002/58/CE[2]. Această dispoziție permite statelor membre să introducă excepții legislative de la obligația, prevăzută de directiva menționată[3], de a asigura confidențialitatea comunicațiilor electronice. În Hotărârea

[1] Limba originală: engleza.

[2] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor [electronice] (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11).

[3] A se vedea articolul 5 din Directiva 2002/58. Protecția confidențialității comunicațiilor electronice, garantată de articolul 5 alineatul (1) din Directiva 2002/58, se aplică măsurilor adoptate de orice persoane, altele decât utilizatorii, indiferent dacă este vorba despre persoane publice sau private. Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punctul 36 și jurisprudența citată).

Prokuratuur [4], Curtea a statuat că accesul la date care permit deducerea unor concluzii precise cu privire la viața privată a unui utilizator, potrivit unor măsuri adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, constituie o ingerință gravă în drepturile fundamentale și în principiile consacrate la articolele 7, 8 și 11, precum și la articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) [5]. Acest acces nu poate fi autorizat în scopul prevenirii, investigării, detectării și urmăririi penale a unor „infracțiuni” în general. Acesta poate fi acordat numai în cadrul procedurilor care vizează combaterea „infracțiunilor grave” [6] și trebuie să fie supus unui control prealabil exercitat de o instanță sau de o entitate administrativă independentă pentru a asigura respectarea acestei cerințe [7]. Tribunale di Bolzano (Tribunalul din Bolzano) solicită Curții să clarifice două aspecte ale Hotărârii Prokuratuur: noțiunea de „infracțiune gravă” și întinderea controlului prealabil pe care o instanță trebuie să îl efectueze în temeiul unei dispoziții de drept național care îi impune să autorizeze accesul la datele păstrate de furnizorii de servicii de comunicații electronice.

II. Cadrul juridic

A. Dreptul Uniunii

3. Articolul 5 din Directiva 2002/58, intitulat „Confidențialitatea comunicațiilor”, prevede:

„(1) 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). […]

[…]”

4. Articolul 6 din Directiva 2002/58, intitulat „Datele de transfer”, prevede:

„(1) Datele de transfer referitoare la abonați și utilizatori prelucrate și stocate de către furnizorul rețelei de comunicații publice sau al serviciilor publice de comunicații electronice trebuie șterse sau trecute în anonimat de îndată ce nu mai sunt necesare în scopul transmiterii comunicației, fără a aduce atingere alineatelor (2), (3) și (5) din prezentul articol sau articolului 15 alineatul (1).

[…]

(5) Prelucrarea de date de transfer în conformitate cu alineatele (1), (2), (3) și (4) trebuie limitată la persoanele care acționează sub autoritatea furnizorilor de rețele de comunicații publice sau de

[4] 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”).

[5] Independent de întinderea perioadei pentru care se solicită accesul la aceste date, de volumul sau de natura datelor disponibile pentru această perioadă.

[6] Sau pentru a preveni amenințările grave împotriva siguranței publice. A se vedea Hotărârea Prokuratuur, punctele 35, 39 și 45. A se vedea de asemenea Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punctul 56), și 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, punctul 140).

[7] Hotărârea Prokuratuur, punctele 48-52.

servicii publice de comunicații electronice în vederea facturării sau pentru gestionarea traficului, serviciul clientelă, detectarea fraudelor, promovarea serviciilor de comunicații electronice sau furnizarea de servicii suplimentare și trebuie să se limiteze la prelucrarea strict necesară scopului respectivei activități.

[…]”

5. Articolul 9 din Directiva 2002/58, intitulat „Datele de localizare altele decât datele de transfer”, prevede:

„(1) În cazul în care datele de localizare altele decât datele de transfer referitoare la abonați sau utilizatori ai rețelelor de comunicații publice sau ai serviciilor publice de comunicații electronice pot fi prelucrate, aceste date pot fi prelucrate doar dacă sunt anonime sau cu acordul utilizatorilor sau abonaților respectivi, în măsura și pe perioada cât sunt necesare în vederea furnizării unui serviciu suplimentar. Prestatorul de servicii trebuie să informeze utilizatorii și abonații, înainte de obținerea acordului lor, despre tipul de date de localizare altele decât datele de transfer care vor fi prelucrate, despre scopul și durata prelucrării și dacă datele respective vor fi transmise unor terțe părți în scopul furnizării de servicii suplimentare. Utilizatorii sau abonații trebuie să aibă în orice moment posibilitatea de a-și retrage acordul pentru prelucrarea datelor de localizare altele decât datele de transfer.

[…]”

6. Potrivit articolului 15 alineatul (1) din Directiva 2002/58:

„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[8]. 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) al Tratatului privind Uniunea Europeană.”

B. Dreptul național

7. Articolul 132 alineatul 3 din decreto legislativo 30 giugno 2003, n. 196, –Codice in materia di protezione dei dati personali (Decretul legislativ nr. 196 privind protecția datelor cu caracter personal)[9], din 30 iunie 2003, astfel cum a fost modificat recent prin articolul 1 din decreto-legge 30 settembre 2021 n. 132 – Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP, convertito con modificazioni nella legge 23

[8] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10).

[9] Supliment ordinar nr. 123 la GURI nr. 174 din 29 iulie 2003, p. 11.

novembre 2021 n. 178 (Decretul-lege nr. 132 din 30 septembrie 2021 [10], transformat, cu modificări, în Legea nr. 178 din 23 noiembrie 2021) [11] (denumit în continuare „articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003"), prevede:

„3. În termenul de conservare impus de lege (și anume 24 de luni de la data notificării), în cazul în care există indicii suficiente că au fost săvârșite infracțiuni pentru care legea prevede pedeapsa cu închisoarea pe viață sau aplicarea maximului prevăzut pentru pedeapsa cu închisoarea, care nu poate fi mai mic de trei ani, stabilită în conformitate cu articolul 4 din Codice di procedura penale [Codul de procedură penală], precum și infracțiuni de amenințare și de hărțuire sau de tulburare a liniștii persoanelor prin intermediul telefonului, în cazul în care amenințarea și tulburarea sunt grave și atunci când sunt relevante pentru stabilirea faptelor, datele se obțin sub rezerva autorizării de către judecător prin ordonanță motivată, la cererea procurorului sau la cererea apărătorului inculpatului, a persoanei cercetate, a părții vătămate și a altor părți private;

[…]

3c. Datele obținute cu încălcarea dispozițiilor de la alineatele 3 și 3a nu pot fi utilizate."

8. Potrivit articolului 4 din Codice di procedura penale (Codul de procedură penală), intitulat „Norme de stabilire a competenței":

„La stabilirea competenței, se ține seama de pedeapsa stabilită prin lege pentru fiecare infracțiune săvârșită sau sub formă de tentativă. Nu se ține seama de continuarea, recidiva și de circumstanțele infracțiunii, cu excepția circumstanțelor agravante pentru care legea stabilește o pedeapsă diferită față de pedeapsa obișnuită pentru infracțiunea respectivă și față de pedepsele speciale."

9. Potrivit instanței de trimitere, parchetul poate efectua *ex officio* urmărirea penală în cazul infracțiunii de furt calificat [12]. În temeiul articolului 625 din Codice penale (Codul penal), persoana vinovată de săvârșirea infracțiunii de furt calificat este pasibilă de o pedeapsă agravată cu închisoarea de la doi la șase ani și cu amendă de la 927 la 1 500 de euro. Articolul 624 din Codice penale (Codul penal) prevede că persoana vinovată de săvârșirea infracțiunii de furt simplu, care poate fi urmărită penal la plângerea persoanei vătămate, este pasibilă de o pedeapsă cu închisoarea de la șase luni la trei ani și cu amendă de la 154 la 516 euro.

III. Litigiile principale și întrebarea preliminară

10. Parchetul (Bolzano) a inițiat două seturi de proceduri penale împotriva unor autori necunoscuți pentru comiterea infracțiunii de furt calificat al unui telefon mobil, în temeiul articolelor 624 și 625 din Codul penal [13]. Pentru a identifica autorii, acesta a solicitat instanței de trimitere, în temeiul articolului 132 alineatul 3 din Decretul legislativ nr. 196/2003, „[…] autorizația de a obține de la toate companiile de telefonie toate datele pe care le deține, prin metode de urmărire și localizare (în special codurile utilizatorilor și, eventual, codurile IMEI ale

[10] GURI nr. 234 din 30 septembrie 2021, p. 1.

[11] GURI nr. 284 din 29 noiembrie 2021, p. 1.

[12] Furturile care fac obiectul anchetei desfășurate în fața instanței de trimitere sunt încadrate drept furturi calificate de dreptul italian.

[13] Primul furt a fost săvârșit la 27 octombrie 2021 (număr de referință RGNR 9228/2021). Al doilea a avut loc la 20 noiembrie 2021 (număr de referință RGNR 9794/2021). Furturile de telefoane mobile au avut loc în Bolzano, iar proprietarii telefoanelor au raportat furturile la Carabinieri (poliție).

persoanelor apelate/apelanților, website-urile vizitate/căutate, ora și durata apelului/conexiunii și indicarea celulelor și/sau a repetitoarelor în cauză, utilizatorii și codurile IMEI ale expeditorilor/destinatarilor SMS-urilor sau MMS-urilor și, după caz, detalii despre titularii respectivi) cu privire la conversațiile/comunicările telefonice primite și efectuate și a conexiunilor efectuate, inclusiv în roaming, chiar dacă este vorba de apeluri fără facturare (bip-uri), de la data furtului și până la data procesării cererii."

11. Instanța de trimitere are îndoieli cu privire la compatibilitatea articolului 132 alineatul 3 din Decretul legislativ nr. 196/2003 cu articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost interpretat în Hotărârea Prokuratuur. Aceasta arată că, la 7 septembrie 2021, Corte suprema di Cassazione (Curtea Supremă de Casație, Italia) [14] a statuat că, întrucât instanțele naționale dispun de o marjă de apreciere pentru a stabili ce fapte constituie „amenințări grave pentru securitatea națională și infracțiuni grave", Hotărârea Prokuratuur nu se aplica în mod direct instanțelor naționale. Ca urmare a pronunțării hotărârii Corte suprema di Cassazione (Curtea Supremă de Casație), legiuitorul italian a adoptat Decretul-lege nr. 132 din 30 septembrie 2021, care, la articolul 132 alineatul 3, califică drept infracțiuni grave în scopul obținerii înregistrărilor telefonice printre altele infracțiunile pasibile de „o pedeapsă cu închisoarea de cel puțin trei ani […]".

12. Potrivit instanței de trimitere, se încadrează sub pragul pentru calificarea infracțiunilor drept grave prevăzut la articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 infracțiuni care provoacă perturbări sociale limitate și care pot fi urmărite penal numai în urma unei plângeri depuse de un particular [15]. Astfel, accesul la înregistrările convorbirilor telefonice poate fi obținut în temeiul acestei dispoziții pentru furtul unui bun cu valoare minimă, precum un telefon mobil sau o bicicletă. Prin urmare, pragul prevăzut la articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 încalcă principiul proporționalității prevăzut la articolul 52 alineatul (1) din cartă, care impune ca, în toate cazurile, gravitatea infracțiunii investigate să fie pusă în balanță cu restrângerea adusă exercitării unui drept fundamental. Urmărirea penală a infracțiunilor minore nu justifică restrângerea exercitării drepturilor fundamentale la respectarea vieții private, la protecția datelor cu caracter personal și la libertatea de exprimare și de informare [16].

13. Instanța de trimitere explică faptul că instanțele italiene dispun de o marjă de apreciere foarte limitată în ceea ce privește refuzul de a autoriza accesul la înregistrările convorbirilor telefonice, întrucât autorizația trebuie acordată atunci când există „indicii suficiente cu privire la săvârșirea unei infracțiuni", iar o asemenea autorizație este „relevantă pentru stabilirea [faptelor]". În special, instanțele nu sunt competente să aprecieze gravitatea infracțiunii care face obiectul anchetei. Această apreciere a fost făcută de către legiuitor atunci când a prevăzut, în mod general și fără a face distincție între diferite tipuri de infracțiuni, că accesul la convorbirile telefonice trebuie să fie acordat printre altele în ceea ce privește anchetarea tuturor infracțiunilor pedepsite cu o pedeapsă cu închisoarea de cel puțin 3 ani.

[14] Cass. Pen. Sez. II, n. 33116, ud. 7.9.2021, est. Pellegrino.

[15] Potrivit instanței de trimitere, „acesta este, de exemplu, cazul infracțiunii de intrare prin efracție, pedepsită la articolul 614 din codul menționat cu o pedeapsă cu închisoarea de la un an la patru ani. Alte infracțiuni, a căror limită a pedepsei legale nu împiedică obținerea de înregistrări telefonice, pedepsite doar la plângerea uneia dintre părți ca urmare a unui grad scăzut de îngrijorare în rândul societății, sunt infracțiunile prevăzute la articolul 633 din Codul penal (invadarea de terenuri și imobile: închisoare de la unu la trei ani și amendă între 103 euro și 1 032 de euro) sau la articolul 640 din Codul penal (înșelăciune simplă: închisoare de la șase luni la trei ani și amendă de la 51 euro la 1 032 de euro)."

[16] A se vedea articolele 7, 8 și 11 din cartă.

14. În aceste condiții, Tribunale di Bolzano (Tribunalul din Bolzano) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarea întrebare preliminară:

„Articolul 15 alineatul (1) din [Directiva 2002/58] se opune reglementării naționale de la [articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003], care are următorul cuprins:

«În termenul de păstrare impus de lege, în cazul în care există indicii suficiente cu privire la infracțiuni pentru care legea prevede pedeapsa cu închisoarea pe viață sau cu închisoarea de cel puțin trei ani, stabilită în conformitate cu articolul 4 din [Codul de procedură penală], precum și cu privire la infracțiuni de amenințare și de hărțuire sau de tulburare a liniștii persoanelor prin intermediul telefonului, atunci când amenințarea, hărțuirea și tulburarea sunt grave, dacă sunt relevante pentru stabilirea faptelor, datele sunt obținute, sub rezerva autorizării judecătorului prin ordonanță motivată, la cererea procurorului sau la cererea apărătorului inculpatului, a persoanei cercetate, a părții vătămate și a altor persoane private?»”

IV. Procedura în fața Curții

15. Guvernele ceh și estonian, Irlanda și guvernele francez, italian, cipriot, maghiar, neerlandez, austriac și polonez, precum și Comisia Europeană au prezentat observații scrise.

16. Pledoariile acestor părți interesate și ale Parchetului (Bolzano), precum și răspunsurile acestora la întrebările adresate de Curte au fost ascultate în ședința desfășurată la data de 21 martie 2023.

V. Apreciere

A. Cu privire la admisibilitate

17. Guvernul italian și Irlanda susțin că o parte din cererea de decizie preliminară este inadmisibilă. Potrivit situației de fapt din decizia de trimitere, cererea de acces a fost formulată în contextul cercetării infracțiunilor de furt calificat de telefoane mobile. Irlanda subliniază că parchetul poate urmări penal această infracțiune *ex officio*. Această competență reflectă opinia potrivit căreia natura și efectele infracțiunii afectează societatea în general. Astfel, cererea de decizie preliminară prezintă un caracter ipotetic în măsura în care se referă și la infracțiuni care nu pot face obiectul urmăririi penale decât în urma unei plângeri formulate de un particular. Guvernul italian arată că instanța de trimitere se referă la o serie de infracțiuni care sunt irelevante pentru cauzele pendinte în fața sa. Guvernul italian și Comisia susțin că, contrar trimiterii din cerere la „o pedeapsă cu închisoarea de cel puțin trei ani”, în temeiul articolului 625 din Codul penal, infracțiunea de furt calificat este pasibilă de o pedeapsă cu închisoarea de la doi la șase ani. Prin urmare, Comisia propune Curții reformularea întrebării. Guvernul francez solicită de asemenea Curții reformularea întrebării. Acesta apreciază că, deși Curtea poate interpreta dispozițiile dreptului Uniunii, ea nu este competentă să aprecieze compatibilitatea dispozițiilor dreptului național cu dreptul Uniunii.

18. Prin întrebarea adresată de instanța de trimitere, Curții i se solicită literalmente să se pronunțe cu privire la compatibilitatea unei dispoziții de drept național cu dreptul Uniunii. Aceasta, în sine, nu o împiedică să furnizeze instanței de trimitere o interpretare a dreptului Uniunii, în speță a articolului 15 alineatul (1) din Directiva 2002/58, care să permită instanței de

trimitere să se pronunțe cu privire la compatibilitatea cu această dispoziție a oricărei norme naționale în discuție în litigiul cu care este sesizată [17].

19. Din cererea de decizie preliminară reiese că Parchetul (Bolzano) a solicitat accesul la date printre altele pentru a cerceta și a urmări penal două cazuri de comitere a infracțiunii de furt calificat al unui telefon mobil în temeiul articolului 625 din Codul penal. În aceste condiții, trimiterile în această cerere la alte infracțiuni, printre care articolul 624 din Codul penal (furt simplu) [18], sunt lipsite de relevanță pentru soluționarea cererilor pendinte în fața instanței de trimitere [19]. În măsura în care întrebarea preliminară se referă la cererea Parchetului (Bolzano) de acces la date în vederea anchetării unor cazuri de comitere a infracțiunii de furt calificat, aceasta nu este ipotetică. În consecință, ne vom limita aprecierea cu privire la aplicarea articolului 132 alineatul 3 din Decretul legislativ nr. 196/2003 la fapte precum cele descrise de instanța de trimitere care se referă la cazurile de furt calificat de telefoane mobile.

B. Cu privire la fond

1. Observații introductive

20. Prezenta trimitere preliminară își are originea într-o cerere a Parchetului (Bolzano) de acces la date păstrate de furnizorii de servicii de comunicații electronice. Aceasta nu privește nici păstrarea acestor date, nici legalitatea acesteia în temeiul, *inter alia*, al articolului 15 alineatul (1) din Directiva 2002/58 [20]. Datele constau, *inter alia*, în detalii privind comunicările primite și efectuate [21] cu telefoanele mobile furate și în datele de localizare [22]. Deși datele nu includ conținutul comunicărilor, acestea permit să se deducă concluzii precise cu privire la viața privată a persoanelor ale căror date sunt vizate, iar accesul la acestea pare să constituie o ingerință „gravă” în drepturile lor fundamentale [23]. Ingerința pe care o implică accesul la astfel de date poate fi justificată de obiectivul [24], la care face trimitere articolul 15 alineatul (1) prima teză din Directiva 2002/58, de prevenire, investigare, detectare și urmărire penală a „infracțiunilor grave”, însă nu și

[17] A se vedea prin analogie Hotărârea din 17 martie 2021, Consulmarketing (C-652/19, EU:C:2021:208, punctul 33). Potrivit unei jurisprudențe constante, în temeiul articolului 267 TFUE, este de competența Curții să ofere instanței naționale un răspuns care să îi permită să soluționeze litigiul cu care este sesizată. Din această perspectivă, Curtea poate reformula întrebările adresate. Hotărârea din 25 iulie 2018, Dyson (C-632/16, EU:C:2018:599, punctul 47 și jurisprudența citată).

[18] O persoană care săvârșește infracțiunea de furt simplu este pasibilă de o pedeapsă cu închisoarea de la șase luni la trei ani și, prin urmare, intră sub incidența articolului 132 alineatul 3 din Decretul legislativ nr. 196/2003.

[19] În măsura în care aceste trimiteri indică faptul că articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 poate fi invocat în cadrul anchetării infracțiunilor care nu constituie infracțiuni grave, a se vedea punctele 35-39 din prezentele concluzii.

[20] Astfel, cererea de decizie preliminară se întemeiază pe premisa potrivit căreia păstrarea datelor solicitate este legală. Păstrarea și accesul la datele care intră sub incidența Directivei 2002/58 constituie ingerințe distincte în drepturile fundamentale garantate la articolele 7, 8 și 11 din cartă și necesită o justificare distinctă, în temeiul articolului 52 alineatul (1) din aceasta. A se vedea în acest sens Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258, punctul 47). Punctele 29-33 din Hotărârea Prokuratuur oferă o imagine de ansamblu asupra normelor care reglementează păstrarea unor astfel de date.

[21] Potrivit articolului 2 litera (d) din Directiva 2002/58, „comunicație” „înseamnă orice informație trimisă sau transmisă între un număr finit de părți prin intermediul unui serviciu public de comunicații electronice […]”.

[22] Potrivit articolului 2 litera (c) din Directiva 2002/58, „date de localizare” înseamnă „orice date […] care indică poziția geografică a echipamentului terminal al unui utilizator al unui serviciu public de comunicații electronice”.

[23] Hotărârea Prokuratuur, punctele 34 și 35. A se vedea prin analogie Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punctele 59-62). Revine instanței naționale sarcina de a aprecia dacă accesul la datele în cauză constituie o ingerință „gravă” în drepturile fundamentale ale persoanelor ale căror vizate prin aceste date. Prezentele concluzii se întemeiază pe premisa potrivit căreia ingerința pe care o implică accesul la datele descrise la punctul 10 din prezentele concluzii este gravă.

[24] Lista obiectivelor de la articolul 15 alineatul (1) din Directiva 2002/58 este exhaustivă. Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctul 90).

a infracțiunilor în general. La interpretarea articolului 15 alineatul (1) din Directiva 2002/58, Curtea stabilește o legătură între gravitatea ingerinței în drepturile fundamentale ale unei persoane și gravitatea infracțiunii care face obiectul anchetei [25].

2. Competența statelor membre de a defini „infracțiunea gravă”

21. Directiva 2002/58 reglementează activitățile furnizorilor de servicii de comunicații electronice în ceea ce privește prelucrarea datelor cu caracter personal [26]. Articolul 1 alineatul (3) exclude în mod expres din domeniul de aplicare al Directivei 2002/58 activitățile statului în domenii specifice precum siguranța publică, apărarea, siguranța statului și legea penală. Activitățile la care face trimitere articolul 15 alineatul (1) din Directiva 2002/58 se suprapun în mod substanțial cu cele descrise la articolul 1 alineatul (3) din aceasta și includ activități ale statului în domeniul legii penale care sunt excluse în mod expres din domeniul de aplicare al Directivei 2002/58 [27]. Există, așadar, o legătură clară între activitățile statului pe care articolul 1 alineatul (3) din Directiva 2002/58 le exclude din domeniul de aplicare al acestei directive și măsurile legislative pe care statele membre le pot adopta în temeiul articolului 15 alineatul (1) din aceasta [28].

22. În pofida acestei legături clare, Curtea a statuat în mod constant că, din moment ce articolul 15 alineatul (1) din Directiva 2002/58 permite în mod expres statelor membre să adopte măsurile legislative naționale prevăzute la acest articol, astfel de măsuri intră în domeniul de aplicare al acestei directive. Din această jurisprudență rezultă că noțiunea de „activități”, inclusiv „activitățile statului în domeniul legii penale”, care figurează la articolul 1 alineatul (3) din Directiva 2002/58, nu include măsurile legislative la care face trimitere articolul 15 alineatul (1) din aceasta [29].

[25] A se vedea în acest sens Concluziile avocatului general Saugmandsgaard Øe prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300, punctele 79-82 și jurisprudența citată). În ceea ce privește obiectivul de combatere a criminalității, accesul nu poate fi acordat, în principiu, decât la datele persoanelor suspectate că ar plănui, că ar săvârși sau că ar fi săvârșit o infracțiune gravă ori că ar fi implicate într-un mod sau altul în infracțiunea respectivă. Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258, punctul 105).

[26] A se vedea în acest sens articolul 3 din Directiva 2002/58, care prevede că această directivă se aplică prelucrării de date cu caracter personal legate de furnizarea de servicii de comunicații electronice destinate publicului. A se vedea de asemenea Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctele 70 și 74), precum și, prin analogie, Concluziile avocatului general Szpunar prezentate în cauza La Quadrature du Net și alții (Date cu caracter personal și combaterea contrafacerii) (C-470/21, EU:C:2022:838, punctul 38).

[27] 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, punctul 97).

[28] Pentru a proteja securitatea națională, apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice.

[29] 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, punctul 98), și Hotărârea din 6 octombrie 2020, Privacy International (C-623/17, EU:C:2020:790, punctul 38 și jurisprudența citată).

23. Nici articolul 2 din Directiva 2002/58, care conține o serie de definiții în scopul aplicării acestei directive, nici vreo altă dispoziție din Directiva 2002/58, inclusiv articolul 15 alineatul (1), nu definește noțiunea de „infracțiuni”. Directiva 2002/58 nu conține o listă de „infracțiuni” [30]. În plus, în jurisprudența prin care a fost interpretat articolul 15 alineatul (1) din Directiva 2002/58 nu este definită această noțiune [31].

24. În pofida lipsei unor astfel de definiții, Directiva 2002/58 nu prevede că fiecare stat membru definește „infracțiunile” în conformitate cu dreptul său național [32]. Potrivit unei jurisprudențe constante a Curții, atât cerințele aplicării uniforme a dreptului Uniunii, cât și principiul egalității de tratament impun ca o dispoziție de drept al Uniunii care nu face nicio trimitere expresă la dreptul statelor membre pentru a stabili sensul și domeniul său de aplicare să primească în întreaga Uniune o interpretare autonomă și uniformă. În contextul interpretării articolului 15 alineatul (1) din Directiva 2002/58, noțiunea de „infracțiuni” poate fi considerată, cel puțin în principiu, o noțiune autonomă de drept al Uniunii care trebuie interpretată în mod uniform în toate statele membre [33].

25. Cu toate acestea, cele zece state membre care au prezentat observații Curții și Comisia consideră în unanimitate că revine fiecărui stat membru sarcina de a defini „infracțiunile”, inclusiv infracțiunile grave, la care face referire articolul 15 alineatul (1) din Directiva 2002/58, prin trimitere la dreptul lor național.

26. Suntem de acord cu aceste argumente pentru motivele enunțate în continuare.

27. În primul rând, Curtea a precizat deja că, în contextul articolului 15 alineatul (1) din Directiva 2002/58, este de competența statelor membre să își definească interesele esențiale de securitate și să adopte măsurile apte să asigure securitatea lor internă și externă [34]. Astfel, deși nu a statuat acest lucru în mod expres, Curtea pare, așadar, să fi considerat că noțiunea de „securitate națională” care figurează la articolul 15 alineatul (1) din Directiva 2002/58 nu este o noțiune autonomă de drept al Uniunii, în pofida lipsei unei definiții a acestei noțiuni sau a unei trimiteri exprese la

[30] A se vedea, în schimb, articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO 2002, L 190, p. 1, Ediție specială, 19/vol. 6, p. 3), astfel cum a fost modificată prin Decizia-cadru 2009/299/JAI a Consiliului din 26 februarie 2009 (JO 2009, L 81, p. 24), care enumeră infracțiunile care duc la predarea pe baza unui mandat european de arestare, precum și anexa II la Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (JO 2016, L 119, p. 132), care enumeră „infracțiunile grave” definite la articolul 3 punctul 9 din această directivă.

[31] Directiva 2002/58 nu se referă la „infracțiuni generale”, la „infracțiuni grave” sau la „infracțiuni”. Curtea menționează aceste noțiuni în jurisprudența sa fără a le defini și fără a furniza criterii cu privire la modul în care legiuitorii naționali ar putea să le definească. A se vedea de exemplu Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctele 115 și 125), precum și Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punctele 54, 56 și 63). A se vedea de asemenea în această privință, punctul 45 din Hotărârea Prokuratuur.

[32] A se vedea, în schimb, articolul 1 alineatul (1) din Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO 2006, L 105, p. 54, Ediție specială, 13/vol. 53, p. 51), care prevedea că „prezenta directivă urmărește să armonizeze dispozițiile statelor membre privind obligațiile furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice cu privire la păstrarea anumitor date generate sau prelucrate de către aceștia, pentru a se asigura că datele sunt disponibile în vederea cercetării, depistării și urmăririi penale a infracțiunilor grave, *astfel cum sunt definite de fiecare stat membru în dreptul său intern*” (sublinierea noastră). Prin Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238), Curtea a declarat nevalidă Directiva 2006/24.

[33] A se vedea prin analogie Hotărârea din 7 septembrie 2022, Staatssecretaris van Justitie en Veiligheid (Natura dreptului de ședere în temeiul articolului 20 TFUE) (C-624/20, EU:C:2022:639, punctele 19 și 20).

[34] 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, punctele 99 și 136).

dreptul statelor membre [35]. Nu vedem niciun motiv pentru care aceeași abordare nu ar trebui să se aplice competențelor statelor membre de a defini „infracțiunile” sau „infracțiunile grave” în sensul articolului 15 alineatul (1) din Directiva 2002/58. Termenii „infracțiuni”, „siguranță publică” și „securitate națională” care figurează în această dispoziție pot fi considerați *noscitur a sociis*, deoarece se pare că legiuitorul Uniunii a intenționat ca fiecare dintre aceștia să fie tratat în mod similar, inclusiv în ceea ce privește modul lor de definire [36].

28. În al doilea rând, articolul 4 alineatul (2) TUE impune Uniunii să respecte identitatea națională a statelor membre, inerentă structurilor lor fundamentale politice și constituționale. În preambulul cartei se recunoaște de asemenea că, deși Uniunea contribuie la păstrarea și la dezvoltarea valorilor comune, aceasta respectă printre altele diversitatea culturilor și tradițiilor popoarelor Europei. Definirea infracțiunilor și a sancțiunilor [37] reflectă sensibilitățile și tradițiile naționale care variază considerabil nu numai între statele membre, ci și în timp, în paralel cu evoluția societății [38].

29. Se poate observa în acest context că, la definirea infracțiunilor și a sancțiunilor, statele membre țin seama, în grade diferite, de diferiți factori. Aprecierea de către un stat membru a „gravității” unei anumite infracțiuni se reflectă adesea, dacă nu în mod invariabil, în gravitatea sancțiunii aplicate. Durata unei pedepse privative de libertate poate reflecta o analiză a mai multor factori, inclusiv „gravitatea” intrinsecă percepută a unei infracțiuni și „gravitatea” relativă a acesteia în raport cu alte infracțiuni. Nu au fost avansate argumente cu privire la motivul pentru care statele membre nu ar trebui să își exercite această competență sau, de altfel, cu privire la motivul pentru care o abordare diferită ar trebui să se aplice definirii „infracțiunilor”, „infracțiunilor grave” sau „infracțiunilor în general” în contextul specific avut în vedere.

30. Competența statelor membre în domeniul legii penale nu aduce atingere competenței de care beneficiază Uniunea Europeană, în anumite cazuri, de a stabili, de exemplu, norme minime cu privire la definirea infracțiunilor și a sancțiunilor în domenii ale criminalității de o gravitate deosebită de dimensiune transfrontalieră ce rezultă din natura sau impactul acestor infracțiuni ori din nevoia specială de a le combate pornind de la o bază comună [39]. Legiuitorul Uniunii nu a stabilit însă norme care să reglementeze definirea infracțiunilor la articolul 15 alineatul (1) din

[35] În plus, articolul 4 alineatul (2) TUE prevede că securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru. Faptul că o măsură națională este adoptată în vederea protejării securității naționale nu determină inaplicabilitatea dreptului Uniunii și nu absolvă statele membre de necesitatea de a respecta acest drept. 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, punctele 99 și 135).

[36] Deși obiectivul de protejare a securității naționale îl depășește ca importanță pe cel al combaterii infracționalității grave și, prin urmare, poate justifica ingerințe mai grave în drepturile fundamentale, aceasta nu aduce atingere dreptului statelor membre de a defini „infracțiuni” sau „infracțiuni grave”. 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, punctul 136).

[37] Și a circumstanțelor atenuante și agravante.

[38] Avocatul general Saugmandsgaard Øe a considerat că legislația penală și normele de procedură penală sunt de competența statelor membre, chiar dacă ordinea juridică a acestora din urmă poate fi totuși afectată de dispozițiile de drept al Uniunii adoptate în acest domeniu pe baza printre altele a dispozițiilor articolului 83 alineatul (2) TFUE. Prin urmare, nu există nicio dispoziție cu aplicabilitate generală care ar furniza o definiție armonizată a noțiunii de „infracțiune gravă”. Concluziile prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300, punctul 95). Avocatul general Pitruzzella a afirmat că definiția noțiunii de „infracțiune gravă” trebuie să fie lăsată la aprecierea statelor membre. Astfel, potrivit sistemelor juridice naționale, aceeași infracțiune poate fi sancționată mai mult sau mai puțin sever. Definirea circumstanțelor agravante poate varia de asemenea în funcție de statele membre. Concluziile prezentate în cauza Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, EU:C:2020:18, punctele 91 și 92). În schimb, avocatul general Szpunar a considerat că „noțiunea «infracționalitate gravă» trebuie […] să primească o interpretare autonomă. Aceasta nu poate depinde de concepțiile fiecărui stat membru, întrucât astfel s-ar permite eludarea cerințelor articolului 15 alineatul (1) din Directiva 2002/58 după cum statele membre adoptă sau nu o concepție extinsă a combaterii infracționalității grave.” Concluziile prezentate în cauza La Quadrature du Net și alții (Date cu caracter personal și combaterea contrafacerii) (C-470/21, EU:C:2022:838, punctul 74).

[39] Primul paragraf al articolului 83 alineatul (1) TFUE. A se vedea de asemenea Hotărârea din 21 octombrie 2021, Okrazhna prokuratura – Varna (C-845/19 și C-863/19, EU:C:2021:864, punctul 32).

Directiva 2002/58 [40]. Astfel, după cum s-a arătat anterior [41], din textul articolului 1 alineatul (3) din Directiva 2002/58 reiese că, prin adoptarea acestei directive, legiuitorul Uniunii nu a intenționat să exercite nicio competență în domeniul legii penale.

31. Aceste două motive sunt suficiente pentru a explica rațiunea pentru care, în pofida faptului că măsurile legislative naționale adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58 pentru cercetarea și urmărirea penală a infracțiunilor intră în domeniul de aplicare al acestei măsuri, statele membre își păstrează competența de a defini „infracțiunile", inclusiv „infracțiunile grave", și de a stabili sancțiuni pentru astfel de comportamente [42].

3. Criteriul de control al exercitării posibilității prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 de a deroga de la principiul confidențialității

32. Curtea a subliniat că posibilitatea de a deroga [43] printre altele de la principiul confidențialității prevăzut la articolul 5 alineatul (1) din Directiva 2002/58 trebuie să facă obiectul unei interpretări stricte, astfel încât să nu devină regula generală, lipsind astfel principiul menționat de conținut [44]. Exercitarea acestei posibilități trebuie astfel să respecte printre altele principiile echivalenței [45] și efectivității [46]. De asemenea, aceasta trebuie să respecte principiile generale ale dreptului Uniunii, inclusiv principiul proporționalității [47], precum și articolele 7, 8 și 11 [48] și articolul 52 alineatul (1) din cartă [49]. Obiectivul combaterii infracțiunilor grave trebuie să fie întotdeauna conciliat cu exercitarea drepturilor fundamentale afectate de aceasta. Drepturile consacrate la articolele 7, 8 și 11 din cartă nu sunt prerogative absolute, iar exercitarea lor trebuie să fie luată în considerare în raport cu funcția lor în societate [50]. Astfel, articolul 52 alineatul (1) din cartă prevede că restrângerile asupra exercitării acestor drepturi, în măsura în care restrângerile sunt prevăzute de

40 A se vedea prin analogie Hotărârea Prokuratuur, punctele 41 și 42. Curtea a precizat că, în lipsa unei reglementări a Uniunii în materie și în conformitate cu principiul autonomiei procedurale, „revine, în principiu, numai dreptului național sarcina de a stabili normele referitoare la admisibilitatea și la aprecierea, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de acte de infracționalitate gravă, a informațiilor și a elementelor de probă care au fost obținute printr-o stocare generalizată și nediferențiată a acestor date, contrară dreptului Uniunii". Temeiul juridic al Directivei 2002/58 îl constituie articolul 114 TFUE (fostul articolul 95 TCE), iar nu, de exemplu, articolul 83 alineatul (1) primul paragraf TFUE. În schimb, temeiul juridic al Directivei 2016/681 îl constituie primul paragraf al articolului 82 alineatul (1) litera (d) TFUE (cooperarea judiciară în materie penală) și articolul 87 alineatul (2) litera (a) TFUE (cooperarea polițienească).

41 A se vedea punctul 21 din prezentele concluzii.

42 A se vedea prin analogie Hotărârea din 23 octombrie 2007, Comisia/Consiliul (C-440/05, EU:C:2007:625, punctele 66, 70 și 71, precum și jurisprudența citată). A se vedea de asemenea Hotărârea din 28 aprilie 2011, El Dridi (C-61/11 PPU, EU:C:2011:268, punctul 53).

43 Articolul 15 alineatul (1) din Directiva 2002/58 prevede că statele membre „pot adopta" măsuri legislative care restrâng anumite drepturi și obligații prevăzute de această directivă.

44 Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctul 89). Avocatul general Saugmandsgaard Øe a considerat că, „chiar dacă fiecare stat membru are posibilitatea de a aprecia care este pragul de pedeapsă adecvat pentru a defini o infracțiune gravă, acesta are totuși obligația de a nu stabili un nivel atât de scăzut, în raport cu nivelul obișnuit al pedepselor aplicabile în statul respectiv, încât excepțiile de la interdicția stocării și utilizării datelor cu caracter personal care sunt prevăzute la articolul 15 alineatul (1) menționat s-ar transforma în principii […]", Concluziile prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300, punctul 114).

45 Nimic nu indică faptul că reglementarea italiană în discuție nu respectă acest principiu.

46 Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258, punctul 127).

47 A se vedea de asemenea considerentul (11) al Directivei 2002/58.

48 A se vedea de asemenea considerentul (2) al Directivei 2002/58.

49 Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctul 89), și 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, punctele 111-113). A se vedea de asemenea Concluziile avocatului general Saugmandsgaard Øe prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300, punctele 116-120). În Hotărârea din 8 martie 2022, Bezirkshauptmannschaft Hartberg-Fürstenfeld (Efect direct) (C-205/20, EU:C:2022:168, punctul 31), Curtea a amintit că principiul proporționalității este obligatoriu pentru statele membre atunci când pun în aplicare dreptul Uniunii. În acest context, statele membre trebuie să respecte articolul 49 alineatul (3) din cartă atunci când adoptă sancțiuni penale, chiar și în lipsa unei reglementări a Uniunii care să armonizeze aceste sancțiuni.

50 Articolul 52 alineatul (1) din cartă. 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, punctul 120).

lege, trebuie să respecte substanța acestor drepturi și, cu respectarea principiului proporționalității, trebuie să fie necesare și să răspundă efectiv obiectivelor de interes general recunoscute de Uniunea Europeană sau necesității protejării drepturilor și libertăților celorlalți. Măsurile legislative naționale adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58 trebuie, așadar, să urmărească în mod efectiv și strict unul dintre obiectivele menționate în această dispoziție. Acestea trebuie să se bazeze pe criterii obiective, să fie obligatorii din punct de vedere juridic și să prevadă norme clare și precise care să indice condițiile de fond și de procedură în care furnizorii de servicii de comunicații electronice trebuie să permită autorităților naționale competente accesul la date [51].

33. Pentru a garanta deplina respectare a acestor condiții în practică, accesul autorităților naționale competente la datele păstrate trebuie, în principiu [52], să fie condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă [53] în urma unei cereri motivate formulate de aceste autorități și a informării persoanelor respective [54]. Potrivit unei jurisprudențe constante, la efectuarea acestui control prealabil, o instanță sau o entitate administrativă independentă trebuie să concilieze diferitele interese și drepturi în cauză pentru a asigura un just echilibru între nevoile investigației și necesitatea de a proteja drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal ale persoanelor vizate [55].

34. În speță, articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 stabilește condițiile în care o instanță națională trebuie să dispună ca furnizorii de servicii de comunicații electronice să acorde parchetului acces la date la cererea acestuia din urmă. Este cert [56] că articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 stabilește în termeni clari și preciși împrejurările și condițiile în care o instanță națională poate impune furnizorilor de servicii de comunicații electronice să permită un astfel de acces. Cu toate acestea, instanța de trimitere consideră că pedeapsa „cu închisoarea de cel puțin trei ani” este excesiv de largă, întrucât intră în sfera sa infracțiuni precum furtul simplu, care nu cauzează tulburări sociale semnificative.

35. Deși articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 vizează în mod potențial o gamă largă de infracțiuni, Curtea nu dispune de niciun element de probă în cadrul prezentei proceduri care să includă un număr atât de mare de infracțiuni astfel încât accesul la date să devină regula, iar nu excepția [57]. Pragul pedepsei cu închisoarea de cel puțin trei ani prevăzut de această dispoziție nu pare excesiv de scăzut [58]. Prin analogie, articolul 3 punctul 9 din Directiva

[51] Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctele 117-119). A se vedea de asemenea 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, punctele 110 și 129-133).

[52] De exemplu, articolul 132 alineatul 3a din Decretul legislativ nr. 196/2003 stabilește norme speciale pentru accesul la date în cazuri urgente. În Concluziile prezentate în cauza La Quadrature du Net și alții (Date cu caracter personal și combaterea contrafacerii) (C-470/21, EU:C:2022:838, punctele 99-105), avocatul general Szpunar a considerat că un control prealabil nu este necesar decât atunci când există o ingerință gravă în viața privată a utilizatorilor de servicii de comunicații electronice. Controlul prealabil este necesar deoarece, în prezenta procedură, având în vedere natura datelor la care parchetul solicită accesul, ingerința este gravă.

[53] Jurisprudența Curții, iar nu Directiva 2002/58, a stabilit obligația de control prealabil: Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctele 120 și 121, precum și jurisprudența citată).

[54] Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970, punctele 120 și 121).

[55] Hotărârea Prokuratuur, punctul 52.

[56] Sub rezerva verificării de către instanța de trimitere.

[57] A se vedea analiza din Concluziile avocatului general Saugmandsgaard Øe prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300, punctele 116-120). Revine însă instanței de trimitere sarcina de a aprecia acest aspect.

[58] Împrejurarea că definirea infracțiunilor și regimul pedepselor dintr-un stat membru diferă de modul în care infracțiunile și pedepsele sunt definite în alt stat membru nu poate, în sine, să afecteze proporționalitatea reglementării. A se vedea prin analogie Hotărârea din 8 iulie 2010, Sjöberg și Gerdin (C-447/08 și C-448/08, EU:C:2010:415, punctul 38).

2016/681 [59] definește „infracțiunile grave” ca fiind „infracțiunile enumerate în anexa II, care sunt pasibile de pedepse cu închisoarea sau cu o măsură privativă de libertate pe o perioadă maximă de cel puțin trei ani în temeiul dreptului intern al unui stat membru” [60]. Cu toate acestea, Curtea a precizat că, întrucât articolul 3 alineatul (9) din Directiva 2016/681 se referă mai curând la pedeapsa maximă aplicabilă decât la minimul necesar, nu este exclus ca „datele […] să poată face obiectul unei prelucrări în scopul combaterii infracțiunilor care, deși îndeplinesc criteriul prevăzut de această dispoziție referitor la pragul de gravitate, nu sunt, date fiind specificitățile sistemului penal național, infracțiuni grave, ci de drept comun” [61].

36. Pedeapsa de trei ani prevăzută la articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 se referă la pedeapsa maximă aplicabilă și, prin urmare, se poate aplica unor infracțiuni precum furtul simplu [62]. Prin urmare, este necesar să se examineze modul în care articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 este aplicat în practică. Sub rezerva verificării de către instanța de trimitere, articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 pare să stabilească două criterii diferite de control prealabil de către o instanță națională, în funcție de natura infracțiunilor care fac obiectul anchetei.

37. Primul dintre aceste criterii de control impune [63] instanțelor naționale să autorizeze accesul parchetului la datele păstrate de furnizorii de servicii de comunicații electronice în cazul în care aceste date sunt relevante pentru stabilirea faptelor și dacă există indicii suficiente cu privire la infracțiuni de amenințare și de hărțuire sau de tulburare a liniștii persoanelor prin intermediul telefonului, atunci când amenințarea, hărțuirea și tulburarea sunt grave. Prin urmare, instanța națională trebuie să efectueze o apreciere individuală a gravității infracțiunii în cauză și să verifice dacă cercetarea și urmărirea penală a infracțiunii justifică restrângerea drepturilor generale consacrate la articolele 7, 8 și 11 din cartă, precum și a drepturilor specifice prevăzute la articolele 5, 6 și 9 din Directiva 2002/58. Acest criteriu impune o apreciere individuală, într-un caz dat, a aspectului dacă ingerința în aceste drepturi este proporțională în raport cu obiectivul de interes general de combatere a infracționalității.

38. În schimb, cel de al doilea dintre aceste criterii de control, care este relevant în contextul prezentei proceduri, impune [64] instanțelor naționale să autorizeze accesul parchetului la datele păstrate de furnizorii de servicii de comunicații electronice în cazul în care aceste date sunt relevante pentru stabilirea faptelor și dacă există indicii suficiente privind săvârșirea unei infracțiuni susceptibile de a fi sancționată printre altele cu o pedeapsă cu închisoarea de cel puțin trei ani. În acest caz, rolul instanței naționale se limitează la verificarea îndeplinirii acestor cerințe

[59] Directiva 2016/681 privește transferul și prelucrarea datelor pasagerilor pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave.

[60] Curtea a statuat că cerințele care rezultă din această dispoziție, referitoare la natura și severitatea sancțiunii aplicabile, sunt, în principiu, în măsură să limiteze aplicarea sistemului instituit prin Directiva 2016/681 la infracțiuni care prezintă un nivel suficient de gravitate care să poată justifica ingerința în drepturile fundamentale consacrate la articolele 7 și 8 din cartă. Hotărârea din 21 iunie 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, punctul 150).

[61] Curtea a statuat astfel că statele membre trebuie să se asigure că sistemul instituit prin Directiva 2016/681 este limitat la combaterea infracțiunilor grave, iar nu a celor de drept comun. Hotărârea din 21 iunie 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, punctele 151 și 152). Obiectul și domeniul de aplicare ale Directivei 2016/681, care prevede printre altele schimbul de date PNR între statele membre, nu se suprapun cu cele ale Directivei 2002/58. Rezultă că dispozițiile acestor directive trebuie apreciate separat și pe baza propriilor cerințe. În această privință și contrar situației în ceea ce privește articolul 15 alineatul (1) din Directiva 2002/58, noțiunea de „infracțiune gravă” care figurează în Directiva 2016/681 este o noțiune autonomă de drept al Uniunii. A se vedea de asemenea în această privință considerentul (12) al Directivei 2016/681, articolul 3 alineatul (9) din aceasta și anexa II la aceasta.

[62] A se vedea prin analogie Hotărârea din 21 iunie 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, punctul 151).

[63] Textul în limba originală utilizează sintagma „i dati sono acquisti”.

[64] Sub rezerva verificării de către instanța de trimitere, utilizarea modului indicativ la articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 („i dati sono acquisiti”) implică faptul că accesul la datele în discuție este acordat de instanța națională cu condiția îndeplinirii condițiilor obiective impuse de această dispoziție.

obiective, fără a avea posibilitatea de a efectua o evaluare individualizată a intereselor în speță [65]. Controlul efectuat de instanța națională în temeiul articolului 132 alineatul 3 din Decretul legislativ nr. 196/2003 nu are astfel nicio legătură reală cu împrejurările specifice ale cauzei cu care este sesizată.

39. Deși este posibil ca instanțele naționale să nu fie competente să controleze definirea de către legiuitor a infracțiunilor sau modul de stabilire a gradului de gravitate a acestora de către legiuitor [66], aceste instanțe trebuie totuși să fie competente să efectueze o apreciere individualizată a aspectului dacă acordarea accesului, potrivit unor măsuri legislative adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, la date sensibile care permit să se tragă concluzii precise cu privire la viața privată a unui utilizator, care constituie astfel o ingerință gravă în drepturile fundamentale consacrate la articolele 7, 8, 11 și la articolul 52 alineatul (1) din cartă, este proporțională.

40. Rezultă că, urmare a măsurilor adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, accesul la date sensibile nu poate fi acordat decât în cazul în care: (i) infracțiunea în cauză atinge pragul de gravitate stabilit în prealabil de legiuitorul național; iar (ii) o instanță sau o altă entitate administrativă independentă consideră, în urma unei aprecieri sau a unui control individualizat, că ingerința în drepturile fundamentale pe care o implică acordarea acestui acces este proporțională, în vederea obiectivului de interes general de combatere a infracționalității într-un caz specific. Cu toate acestea, în anumite cazuri, este posibil să nu se acorde acces la astfel de date chiar și în cazul în care infracțiunea atinge pragul de gravitate prevăzut de dreptul național.

41. Infracțiunea de furt calificat în speță este considerată „gravă” în dreptul național, întrucât poate fi sancționată printre altele cu o pedeapsă cu închisoarea de la doi la șase ani, întrunind astfel în pragul de gravitate prevăzut la articolul 132 alineatul 3 din Decretul legislativ nr. 196/2003 [67]. Atunci când aplică măsurile adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, instanțele italiene nu par să fie competente să repună în discuție calificarea furtului calificat drept „infracțiune gravă” în dreptul național. În cazul în care pragul stabilit de dreptul național nu a fost atins, instanța de trimitere nu poate, așadar, să acorde accesul la datele solicitate [68].

42. În cazul în care pragul stabilit de legiuitorul național este atins, instanța de trimitere trebuie, în temeiul articolului 15 alineatul (1) din Directiva 2002/58, să verifice dacă, având în vedere ansamblul împrejurărilor specifice speței, ingerința în drepturile fundamentale pe care o implică accesul este proporțională cu obiectivul de interes general de combatere a infracțiunii respective. În această privință, instanța de trimitere trebuie să ia în considerare și să evalueze comparativ toate drepturile și interesele relevante, inclusiv printre altele prejudiciul cauzat drepturilor de proprietate ale victimelor, protejate de articolul 17 din cartă, precum și faptul că telefoanele mobile pot conține informații foarte sensibile referitoare la viața privată, profesională și

[65] În ședință, observațiile Parchetului (Bolzano) și ale guvernului italian cu privire la rolul instanței naționale și la întinderea controlului prealabil în temeiul articolului 132 alineatul 3 din Decretul legislativ nr. 196/2003 au fost divergente. În timp ce Parchetul (Bolzano) a susținut că instanța națională trebuie, înainte de a acorda accesul la astfel de date, să efectueze o evaluare individuală a proporționalității acordării acestui acces, guvernul italian a subliniat că instanța națională trebuie să respecte, în conformitate cu articolul 101 din Costituzione della Repubblica Italiana (Constituția Republicii Italiene) și cu articolul 1 din Codice penale (Codul penal), principiul legalității și, prin urmare, nu poate adopta ceea ce a descris ca fiind o interpretare creativă a legii. Revine instanței de trimitere sarcina de a interpreta dispozițiile aplicabile de drept național.

[66] Cu excepția cazului în care dreptul național permite acest lucru și sub rezerva respectării printre altele a articolului 49 din cartă.

[67] O pedeapsă cu închisoarea de cel puțin trei ani.

[68] Articolul 52 alineatul (1) din cartă prevede că legea trebuie să prevadă orice restrângere a exercițiului unui drept recunoscut de cartă. Aceasta implică faptul că instanțele naționale sunt, în principiu, obligate să respecte legislația națională care conține astfel de restrângeri.

financiară a proprietarilor lor [69]. Accesul la datele în cauză poate fi singurul mijloc eficient disponibil pentru a cerceta și a urmări penal infracțiunile în cauză și pentru a asigura că autorii lor, încă necunoscuți, nu acționează în condiții de impunitate. Drepturile terților [70] trebuie de asemenea să fie luate în considerare.

43. În ceea ce privește drepturile terților, din dosarele instanței de trimitere reiese [71] că Parchetul (Bolzano) a solicitat accesul la datele referitoare la comunicările efectuate pe telefoanele mobile furate începând cu 29 octombrie 2021 cu privire la primul furt comis la 27 octombrie 2021 [72] și începând cu 20 noiembrie 2021 cu privire la al doilea furt comis la această dată [73]. Aceste date arată că cererile de acces afectează, într-o măsură foarte limitată, drepturile victimelor, care sunt garantate printre altele de articolele 7, 8 și 11 din cartă [74]. Guvernul italian a precizat de asemenea în observațiile sale scrise că procedura națională se referă numai la date care ar fi utile pentru identificarea autorului/autorilor furturilor în cauză. În cazul identificării apelurilor către sau de la terți care nu au legătură cu furtul, aceste date ar fi distruse, în conformitate cu articolul 269 din Codul de procedură penală [75]. În sfârșit, alineatul 3c al articolului 132 din Decretul legislativ nr. 196/2003 prevede că datele obținute cu încălcarea dispozițiilor alineatelor 3 și 3a nu pot fi utilizate [76].

VI. Concluzie

44. Având în vedere considerațiile care precedă, propunem Curții să răspundă la întrebarea preliminară adresată de Tribunale di Bolzano (Tribunalul din Bolzano, Italia) după cum urmează:

Articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, și articolele 7, 8 și 11, precum și articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene

trebuie interpretate în sensul că nu se opun unei reglementări naționale care impune unei instanțe să autorizeze accesul parchetului la datele păstrate în mod legal de furnizorii de servicii de comunicații electronice care permit deducerea unor concluzii precise cu privire la viața privată a unui utilizator în cazul în care aceste date sunt relevante pentru stabilirea faptelor și în cazul în care există indicii suficiente privind săvârșirea unei infracțiuni grave, astfel cum este definită de dreptul național, pasibilă de o pedeapsă cu închisoarea de cel puțin trei ani. Înainte de a acorda

[69] Telefoanele mobile pot conține fotografii, date medicale, extrase de cont, parole etc. Prin urmare, furtul unui telefon mobil poate compromite identitatea digitală a proprietarului său, iar efectele furtului pot depăși considerabil pierderea valorii monetare a telefonului. Prin urmare, instanța de trimitere ar trebui de asemenea să ia în considerare și să pună în balanță eventualele prejudicii cauzate drepturilor victimelor în special în temeiul articolelor 7, 8 și 17 din cartă.

[70] Cum ar fi victimele presupusei infracțiuni.

[71] Sub rezerva verificării de către instanța de trimitere.

[72] Număr de referință RGNR 9228/2021.

[73] Număr de referință RGNR 9794/2021.

[74] Deși datele pot viza comunicări adresate victimei după data furtului, acestea nu se referă, într-o măsură reală, la comunicările efectuate de victimă și nici la datele de localizare a acesteia.

[75] Potrivit guvernului italian, versiunea aplicabilă a articolului 269 alineatul 2 din Codul de procedură penală prevede că „[…] înregistrările se păstrează până la pronunțarea hotărârii definitive. Cu toate acestea, pentru a proteja confidențialitatea, părțile interesate pot solicita instanței care a autorizat sau a validat interceptarea să distrugă înregistrările care nu au fost incluse în dosar” (întrucât sunt irelevante). Deși accesul la datele referitoare la terți nevinovați este nelimitat, utilizarea acestor date pare, sub rezerva verificării de către instanța de trimitere, să fie circumscrisă de dreptul național.

[76] În cererea de decizie preliminară nu se explică nici sensul exact al acestei dispoziții, nici aplicarea sa în practică.

accesul, instanța națională trebuie să efectueze o apreciere individualizată a aspectului dacă ingerința în drepturile fundamentale ocazionată de acordarea acestui acces este proporțională, având în vedere printre altele gravitatea infracțiunii concrete și situația de fapt din speță.