



Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
DOMNUL GIOVANNI PITRUZZELLA
prezentate la 21 ianuarie 2020¹

Cauza C-746/18

**H. K.
împotriva
Prokuratuur**

[cerere de decizie preliminară formulată de Riigikohus (Curtea Supremă, Estonia)]

„Trimitere preliminară – Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice – Confidențialitatea comunicațiilor – Furnizori de servicii de comunicații electronice – Păstrare generalizată și nediferențiată a datelor de transfer și a datelor de localizare – Investigații preliminare – Accesul autorității de investigare la datele păstrate pentru perioade cuprinse între o zi și un an – Autorizație dată de Ministerul Public – Utilizarea datelor ca probe în cadrul procesului penal – Directiva 2002/58/CE – Articolul 1 alineatul (3), articolul 3 și articolul 15 alineatul (1) – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8 și 11, precum și articolul 52 alineatul (1)”

I. Introducere

1. Prezenta cerere de decizie preliminară privește interpretarea articolului 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)², astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009³, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene⁴.

2. Această cerere a fost formulată în cadrul unei proceduri penale declanșate împotriva lui H. K., pentru motivul că aceasta din urmă ar fi săvârșit mai multe furturi, ar fi utilizat un card bancar care aparținea unei alte persoane și ar fi săvârșit acte de violență asupra altui participant la o procedură judiciară.

3. Procesele-verbale pe care se întemeiază constatarea acestor infracțiuni au fost întocmite în special pe baza datelor cu caracter personal generate în cadrul furnizării de servicii de comunicații electronice. Riigikohus (Curtea Supremă, Estonia) are îndoieli cu privire la compatibilitatea cu dreptul Uniunii a condițiilor în care serviciile de investigare au avut acces la aceste date.

¹ Limba originală: franceza.

² JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63.

³ JO 2009, L 337, p. 11. Denumită în continuare „Directiva 2002/58”.

⁴ Denumită în continuare „carta”.

4. Aceste îndoieli privesc, în primul rând, problema dacă durata perioadei pentru care serviciile de investigare au avut acces la date constituie un criteriu care permite să se evalueze gravitatea ingerinței pe care o constituie acest acces în drepturile fundamentale ale persoanelor în cauză.

5. În al doilea rând, instanța de trimitere dorește să afle dacă Prokuratuur (Ministerul Public, Estonia), ținând seama de diferitele misiuni care îi sunt încredințate de reglementarea estoniană, constituie o autoritate administrativă „independentă” în sensul Hotărârii din 21 decembrie 2016, *Tele2 Sverige* și *Watson* și alții⁵.

II. Cadrul juridic

A. Directiva 2002/58

6. În temeiul articolului 1 alineatul (3) din Directiva 2002/58, aceasta „nu se aplică activităților care nu sunt cuprinse în domeniul de aplicare al Tratatului de instituire a Comunității Europene, cum sunt cele menționate la titlurile V și VI ale Tratatului privind Uniunea Europeană, și în orice caz activităților legate de siguranța publică, de apărare, de siguranța statului (inclusiv de bunăstarea economică a acestuia, dacă activitățile respective sunt legate de chestiuni de siguranța statului) și activităților statului în domeniul legii penale”.

7. În plus, articolul 15 alineatul (1) din această directivă prevede că „[s]tatele 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/CE⁶]. 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 [Uniunii], inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) al Tratatului privind Uniunea Europeană”.

B. Dreptul estonian

1. Legea privind comunicațiile electronice

8. *Elektroonilise side seadus* (Legea privind comunicațiile electronice)⁷ din 8 decembrie 2004, în versiunea aplicabilă litigiului principal, prevede la articolul 111¹, intitulat „Obligația de păstrare a datelor”:

„[...]”

⁵ C-203/15 și C-698/15, denumită în continuare „Hotărârea *Tele2 Sverige* și *Watson* și alții”, EU:C:2016:970 [punctul 120 și dispozitiv, punctul 2)].

⁶ Directiva 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).

⁷ RT I 2004, 87, 593.

(2) Furnizorii de servicii de telefonie fixă și mobilă, precum și de rețea de servicii de telefonie fixă și mobilă în rețea au obligația să păstreze următoarele date:

- 1) numărul de la care se efectuează apelul, precum și numele și adresa abonatului;
- 2) numărul apelat, precum și numele și adresa abonatului;
- 3) în cazul utilizării unor servicii suplimentare, precum redirectionarea sau transferul apelului, numărul format, precum și numele și adresa abonatului;
- 4) data, precum și ora la care a fost inițiat și s-a terminat apelul;
- 5) serviciul de telefonie fixă sau mobilă utilizat;
- 6) identificatorul internațional al abonatului mobil (*International Mobile Subscriber Identity* – IMSI) al persoanei care efectuează apelul și al persoanei apelate;
- 7) identificatorul internațional al echipamentului mobil (*International Mobile Equipment Identity* – IMEI) al persoanei care efectuează apelul și al persoanei apelate;
- 8) identificatorul de celulă la momentul inițierii unui apel;
- 9) datele privind localizarea geografică a celulelor de comunicații prin raportare la identificatorul de celulă al acestora în perioada în care sunt păstrate datele;
- 10) în cazul unor servicii de telefonie mobilă anonime preplătite, data și ora primei activări a serviciului, precum și identificatorul locului în care serviciul a fost activat.

[...]

(4) Datele menționate la alineatele 2 și 3 ale prezentului articol sunt păstrate o perioadă de un an de la data comunicației, în cazul în care sunt generate sau prelucrate în cursul furnizării unui serviciu de comunicații [...]

[...]

(11) Datele menționate la alineatele (2) și (3) ale prezentului articol sunt transferate:

- 1) potrivit kriminaalmenetluse seadustik [Codul de procedură penală⁸], unei autorități de investigare, unei autorități autorizate să ia măsuri de supraveghere, Ministerului Public și instanței;

[...]”

2. Codul de procedură penală

9. Articolul 17 din Codul de procedură penală, în versiunea aplicabilă litigiului principal, intitulat „Participanții la procedura judiciară”, prevede la alineatul (1):

„Participanții la procedura judiciară sunt: Ministerul Public [...]”

⁸ RT I 2003, 27, 166.

10. Potrivit articolului 30 din Codul de procedură penală, intitulat „Ministerul Public în procedura penală”:

„(1) Ministerul Public conduce procedura de cercetare, căreia îi asigură legalitatea și efectivitatea, și susține acțiunea publică în fața instanței.

(2) Competențele Ministerului Public în procedura penală sunt exercitate de un procuror în numele Ministerului Public, care își desfășoară activitatea în mod independent și este supus numai legii.”

11. Articolul 90¹ din Codul de procedură penală, intitulat „Solicitarea de date adresată întreprinderilor de comunicații”, prevede la alineatele (2) și (3):

„(2) Autoritatea de investigare poate, în procedura de cercetare, cu autorizarea dată de Ministerul Public, sau în procedura judiciară, cu autorizarea dată de instanță, să solicite unui furnizor de servicii de comunicații electronice datele prevăzute la articolul 111¹ alineatele (2) și 3 din Legea privind comunicațiile electronice, care nu sunt menționate la alineatul (1) al prezentului articol. Autorizația de solicitare a datelor menționează perioada pentru care este autorizată solicitarea datelor, cu indicarea exactă a zilelor.

(3) Potrivit prezentului articol, datele pot fi solicitate numai dacă sunt absolut necesare pentru atingerea obiectivului procedurii penale.”

12. Articolul 211 din Codul de procedură penală, intitulat „Obiectivul procedurii de cercetare”, are următorul cuprins:

„(1) Obiectivul procedurii de cercetare este colectarea probelor și crearea celorlalte condiții necesare desfășurării unei proceduri judiciare.

(2) În cursul procedurii de cercetare, autoritatea de investigare și Ministerul Public examinează elementele incriminatoare și dezincriminatoare în privința suspectului sau a inculpatului.”

3. *Legea privind Ministerul Public*

13. Prokuratuuriseadus (Legea privind Ministerul Public)⁹ din 22 aprilie 1998, în versiunea aplicabilă litigiului principal, prevede la articolul 1, intitulat „Ministerul Public”:

„(1) Ministerul Public este o autoritate aflată sub controlul Justiitsministeeriumi [Ministerul Justiției, Estonia] care participă la planificarea măsurilor necesare de supraveghere în vederea combaterii și a identificării infracțiunilor, conduce procedura de cercetare penală, căreia îi asigură legalitatea și efectivitatea, susține acțiunea publică în fața instanței și îndeplinește alte misiuni care îi revin potrivit legii.

(1¹) Ministerul Public îndeplinește misiunile care îi revin potrivit legii în mod independent și își desfășoară activitatea conform prezentei legi, altor legi sau actelor juridice adoptate în temeiul acestora.

[...]”

⁹ RT I 1998, 41, 625.

14. Articolul 2 din Legea privind Ministerul Public, intitulat „Procurorul”, prevede la alineatul (2):

„Procurorul își îndeplinește misiunile în mod independent și își desfășoară activitatea numai în conformitate cu legea și cu propria convingere.”

III. Situația de fapt, procedura principală și întrebările preliminare

15. Prin decizia din 6 aprilie 2017, H. K. a fost condamnată de Viru Maakohus (Tribunalul de Primă Instanță din Viru, Estonia) la o pedeapsă cu închisoarea de doi ani pentru săvârșirea, în cursul perioadei cuprinse între 4 august 2015 și 1 februarie 2016, a opt furturi de produse alimentare și de alte bunuri materiale cu o valoare cuprinsă între 3 euro și 40 de euro, precum și de sume de bani cu valori cuprinse între 5,20 euro și 2 100 de euro, pentru utilizarea cardului bancar al unei alte persoane pentru a retrage bani de la un bancomat, cauzându-i acestei persoane un prejudiciu de 3 941,82 euro, și pentru săvârșirea unor acte de violență asupra altui participant la o procedură judiciară¹⁰.

16. Pentru a o condamna pe H. K. pentru aceste infracțiuni, Viru Maakohus (Tribunalul de Primă Instanță din Viru) s-a întemeiat, între altele, pe mai multe procese-verbale întocmite pe baza datelor referitoare la comunicații electronice, menționate la articolul 111¹ alineatul (2) din Legea privind comunicațiile electronice, pe care autoritatea de investigare le-a colectat de la un furnizor de servicii de telecomunicații în cursul procedurii de cercetare, după ce a obținut, în temeiul articolului 90¹ alineatul (2) din Codul de procedură penală, autorizații acordate de un procuror din cadrul Viru Ringkonnaprokuratuur (Parchetul Districtual din Viru, Estonia).

17. Astfel, la 2 noiembrie 2015, un procuror din cadrul Parchetului Districtual din Viru a autorizat autoritatea de investigare să solicite întreprinderii de telecomunicații furnizarea datelor menționate la articolul 111¹ alineatul (2) din Legea privind comunicațiile electronice pentru a se stabili, prin intermediul a două numere de telefon mobil ale H. K., transmiterea comunicațiilor și a mesajelor, durata acestora și modul în care a fost efectuată transmiterea, precum și datele personale și localizarea persoanei care a efectuat apeluri sau a transmis mesaje și a persoanei apelate sau a destinatarului mesajelor, la 21 septembrie 2015.

18. În temeiul acestei autorizații, autoritatea de investigare a întocmit la 4 noiembrie 2015 un proces-verbal privind datele obținute de la întreprinderea de comunicații, în care erau menționate antenele de transmisie în raza cărora a fost utilizat numărul de abonat al H. K. la 21 septembrie 2015 după ora 19.00. Prin intermediul acestui proces-verbal și al altor probe, Ministerul Public a dorit să demonstreze în fața instanței că H. K. a săvârșit furtul din 21 septembrie 2015.

19. La 25 februarie 2016, în vederea investigației referitoare la o infracțiune prevăzută la articolul 303 alineatul (1) din Karistusseadustik (Codul penal)¹¹, un procuror din cadrul Parchetului Districtual din Viru a autorizat autoritatea de investigare să solicite întreprinderii de telecomunicații să furnizeze datele prevăzute la articolul 111¹ alineatul (2) din Legea privind comunicațiile electronice în legătură cu șapte numere de abonat utilizate de H. K. în perioada cuprinsă între 1 martie 2015 și 19 februarie 2016.

¹⁰ Instanța de trimitere precizează că, în urma contopirii acestei pedepse cu pedeapsa cu închisoarea de patru ani și șapte luni la care H. K. a fost condamnată prin hotărârea Viru Maakohus (Tribunalul de Primă Instanță din Viru) din 22 martie 2016, H. K. a fost condamnată la o pedeapsă cu închisoarea cumulată de cinci ani și o lună.

¹¹ Este vorba despre infracțiunea care constă în exercitarea unei influențe asupra justiției. Arătăm că faptele reproșate lui H. K. au fost recalificate, cu privire la acest aspect, de către Viru Maakohus (Tribunalul de Primă Instanță din Viru) în conformitate cu articolul 323 alineatul (1) din Codul penal, în violență asupra altui participant la procedura judiciară.

20. În temeiul acestei autorizații, autoritatea de investigare a întocmit la 15 martie 2016 un proces-verbal privind datele obținute de la întreprinderea de comunicații în care sunt indicate zilele în care H. K. i-a apelat pe ceilalți inculpați în cauză și a primit apeluri de la aceștia, precum și zilele în care H. K. a trimis mesaje către ceilalți inculpați și a primit mesaje de la aceștia. Prin intermediul acestui proces-verbal și al altor probe, Ministerul Public a dorit să demonstreze în fața instanței că, începând cu primăvara anului 2015, H. K. i-a amenințat în mod repetat prin telefon pe ceilalți inculpați.

21. Tot în temeiul acestei autorizații, autoritatea de investigare a întocmit la 20 aprilie 2016 și la 6 mai 2016 alte procese-verbale privind date obținute de la întreprinderea de comunicații. Aceste procese-verbale indică stațiile de bază în raza cărora au fost efectuate și au fost primite apeluri la 4, la 27 și la 31 august 2015, precum și între 1 și 3 septembrie 2015, prin șase numere de abonat utilizate de H. K. Prin intermediul acestor procese-verbale și al altor probe, Ministerul Public a dorit să probeze în fața instanței că H. K. a săvârșit șase furturi în zilele menționate.

22. La 20 aprilie 2016, autoritatea de investigare a întocmit un proces-verbal care cuprinde date referitoare la două numere de abonat utilizate de H. K. Mai precis, acest proces-verbal indică în special stațiile de bază în raza cărora au fost efectuate și au fost primite apeluri în perioada cuprinsă între 16 și 19 ianuarie 2015 prin aceste numere de abonat. Prin intermediul acestui proces-verbal și al altor probe, Ministerul Public a dorit să probeze că, în perioada cuprinsă între 17 și 19 ianuarie 2015, H. K. este persoana care, cu ajutorul cardului bancar al victimei, a retras numerar de la bancomat.

23. Datele aflate la originea procesului-verbal menționat au fost obținute de la întreprinderea de telecomunicații pe baza autorizațiilor emise la 28 ianuarie 2015 și la 2 februarie 2015 într-o altă cauză penală de un procuror din cadrul Parchetului Districtual din Viru. Acea cauză privea infracțiuni prevăzute la articolul 200 alineatul 2 punctele 7, 8 și 9 din Codul penal, respectiv două tâlhării săvârșite la 23 și la 27 ianuarie 2015 de un grup în care a fost utilizată o armă și care s-au realizat prin efracție. Aceste autorizații au permis autorității de investigare să solicite întreprinderii de telecomunicații să furnizeze datele prevăzute la articolul 111¹ alineatul (2) din Legea privind comunicațiile electronice în legătură cu două numere de abonat și cu diferite identificatoare internaționale ale echipamentului mobil ale H. K. în perioada cuprinsă între 1 ianuarie 2015 și 2 februarie 2015.

24. Din această descriere a situației de fapt din procedura principală reiese că Ministerul Public a autorizat autoritatea de investigare, în conformitate cu articolul 90¹ alineatul (2) din Codul de procedură penală, să adreseze cereri de furnizare de date întreprinderii de telecomunicații în cadrul procedurii de cercetare. Autorizațiile au fost emise în privința datelor aferente numărului de abonat al inculpatului în scopul investigării diferitor infracțiuni pe durata unei zile, a aproximativ o lună și, respectiv, a aproximativ un an.

25. H. K. a formulat apel împotriva hotărârii Viru Maakohus (Tribunalul de Primă Instanță din Viru) în fața Tartu Ringkonnakohus (Curtea de Apel din Tartu, Estonia), care a respins acest apel prin decizia din 17 noiembrie 2017. Astfel, H. K. a formulat recurs la Riigikohus (Curtea Supremă), prin care a solicitat anularea deciziilor primei instanțe și celei de a doua instanțe, încetarea urmăririi penale împotriva sa, precum și achitarea sa.

26. H. K. arată că procesele-verbale care conțin date obținute de la întreprinderea de telecomunicații nu constituie probe admisibile, iar condamnarea sa pe baza acestor procese-verbale este neîntemeiată. În conformitate cu Hotărârea Tele2 Sverige și Watson și alții, normele din articolul 111¹ din Legea privind comunicațiile electronice, care prevăd obligația acestor furnizori de servicii să păstreze date referitoare la comunicații, precum și utilizarea acestor date în scopul condamnării sale, ar fi contrare articolului 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă.

27. Astfel, potrivit instanței de trimitere, se ridică problema dacă procesele-verbale în cauză, pe care autoritatea de investigare le-a întocmit pe baza unor date, menționate la articolul 111¹ alineatul (2) din Legea privind comunicațiile electronice, solicitate întreprinderii de telecomunicații cu autorizarea Ministerului Public, pot fi considerate probe admisibile.

28. Datele pe care furnizorii de servicii de comunicații electronice ar trebui să le păstreze o perioadă de un an ar cuprinde, printre altele, numărul persoanei care efectuează apelul și al persoanei apelate, numele și adresa abonatului, data și ora la care a fost inițiat și s-a terminat apelul, serviciul de telefonie fixă sau mobilă utilizat, identificatorul internațional al abonatului mobil și identificatorul internațional al echipamentului mobil al persoanei care efectuează apelul și al persoanei apelate, precum și identificatorul de celulă la momentul inițierii apelului și datele de identificare a localizării geografice a celulei. Instanța de trimitere arată că, în acest cadru, este vorba despre date care privesc existența unui transfer de apeluri și de mesaje prin intermediul unui telefon fix sau mobil, precum și localizarea utilizării echipamentului terminal mobil, dar că aceste date nu furnizează indicii cu privire la conținutul informațiilor.

29. Astfel cum ar reieși din Hotărârea Tele2 Sverige și Watson și alții, precum și din Hotărârea din 2 octombrie 2018, Ministerio Fiscal¹², o reglementare națională care guvernează păstrarea datelor de transfer și a datelor de localizare, precum și accesul la aceste date în cadrul unei proceduri penale precum articolul 111¹ alineatele (2) și (4) din Legea privind comunicațiile electronice și articolul 90¹ alineatul (2) din Codul de procedură penală, ar intra în domeniul de aplicare al Directivei 2002/58.

30. Admisibilitatea probelor ar depinde de respectarea normelor de procedură ce reglementează colectarea acestora. Astfel, în cadrul aprecierii admisibilității ca probe a proceselor-verbale în discuție în litigiul principal, ar trebui de asemenea să se examineze în ce măsură colectarea datelor de la întreprinderea de telecomunicații, pe care sunt întemeiate aceste procese-verbale, era conformă cu articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă.

31. Având în vedere Hotărârea Tele2 Sverige și Watson și alții¹³, precum și Hotărârea Ministerio Fiscal¹⁴, instanța de trimitere ridică problema dacă articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că accesul autorităților naționale la date care permit urmărirea și identificarea sursei și a destinației unei comunicații telefonice pe baza telefonului fix sau mobil al suspectului, determinarea datei, a orei, a duratei și a naturii acesteia, identificarea echipamentului terminal mobil utilizat, precum și localizarea echipamentului terminal mobil utilizat constituie o ingerință atât de gravă în drepturile fundamentale garantate de aceste articole din cartă încât acest acces trebuie să fie limitat la combaterea infracționalității grave, independent de perioada pentru care aceste autorități naționale au solicitat accesul la datele păstrate.

32. În această privință, instanța de trimitere consideră că perioada pentru care datele în cauză sunt solicitate constituie un element esențial pentru aprecierea gravității ingerinței în drepturile fundamentale pe care ar constitui-o accesul la datele în cauză. Prin urmare, ar fi posibil ca această ingerință să nu fie considerată gravă, din moment ce datele solicitate ar privi doar o perioadă foarte scurtă, precum o zi. În acest caz, în general, nu ar fi posibil să se deducă, pe baza acestor date, concluzii precise privind viața privată a persoanei în cauză, astfel încât accesul autorităților naționale la datele menționate ar putea fi justificat prin obiectivul de investigare și de urmărire penală a infracțiunilor în general.

¹² C-207/16, denumită în continuare „Hotărârea Ministerio Fiscal”, EU:C:2018:788.

¹³ Dispozitivul acestei hotărâri, punctul 2).

¹⁴ Punctele 53 și 57 din această hotărâre.

33. În plus, instanța de trimitere ridică problema dacă accesul la date precum cele în discuție în litigiul principal poate, având în vedere învățămintele care decurg din Hotărârea Ministerio Fiscal¹⁵, să fie justificat prin același obiectiv, în cazul în care volumul de date la care au acces autoritățile este redus și, prin urmare, ingerința în drepturile fundamentale în cauză nu ar fi gravă. În ceea ce privește volumul de date, ar fi esențial să se țină seama de tipul de date (precum cele referitoare la destinația unei comunicații sau la localizarea echipamentului) și de durata perioadei în cauză (de exemplu, o zi, o lună sau un an). Potrivit acestei instanțe, cu cât infracțiunea ar fi mai gravă, cu atât mai mult ingerința permisă în drepturile fundamentale în cadrul procedurii ar putea fi gravă, ceea ce înseamnă că volumul de date la care autoritățile naționale pot avea acces ar fi mai mare.

34. În sfârșit, instanța de trimitere ridică problema dacă Ministerul Public poate fi considerat autoritate administrativă „independentă” în sensul Hotărârii Tele2 Sverige și Watson și alții¹⁶. Ea arată că, în Estonia, Ministerul Public este cel care conduce procedura de cercetare, al cărei obiectiv este în special colectarea probelor. Ea subliniază de asemenea că autoritatea de investigare și Ministerul Public verifică elementele incriminatoare și elementele dezincriminatoare privind suspectul. În sfârșit, ea observă că competențele Ministerului Public sunt exercitate în numele său de un procuror care își îndeplinește misiunile în mod independent, ceea ce rezultă din articolul 30 alineatele (1) și (2) din Codul de procedură penală și din articolul 1 alineatele (1) și (1¹), precum și din articolul 2 alineatul (2) din Legea privind Ministerul Public.

35. În acest context, instanța de trimitere subliniază că îndoielile sale cu privire la independența impusă de dreptul Uniunii sunt datorate în principal faptului că, după procedura de cercetare, dacă Ministerul Public este convins că au fost colectate toate probele necesare și dacă este cazul, acesta prezintă acuzațiile sale împotriva persoanei în cauză. Această instanță arată că, în acest caz, Ministerul Public este cel care susține acțiunea publică în cadrul procesului și, prin urmare, este în egală măsură participant la procedură. Instanța de trimitere arată de asemenea că Curtea Europeană a Drepturilor Omului a admis deja că, în anumite condiții, pot fi autorizate acte de supraveghere în lipsa unui control judiciar prealabil, cu condiția ca un control judiciar să intervină *a posteriori*¹⁷.

36. În aceste condiții, Riigikohus (Curtea Supremă) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

- „1) Articolul 15 alineatul (1) din Directiva [2002/58], citit în lumina articolelor 7, 8, 11, precum și a articolului 52 alineatul (1) din [cartă], trebuie interpretat în sensul că, în cadrul unei proceduri penale, accesul autorităților statului la date care permit să se stabilească sursa și destinația, data, ora și durata, natura serviciului de comunicații, echipamentul terminal mobil utilizat, precum și locul în care a fost utilizat echipamentul terminal în legătură cu comunicații de la un telefon fix sau mobil al unui suspect implică o ingerință în drepturile fundamentale consacrate la articolele menționate din cartă care prezintă o asemenea gravitate încât să fie necesar ca acest acces să fie limitat, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, la combaterea infracționalității grave, independent de perioada la care se raportează datele păstrate la care au acces autoritățile statului?
- 2) Pornind de la principiul proporționalității formulat la punctele 55-57 din Hotărârea [Ministerio Fiscal], articolul 15 alineatul (1) din Directiva [2002/58] trebuie interpretat în sensul că, în cazul în care volumul datelor menționate în prima întrebare la care autoritățile statului au acces nu este mare (atât din punctul de vedere al naturii datelor, cât și din punctul de vedere al întinderii în timp a acestora), ingerința în drepturile fundamentale ce rezultă astfel poate fi justificată prin

15 Punctele 55-57 din această hotărâre.

16 Punctul 120 și dispozitivul acestei hotărâri, punctul 2).

17 Instanța de trimitere citează în această privință Hotărârea Curții EDO din 2 septembrie 2010, Uzun împotriva Germaniei (CE:ECHR:2010:0902JUD003562305, § 71-74, și Hotărârea Curții EDO din 12 ianuarie 2016, Szabó și Vissy împotriva Ungariei (CE:ECHR:2016:0112JUD003713814, § 77).

obiectivul privind prevenirea, investigarea, detectarea și urmărirea penală a unor infracțiuni în general și că, cu cât volumul de date la care au acces autoritățile statului este mai mare, cu atât infracțiunile împotriva cărora este destinată ingerința trebuie să fie grave?

- 3) Cerința menționată la punctul 2 din dispozitivul Hotărârii [Tele2 Sverige și Watson și alții], potrivit căreia accesul la date al autorităților competente ale statului trebuie să fie supus unui control prealabil exercitat de o instanță sau de o autoritate administrativă independentă, are semnificația că articolul 15 alineatul (1) din Directiva [2002/58] trebuie interpretat în sensul că Ministerul Public, care conduce procedura de cercetare în cadrul căreia, potrivit legii, are obligația să își desfășoare activitatea în mod independent și se supune numai legii și examinează atât elementele incriminatoare, cât și elementele dezincriminatoare în privința inculpatului, însă ulterior susține acțiunea publică în cadrul procedurii judiciare, poate fi considerat autoritate administrativă independentă?”

IV. Analiză

37. Prin intermediul primei și al celei de a doua întrebări preliminare, instanța de trimitere dorește să afle în esență dacă articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că printre criteriile care permit să se aprecieze gravitatea ingerinței în drepturile fundamentale pe care o constituie accesul autorităților naționale competente la date cu caracter personal pe care furnizorii de servicii de comunicații electronice sunt obligați să le păstreze în temeiul unei reglementări naționale figurează categoriile de date în cauză, precum și durata perioadei pentru care este solicitat accesul.

38. Înainte de a răspunde la această întrebare, vom formula două serii de observații introductive care ne vor permite să răspundem, pe de o parte, la argumentele invocate de anumite state membre în ceea ce privește domeniul de aplicare al Directivei 2002/58 și, pe de altă parte, la sugestia Comisiei Europene de a se examina în cadrul prezentei trimiteri preliminare compatibilitatea cu dreptul Uniunii a reglementării estone, în măsura în care impune furnizorilor de servicii de comunicații electronice să păstreze mai multe categorii de date cu caracter personal generate în cadrul acestor servicii.

A. *Observații introductive*

1. *Cu privire la domeniul de aplicare al Directivei 2002/58*

39. Guvernele irlandez, maghiar și polonez ridică probleme cu privire la domeniul de aplicare al Directivei 2002/58.

40. Guvernul irlandez pare să considere că o reglementare națională referitoare la accesul autorităților competente în materie penală la date păstrate ar fi, în temeiul articolului 1 alineatul (3) din Directiva 2002/58, exclusă din domeniul de aplicare al acestei directive.

41. Acest argument trebuie respins în temeiul jurisprudenței Curții rezultate din Hotărârea Tele2 Sverige și Watson și alții, precum și din Hotărârea Ministerio Fiscal.

42. În această privință, trebuie să se arate că Curtea a statuat că măsurile legislative prevăzute la articolul 15 alineatul (1) din Directiva 2002/58 „intră în domeniul de aplicare al acestei directive chiar dacă ele se raportează la activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor și chiar dacă finalitățile la care trebuie să răspundă asemenea măsuri se pliază în esență pe finalitățile urmărite de activitățile menționate la articolul 1 alineatul (3) din

Directiva 2002/58”¹⁸. Astfel, potrivit Curții, „articolul 15 alineatul (1) din directiva respectivă presupune în mod necesar că măsurile naționale prevăzute la acest articol intră în domeniul de aplicare al directivei menționate, din moment ce aceasta din urmă permite în mod expres statelor membre să le adopte numai cu respectarea condițiilor pe care le prevede. În plus, măsurile legislative vizate la articolul 15 alineatul (1) din Directiva 2002/58 guvernează, în scopurile menționate la această dispoziție, activitatea furnizorilor de servicii de comunicații electronice”¹⁹.

43. Curtea a concluzionat că „respectivul articol 15 alineatul (1) coroborat cu articolul 3 din Directiva 2002/58 trebuie interpretat în sensul că intră în domeniul de aplicare al acestei directive nu numai o măsură legislativă care impune furnizorilor de servicii de comunicații electronice să păstreze datele de transfer și datele de localizare, ci și o măsură legislativă privind accesul autorităților naționale la datele păstrate de acești furnizori”²⁰.

44. Astfel, potrivit Curții, „protecția confidențialității comunicațiilor electronice și a datelor de transfer aferente acestora, garantată de articolul 5 alineatul (1) din Directiva 2002/58, se aplică măsurilor adoptate de orice alte persoane decât utilizatorii, indiferent dacă este vorba despre persoane sau entități private ori despre entități statale. După cum se confirmă în considerentul (21) al directivei menționate, aceasta urmărește să evite «accesul» neautorizat la comunicații, inclusiv la «datel[e] referitoare la comunicații», pentru a proteja confidențialitatea comunicațiilor electronice”²¹.

45. La aceste argumente, Curtea a adăugat că „măsurile legislative care impun furnizorilor de servicii de comunicații electronice să păstreze date cu caracter personal sau să acorde autorităților naționale competente accesul la aceste date implică în mod necesar o prelucrare, de către acești furnizori, a datelor respective [...] Astfel de măsuri, întrucât guvernează activitățile furnizorilor menționați, nu pot fi asimilate, așadar, unor activități proprii statelor, vizate la articolul 1 alineatul (3) din Directiva 2002/58”²².

46. Astfel cum Curtea a statuat în Hotărârea Ministerio Fiscal²³, trebuie să se deducă din ansamblul acestor argumente că o cerere de acces la date cu caracter personal păstrate de furnizori de servicii de comunicații electronice, formulată în cadrul unei proceduri de urmărire penală, intră în domeniul de aplicare al Directivei 2002/58.

47. Pe de altă parte, guvernele maghiar și polonez invocă argumentul potrivit căruia dreptul Uniunii nu reglementează problema admisibilității probelor în procedurile penale.

48. Deși este adevărat că acest drept nu reglementează, în stadiul actual al evoluției sale, normele referitoare la admisibilitatea probelor într-o procedură penală, instanța de trimitere a subliniat totuși în mod clar de ce interpretarea dreptului Uniunii pe care o solicită este necesară pentru ca aceasta să se poată pronunța cu privire la admisibilitatea probelor. Într-adevăr, aceasta depinde de respectarea condițiilor și a normelor de procedură care reglementează colectarea acestor probe. Astfel, în cadrul aprecierii admisibilității ca probe a proceselor-verbale în discuție în litigiul principal, instanța de trimitere trebuie să examineze în prealabil în ce măsură colectarea datelor de la întreprinderea de telecomunicații, pe care sunt întemeiate aceste procese-verbale, era conformă cu articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă. Or, această chestiune prealabilă privește un aspect care, astfel cum am subliniat

18 Hotărârea Ministerio Fiscal (punctul 34 și jurisprudența citată).

19 *Idem*.

20 Hotărârea Ministerio Fiscal (punctul 35 și jurisprudența citată).

21 Hotărârea Ministerio Fiscal (punctul 36 și jurisprudența citată).

22 Hotărârea Ministerio Fiscal (punctul 37 și jurisprudența citată).

23 A se vedea Hotărârea Ministerio Fiscal (punctele 38 și 39).

anterior, este reglementat de dreptul Uniunii. Prin urmare, cu privire la acest aspect, normele naționale aplicabile în materia administrării probelor trebuie să respecte cerințele care decurg din drepturile fundamentale garantate de dreptul Uniunii²⁴. În aceste condiții, argumentul invocat de guvernele maghiar și polonez este, în opinia noastră, lipsit de relevanță.

2. Cu privire la păstrarea datelor de transfer și a datelor de localizare

49. Chiar dacă întrebările adresate de instanța de trimitere privesc condițiile de acces la date, Comisia solicită Curții să se pronunțe, în cadrul prezentei trimiteri preliminare, și cu privire la problematica referitoare la păstrarea datelor. În această privință, ea observă în esență că un acces legal la datele păstrate necesită ca reglementarea națională care impune furnizorilor de servicii de comunicații electronice păstrarea datelor generate în cadrul acestor servicii să îndeplinească cerințele prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina cartei, sau ca datele în cauză să fi fost păstrate de acești furnizori din propria lor inițiativă, în special în scopuri comerciale, în conformitate cu aceeași directivă.

50. În ceea ce privește cauza principală, Comisia observă că datele la care autoritatea de investigare a avut acces nu au fost păstrate de furnizorii de servicii de comunicații electronice din propria lor inițiativă în scopuri comerciale, ci în temeiul obligației de păstrare pe care le-o impune articolul 111¹ din Legea privind comunicațiile electronice. Ea arată de asemenea că H. K. contestă legalitatea normelor naționale referitoare atât la accesul la date, cât și la păstrarea lor²⁵.

51. În aceste condiții, arătăm că, astfel cum s-a întâmplat în cadrul trimiterii preliminare care a condus la pronunțarea Hotărârii Ministerio Fiscal²⁶, întrebările formulate de instanța de trimitere în cadrul prezentei cauze nu urmăresc să se determine dacă datele cu caracter personal în discuție în litigiul principal au fost păstrate de furnizorii de servicii de comunicații electronice cu respectarea condițiilor prevăzute la articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă. Aceste întrebări privesc numai compatibilitatea cu aceste dispoziții a condițiilor în care accesul autorităților naționale de investigare la asemenea date este autorizat în temeiul reglementării estoniene. Acesta este motivul pentru care dezbaterile care au fost inițiate în fața Curții a privit aproape exclusiv aceste condiții de acces.

52. În orice caz, instanța de trimitere se poate întemeia pe jurisprudența rezultată din Hotărârea Tele2 Sverige și Watson și alții dacă apreciază că este necesar, pentru a soluționa litigiul principal, să statueze cu privire la compatibilitatea cu dreptul Uniunii a articolului 111¹ din Legea privind comunicațiile electronice.

53. În această privință, ne vom limita la a aminti că, potrivit Curții, „articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică”²⁷.

²⁴ A se vedea în special, prin analogie, Hotărârea din 10 aprilie 2003, Steffensen (C-276/01, EU:C:2003:228, punctul 71). În această hotărâre, Curtea abordează de asemenea această problemă din perspectiva principiului efectivității ca limită a autonomiei procedurale a statelor membre (punctele 66-68 din hotărârea menționată).

²⁵ Comisia subliniază în acest context că prezenta cauză se distinge de cea în care s-a pronunțat Hotărârea Ministerio Fiscal.

²⁶ A se vedea Hotărârea Ministerio Fiscal (punctele 49 și 50).

²⁷ Hotărârea Tele2 Sverige și Watson și alții (punctul 112).

54. Revine instanței de trimitere sarcina de a verifica, dacă este cazul, dacă reglementarea estoniană impune furnizorilor de servicii de comunicații electronice o obligație de păstrare a datelor care prezintă un asemenea caracter generalizat și nediferențiat și de a trage concluziile în vederea soluționării litigiului principal. Dacă regimul de păstrare a datelor instituit de Republica Estonia ar fi considerat neconform cu dreptul Uniunii, întrucât este disproporționat în raport cu obiectivul urmărit, nici accesul la datele astfel păstrate nu ar putea fi justificat prin același obiectiv.

55. Numai în cazul în care această obligație de păstrare este însoțită de limitări adecvate, în special în ceea ce privește categoriile de date vizate și durata păstrării, potrivit unui regim diferențiat în funcție de obiectivul urmărit și strict necesar pentru atingerea acestui obiectiv, ea va putea trece testul de proporționalitate.

56. Nu vom dezvolta mai mult în cadrul prezentelor concluzii noțiunea de „păstrare limitată a datelor” care este examinată în detaliu de domnul avocat general Campos Sánchez-Bordona în Concluziile pe care le-a prezentat la 15 ianuarie 2020 în cadrul cauzei *Ordre des barreaux francophones et germanophone și alții*²⁸.

B. Cu privire la accesul autorităților naționale competente la datele păstrate

1. Învățămintele trase din Hotărârea Tele2 Sverige și Watson și alții

57. Curtea înțelege problematica referitoare la accesul autorităților naționale competente la datele păstrate „independent de întinderea obligației de păstrare a unor date care ar fi impusă furnizorilor de servicii de comunicații electronice” și în special independent de caracterul generalizat sau direcționat al unei păstrări a datelor²⁹. Această constatare este în legătură cu faptul că Curtea consideră păstrarea datelor și accesul la acestea ca două ingerințe distincte în drepturile fundamentale protejate de cartă.

58. Accesul la datele păstrate „trebuie să urmărească în mod efectiv și strict unul dintre [...] obiective[le]” care figurează la articolul 15 alineatul (1) prima teză din Directiva 2002/58. De asemenea, trebuie să existe o concordanță între gravitatea ingerinței și obiectivul urmărit. Dacă ingerința este calificată drept „gravă”, ea poate fi justificată numai de combaterea infracționalității grave³⁰.

59. Precum în cazul păstrării datelor, accesul autorităților naționale competente la acestea poate fi autorizat numai în limitele strictului necesar³¹. În plus, măsurile legislative trebuie „să prevadă norme clare și precise care să indice în ce împrejurări și în ce condiții furnizorii de servicii de comunicații electronice trebuie să acorde autorităților naționale competente accesul la date. De asemenea, o măsură de această natură trebuie să fie obligatorie din punct de vedere juridic în dreptul intern”³². Mai precis, reglementările naționale trebuie „să prevadă și condițiile materiale și procedurale care guvernează accesul autorităților naționale competente la datele păstrate”³³.

60. Din cele ce precedă se poate deduce că „un acces general la toate datele păstrate, independent de orice legătură, chiar indirectă, cu scopul urmărit, nu poate fi considerat limitat la strictul necesar”³⁴.

28 C-520/18, EU:C:2020:7. A se vedea în special punctele 72-107 din aceste concluzii.

29 A se vedea Hotărârea Tele2 Sverige și Watson și alții (punctul 113).

30 A se vedea Hotărârea Tele2 Sverige și Watson și alții (punctul 115).

31 A se vedea Hotărârea Tele2 Sverige și Watson și alții (punctul 116).

32 Hotărârea Tele2 Sverige și Watson și alții (punctul 117).

33 Hotărârea Tele2 Sverige și Watson și alții (punctul 118).

34 Hotărârea Tele2 Sverige și Watson și alții (punctul 119).

61. Potrivit Curții, „reglementarea națională în cauză trebuie să se întemeieze pe criterii obiective pentru a defini împrejurările și condițiile în care trebuie să se acorde autorităților naționale competente accesul la datele abonaților sau ale utilizatorilor înregistrați. În această privință, accesul nu poate fi acordat, în principiu, în raport cu obiectivul de combatere a infracționalității, decât la datele persoanelor bănuite că ar pregăti, că ar săvârși sau că ar fi săvârșit o infracțiune gravă ori că ar fi implicate în orice mod într-o astfel de infracțiune”³⁵.

62. Cu alte cuvinte, reglementarea națională care acordă autorităților naționale competente accesul la datele păstrate trebuie să aibă un domeniu de aplicare suficient de delimitat pentru a împiedica faptul ca un astfel de acces să poată privi un număr important de persoane sau chiar toate persoanele și toate mijloacele de comunicare electronică, precum și ansamblul datelor păstrate. În consecință, Curtea a evidențiat criteriul legăturii între persoanele vizate și obiectivul urmărit.

63. Pe de altă parte, Curtea a stabilit condițiile pe care trebuie să le îndeplinească orice acces al autorităților naționale competente la datele păstrate.

64. Mai întâi, acest acces trebuie, „în principiu, cu excepția unor situații de urgență justificate corespunzător, [să fie] condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă”³⁶. Decizia acestei instanțe sau a acestei entități trebuie 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”³⁷.

65. În continuare, se impune, potrivit Curții, ca „autoritățile naționale competente cărora le-a fost acordat accesul la datele păstrate să informeze persoanele în cauză, în cadrul procedurilor naționale aplicabile, din momentul în care această comunicare nu poate compromite anchetele desfășurate de autoritățile respective”³⁸.

66. În sfârșit, statele membre trebuie să adopte norme referitoare la securitatea și la protecția datelor păstrate de furnizorii de servicii de comunicații electronice pentru a se evita abuzurile, precum și orice acces ilicit la date”³⁹.

2. Învățămintele trase din Hotărârea Ministerio Fiscal

67. În această cauză, Curtea a fost sesizată cu problema compatibilității cu articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7 și 8 din cartă, a unei reglementări naționale care prevede accesul autorităților naționale competente, precum poliția judiciară, la date referitoare la identitatea civilă a titularilor anumitor cartele SIM.

68. În hotărârea sa, Curtea a arătat că, în ceea ce privește obiectivul prevenirii, cercetării, detectării și urmăririi penale a infracțiunilor, textul articolului 15 alineatul (1) prima teză din Directiva 2002/58 nu limitează acest obiectiv numai la combaterea infracțiunilor grave, ci se referă la „infracțiuni” în general⁴⁰.

69. Raționamentul dezvoltat de Curte clarifică faptul că, în ceea ce privește accesul autorităților naționale competente la date, trebuie să existe o corespondență între gravitatea ingerinței și gravitatea infracțiunilor în cauză.

³⁵ *Idem*.

³⁶ Hotărârea Tele2 Sverige și Watson și alții (punctul 120).

³⁷ *Idem*.

³⁸ Hotărârea Tele2 Sverige și Watson și alții (punctul 121).

³⁹ A se vedea Hotărârea Tele2 Sverige și Watson și alții (punctul 122).

⁴⁰ A se vedea Hotărârea Ministerio Fiscal (punctul 53).

70. Astfel, Curtea amintește, făcând trimitere la punctul 99 din Hotărârea Tele2 Sverige și Watson și alții, că a statuat desigur că, „în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, numai combaterea infracționalității grave este susceptibilă să justifice un acces al autorităților publice la date cu caracter personal păstrate de furnizorii de servicii de comunicații electronice care, considerate în ansamblu, permit deducerea unor concluzii precise privind viața privată a persoanelor ale căror date sunt vizate”⁴¹.

71. Totuși, Curtea precizează că a „motivată [...] această interpretare prin faptul că obiectivul urmărit de o reglementare care guvernează acest acces trebuie să se raporteze la gravitatea ingerinței în drepturile fundamentale în cauză pe care o determină această operațiune”⁴².

72. Astfel, „în conformitate cu principiul proporționalității, o ingerință gravă nu poate fi justificată, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, decât prin obiectivul privind combaterea infracționalității care trebuie calificată drept «gravă»”⁴³.

73. În schimb, „dacă ingerința pe care o implică un asemenea acces nu este gravă, respectivul acces este susceptibil să fie justificat de un obiectiv privind prevenirea, investigarea, detectarea și urmărirea penală a unor «infracțiuni» în general”⁴⁴.

74. Prin urmare, aceste considerații necesitau o apreciere a aspectului dacă, având în vedere circumstanțele cauzei, ingerința în drepturile fundamentale consacrate la articolele 7 și 8 din cartă pe care ar determina-o un acces al poliției judiciare la datele în discuție în litigiul principal trebuia sau nu trebuia considerată „gravă”.

75. Or, spre deosebire de situația din Hotărârea Tele2 Sverige și Watson și alții, ingerința în drepturile protejate la articolele 7 și 8 din cartă, constituită din accesul la datele în cauză, nu a fost calificată de Curte drept „gravă”⁴⁵. Astfel, cererea de acces avea „drept unic obiect să identifice titularii cartelelor SIM activate, într-o perioadă de douăsprezece zile, cu codul [referitor la identificatorul internațional al echipamentului mobil] al telefonului mobil furat”⁴⁶. Era vorba despre accesul „numai [...] la numerele de telefon corespunzătoare acestor cartele SIM, precum și la datele referitoare la identitatea civilă a titularilor cartelelor menționate, cum ar fi numele, prenumele și, dacă este cazul, adresa lor. În schimb, aceste date nu [priveau] [...] comunicațiile efectuate cu telefonul mobil furat și nici localizarea acestuia”⁴⁷.

76. Curtea a dedus că „datele vizate de cererea de acces în discuție în litigiul principal permit doar să se pună în legătură, pe o perioadă determinată, cartela sau cartelele SIM activate cu telefonul mobil furat cu identitatea civilă a titularilor acestor cartele SIM. Fără o verificare încrucișată a datelor aferente comunicațiilor efectuate cu respectivele cartele SIM și a datelor de localizare, aceste date nu permit să se cunoască nici data, ora, durata și destinatarul comunicațiilor efectuate cu cartela sau cu cartelele SIM în cauză, nici locurile în care aceste comunicații au avut loc sau frecvența acestora cu anumite persoane într-o perioadă determinată. Prin urmare, aceste date nu permit să se tragă concluzii precise cu privire la viața privată a persoanelor ale căror date sunt vizate”⁴⁸.

41 Hotărârea Ministerio Fiscal (punctul 54).

42 Hotărârea Ministerio Fiscal (punctul 55).

43 Hotărârea Ministerio Fiscal (punctul 56).

44 Hotărârea Ministerio Fiscal (punctul 57).

45 Hotărârea Ministerio Fiscal (punctul 61).

46 Hotărârea Ministerio Fiscal (punctul 59).

47 *Idem*.

48 Hotărârea Ministerio Fiscal (punctul 60).

77. Odată respinsă calificarea drept „ingerință gravă”, Curtea a putut considera că obiectivul privind prevenirea, detectarea, investigarea și urmărirea penală a unor infracțiuni în general, chiar dacă nu sunt grave, putea fi invocat pentru a justifica ingerința în cauză⁴⁹.

78. Tocmai având în vedere această jurisprudență, instanța de trimitere adresează prima și a doua întrebare preliminară, în scopul de a aprecia gravitatea ingerinței pe care o constituie accesul la date în cadrul procedurii penale în discuție în litigiul principal. Mai precis, ea urmărește să afle dacă categoriile de date vizate, precum și durata perioadei pentru care se solicită accesul la aceste date constituie, din această perspectivă, criterii relevante.

3. Cu privire la criteriile care permit să se evalueze gravitatea ingerinței

79. Astfel cum reiese din jurisprudența Curții, cu cât sunt mai numeroase categoriile de date la care este solicitat accesul, cu atât mai mult ingerința poate fi calificată drept „gravă”.

80. În aceste condiții, prima și a doua întrebare pe care le adresează instanța de trimitere vor determina Curtea să precizeze dacă, pe lângă categoriile de date în cauză, întinderea perioadei vizate de acest acces are de asemenea un rol în determinarea gravității ingerinței.

81. În opinia noastră, răspunsul ar trebui să fie afirmativ. Arătăm de altfel că, în Hotărârea Ministerio Fiscal, Curtea a ținut seama de asemenea de durata perioadei vizate de acces în cadrul aprecierii sale, și anume douăsprezece zile în speță⁵⁰.

82. Combinația dintre natura datelor vizate și durata perioadei la care se referă accesul este cea care permite să se aprecieze gravitatea ingerinței. Astfel, aceste două aspecte permit să se verifice dacă este îndeplinit criteriul determinant al gravității ingerinței, și anume dacă accesul la datele în cauză poate permite autorităților naționale competente deducerea unor concluzii precise privind viața privată a persoanelor ale căror date sunt vizate de acest acces. Or, pentru a putea schița portretul precis al unei persoane, este necesar nu numai ca accesul să vizeze mai multe categorii de date, precum datele de identificare, datele de transfer și datele de localizare, ci și ca acest acces să privească o perioadă suficient de lungă pentru a putea dezvălui cu suficientă precizie caracteristicile principale ale vieții unei persoane.

83. Prin urmare, ca și numărul de categorii vizate, durata perioadei pentru care sunt solicitate date în conformitate cu autorizația de acces constituie un element esențial în vederea aprecierii gravității ingerinței în drepturile fundamentale ale persoanelor în cauză. După cum arată Comisia, cumulul mai multor cereri de acces referitoare la una și aceeași persoană trebuie de asemenea să fie luat în considerare, chiar dacă acestea privesc perioade scurte.

84. Astfel cum reiese din cererea de decizie preliminară, datele la care a avut acces autoritatea de investigare sunt cele care sunt menționate la articolul 111¹ alineatul (2) din Legea privind comunicațiile electronice. Aceste date permit urmărirea și identificarea sursei și a destinației unei sesiuni de comunicații telefonice pe baza telefonului fix sau mobil al unei persoane, determinarea datei, a orei, a duratei și a naturii acesteia, identificarea echipamentului terminal mobil utilizat, precum și localizarea echipamentului terminal mobil utilizat. Aceste date au fost transmise autorității de investigare pentru perioade de o zi, de o lună și de aproape un an.

49 Hotărârea Ministerio Fiscal (punctul 62).

50 A se vedea Hotărârea Ministerio Fiscal (punctul 59). A se vedea în același sens Concluziile avocatului general Saugmandsgaard Øe prezentate în cauza Ministerio Fiscal (C-207/16, EU:C:2018:300), care observă că cererea autorităților polițienești privea „o perioadă clar definită și limitată în timp, și anume aproximativ douăsprezece zile” (punctul 33, precum și punctul 84).

85. Aprecierea gradului de ingerință în drepturile fundamentale pe care îl implică accesul autorităților naționale competente la datele cu caracter personal păstrate rezultă dintr-o examinare concretă a circumstanțelor proprii fiecărei cauze. În fiecare situație, revine instanței de trimitere sarcina de a aprecia dacă datele la care a fost autorizat accesul erau de natură să permită, în funcție de natura lor și de durata perioadei vizate de acest acces, să se tragă concluzii precise cu privire la viața privată a persoanelor vizate.

86. Într-un asemenea caz, ingerința ar trebui calificată drept „gravă” în sensul jurisprudenței Curții și, prin urmare, nu ar putea fi justificată în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor decât prin obiectivul privind combaterea infracționalității, care trebuie calificată drept „gravă”⁵¹.

4. Cu privire la concordanța dintre gravitatea ingerinței și obiectivul urmărit

87. Rezultă din jurisprudența Curții că o ingerință în drepturile fundamentale care este calificată drept „gravă” implică o cerință de justificare sporită.

88. În ceea ce privește gravitatea infracțiunilor prezumate în legătură cu care a fost acordat accesul la date, Comisia evidențiază că reglementarea națională în discuție în litigiul principal autorizează în special accesul pentru combaterea infracțiunilor în general⁵².

89. Revine instanței de trimitere sarcina de a verifica, în funcție de împrejurările cauzei, dacă accesul la date precum cele în discuție în cauza principală urmărește în mod efectiv și strict unul dintre obiectivele prevăzute la articolul 15 alineatul (1) din Directiva 2002/58. În această privință, trebuie amintit că această dispoziție nu limitează obiectivul prevenirii, cercetării, detectării și urmăririi penale a infracțiunilor numai la combaterea infracțiunilor grave, ci se referă la „infracțiuni” în general⁵³.

90. Dacă instanța de trimitere ajunge la concluzia că ingerința trebuie calificată drept „gravă”, îi revine sarcina de a aprecia dacă infracțiunea în cauză poate fi de asemenea calificată drept „gravă” potrivit dreptului penal național.

91. În această privință, considerăm că definirea a ceea ce poate fi calificat drept „infracțiune gravă” trebuie să fie lăsată la aprecierea statelor membre.

92. 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.

93. Astfel cum arată în mod întemeiat guvernul estonian, pentru a determina gravitatea infracțiunilor, pedeapsa aplicabilă nu este singurul criteriu. Trebuie de asemenea să se ia în considerare natura infracțiunilor, prejudiciul pe care îl cauzează societății, atingerea pe care o aduc intereselor juridice și efectele globale pe care le au asupra ordinii juridice naționale, precum și asupra valorilor unei societăți democratice. Contextul istoric, economic și social specific fiecărui stat membru are de asemenea un rol în această privință. Pe de altă parte, referitor la circumstanțele agravante, trebuie să se ridice problema dacă infracțiunile au fost săvârșite, de exemplu, fie în mod repetat, fie față de un grup de persoane vulnerabile.

⁵¹ Hotărârea Ministerio Fiscal (punctul 56).

⁵² Articolul 111¹ alineatul (11) din Legea privind comunicațiile electronice și articolul 90¹ din Codul de procedură penală.

⁵³ A se vedea Hotărârea Ministerio Fiscal (punctul 53).

94. Pentru a evalua proporționalitatea accesului, trebuie să se țină seama și de faptul că, în conformitate cu articolul 90¹ alineatul (3) din Codul de procedură penală, „[d]atele pot fi solicitate numai dacă sunt absolut necesare pentru atingerea obiectivului procedurii penale”. Astfel cum arată guvernul estonian, criteriul necesității absolute⁵⁴ obligă atât persoanele care realizează investigația, cât și persoanele însărcinate cu eliberarea autorizației să ia în considerare și să aprecieze ce date sunt necesare pentru finalizarea procedurii penale și fără de care nu ar fi posibilă, în cadrul unei anumite cauze, descoperirea adevărului sau arestarea unui presupus infractor.

95. Adăugăm că, astfel cum a subliniat în mod întemeiat guvernul francez, gradul de gravitate a unei infracțiuni sau chiar calificarea juridică exactă a acesteia nu pot fi determinate întotdeauna în mod precis atunci când autorizația de acces la date păstrate intervine într-un stadiu precoce al investigației, astfel încât ar putea părea prematur în acest stadiu să se introducă această infracțiune în categoria infracțiunilor grave sau în cea a infracțiunilor în general. Această incertitudine, care este inerentă investigațiilor preliminare al căror obiect însuși este de a contribui la descoperirea adevărului, trebuie luată în considerare de instanța de trimitere în cadrul aprecierii sale referitoare la caracterul proporțional al accesului.

96. În aceste condiții, incertitudinea care poate exista astfel la începutul investigației preliminare cu privire la aceste aspecte nu poate elimina cerința potrivit căreia fiecare cerere de acces trebuie motivată prin necesitatea de a căuta probe referitoare la un comportament infracțional specific, pe baza unei bănuieli susținute de elemente obiective. Astfel, o cerere de acces nu poate avea drept scop examinarea, pe o anumită perioadă, a tuturor faptelor și gesturilor unei persoane în vederea investigării unor eventuale infracțiuni. Pe de altă parte, dacă se vor descoperi fapte noi în cursul investigației, accesul la date pentru a le dovedi pe acestea din urmă va trebui să facă obiectul unei noi autorizații de acces.

97. Ținând seama de dezvoltările care precedă, propunem Curții să declare că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că printre criteriile care permit să se evalueze gravitatea ingerinței în drepturile fundamentale pe care o constituie accesul autorităților naționale competente la date cu caracter personal pe care furnizorii de servicii de comunicații electronice sunt obligați să le păstreze în temeiul unei reglementări naționale figurează categoriile de date în cauză, precum și durata perioadei pentru care este solicitat acest acces. Revine instanței de trimitere sarcina de a aprecia, în funcție de gravitatea ingerinței, dacă accesul menționat era strict necesar pentru atingerea obiectivului de a asigura prevenirea, investigarea, detectarea și urmărirea penală a unor infracțiuni.

C. Controlul prealabil de către o instanță sau o autoritate administrativă independentă

98. În scopul de a garanta că accesul autorităților naționale competente la datele păstrate este limitat la ceea ce este strict necesar pentru atingerea obiectivului urmărit, Curtea a considerat că este esențial ca acest acces „să fie, în principiu, cu excepția unor situații de urgență justificate corespunzător, 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”⁵⁵.

⁵⁴ Calificat de asemenea drept „principiul *ultima ratio*”.

⁵⁵ Hotărârea Tele2 Sverige și Watson și alții (punctul 120 și jurisprudența citată), sublinierea noastră. A se vedea în același sens Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (EU:C:2017:592, punctele 202 și 208).

99. Prin intermediul celei de a treia întrebări preliminare, instanța de trimitere solicită Curții să precizeze criteriile pe care trebuie să le îndeplinească o autoritate administrativă pentru a putea fi considerată ca fiind „independentă”, în sensul Hotărârii Tele2 Sverige și Watson și alții. Mai precis, instanța de trimitere ridică problema dacă Ministerul Public poate fi considerat o autoritate administrativă independentă, ținând seama de faptul că el conduce procedura de cercetare și că susține acțiunea publică în cursul procesului.

100. Pentru a răspunde la această întrebare, apreciem că este util să se ia în considerare două componente ale jurisprudenței Curții, și anume, pe de o parte, jurisprudența referitoare la independența autorităților naționale de supraveghere a protecției datelor cu caracter personal și, pe de altă parte, jurisprudența referitoare la independența autorității judiciare emitente în cadrul mandatului european de arestare.

101. Potrivit Curții, independența constituie o caracteristică esențială, afirmată în special la articolul 8 alineatul (3) din cartă, a autorităților responsabile de supravegherea respectării normelor Uniunii referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, în scopul de a asigura eficiența și fiabilitatea acestei supravegheri și de a consolida protecția persoanelor vizate de deciziile acestor autorități⁵⁶.

102. Curtea a statuat deja, în legătură cu articolul 28 alineatul (1) al doilea paragraf din Directiva 95/46, că „autoritățile de supraveghere competente pentru supravegherea prelucrării datelor cu caracter personal trebuie să beneficieze de o independență care să le permită să își exercite atribuțiile fără a fi supuse unei influențe exterioare. Această independență exclude printre altele orice ingerință și orice altă influență exterioară, sub orice formă, fie directă, fie indirectă, care ar fi susceptibile să le orienteze deciziile și care, astfel, ar putea să pună în discuție îndeplinirea de către autoritățile menționate a sarcinii lor care constă în stabilirea unui echilibru just între protecția dreptului la viață privată și libera circulație a datelor cu caracter personal”⁵⁷.

103. Curtea a pus accentul de asemenea pe cerința potrivit căreia, ținând seama de rolul lor de gardian al dreptului la viață privată, aceste autorități de supraveghere trebuie să fie „mai presus de orice suspiciune de părtinire”⁵⁸.

104. În măsura în care a treia întrebare adresată de instanța de trimitere privește Ministerul Public, este relevant de asemenea să se țină seama de criteriile formulate de Curte în jurisprudența sa referitoare la independența autorității judiciare emitente în cadrul mandatului european de arestare. Astfel, potrivit Curții, controlul efectuat cu ocazia adoptării unui mandat european de arestare „trebuie să fie exercitat în mod obiectiv, ținând seama de toate elementele incriminatoare și dezincriminatoare, precum și în mod independent, ceea ce presupune existența unor norme statutare și organizatorice în măsură să excludă orice risc ca adoptarea unei decizii de emiterie a unui astfel de mandat de arestare să fie supusă unor instrucțiuni exterioare, printre altele din partea puterii executive”⁵⁹. Trebuie totuși să se țină seama că aprecierea concretă a Curții, în fiecare caz, a chestiunii dacă Ministerul Public îndeplinește sau nu aceste criterii⁶⁰ este efectuată în cadrul specific al emiterii unui mandat european de arestare și, așadar, nu poate fi transpusă în mod automat în alte domenii precum cel referitor la protecția datelor cu caracter personal.

56 A se vedea în special Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650, punctele 40 și 41, precum și jurisprudența citată). A se vedea de asemenea Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (EU:C:2017:592, punctul 229).

57 Hotărârea din 8 aprilie 2014, Comisia/Ungaria (C-288/12, EU:C:2014:237, punctul 51 și jurisprudența citată).

58 Hotărârea din 8 aprilie 2014, Comisia/Ungaria (C-288/12, EU:C:2014:237, punctul 53 și jurisprudența citată).

59 A se vedea Hotărârea din 9 octombrie 2019, NJ (Parchetul din Viena) (C-489/19 PPU, EU:C:2019:849, punctul 38 și jurisprudența citată).

60 A se vedea în ultimul rând Hotărârea din 12 decembrie 2019, JR și YC (Procurorii din Lyon și din Tours și Procurorii din Lyon și din Tours) (C-566/19 PPU și C-626/19 PPU, EU:C:2019:1077), în care Curtea a considerat printre altele că elementele care i-au fost prezentate erau suficiente pentru a se demonstra că, „în Franța, magistrații din cadrul parchetului dispun de puterea de a aprecia în mod independent, în special în raport cu puterea executivă, necesitatea și proporționalitatea emiterii unui mandat european de arestare și exercită această putere în mod obiectiv, luând în considerare toate elementele incriminatoare și dezincriminatoare” (punctul 55 din această hotărâre).

105. Fiind făcute aceste precizări, cele două componente ale jurisprudenței Curții se alătură, subliniind, în fiecare dintre domeniile vizate, că autoritatea națională competentă să verifice respectarea normelor dreptului Uniunii trebuie să aibă un caracter independent, ceea ce include două cerințe⁶¹. Pe de o parte, această autoritate nu trebuie să fie supusă unor instrucțiuni sau unor presiuni externe care îi pot influența deciziile. Pe de altă parte, autoritatea menționată trebuie, în temeiul statutului său și al misiunilor care îi sunt conferite, să îndeplinească o cerință de obiectivitate în cadrul controlului pe care îl realizează, și anume ea trebuie să ofere garanții de imparțialitate. Mai precis, aprecierea de către o autoritate administrativă a caracterului proporțional al accesului la datele păstrate necesită ca aceasta să fie în măsură să efectueze un just echilibru între interesele legate de eficacitatea investigației în cadrul combaterii infracționalității și cele care privesc protecția datelor cu caracter personal a persoanelor vizate de acces. În consecință, sub acest din urmă aspect, cerința de imparțialitate este inerentă noțiunii de „autoritate administrativă independentă” evidențiată de Curte în Hotărârea Tele2 Sverige și Watson și alții.

106. Trebuie să se verifice dacă Ministerul Public, ținând seama de diferitele misiuni care îi sunt atribuite de reglementarea estoniană, îndeplinește acest criteriu de independență, în cele două dimensiuni ale acestuia, atunci când trebuie să controleze caracterul strict necesar al accesului la date. Astfel, noțiunea de „independență” care trebuie să caracterizeze autoritatea administrativă însărcinată cu un asemenea control are o dimensiune funcțională, în sensul că tocmai în raport cu obiectul specific al acestui control trebuie să se aprecieze dacă această autoritate este în măsură să acționeze fără intervenții și fără presiuni externe care îi pot influența deciziile, precum și cu respectarea obiectivității și a strictei aplicări a normei de drept. În concluzie, noțiunea de „autoritate administrativă independentă” în sensul Hotărârii Tele2 Sverige și Watson și alții este destinată să garanteze obiectivitatea, fiabilitatea și eficiența acestui control.

107. Acest lucru presupune să se examineze dacă reglementarea estoniană care precizează statutul și misiunile Ministerului Public este de natură să creeze îndoieli legitime, în percepția persoanelor în cauză, cu privire la impermeabilitatea procurorilor în ceea ce privește elementele externe și cu privire la neutralitatea lor în raport cu interesele care se confruntă, atunci când trebuie să asigure controlul prealabil al caracterului proporțional al accesului la date.

108. Ministerul Public joacă un rol esențial în desfășurarea procedurii penale, întrucât conduce procedura de cercetare și are competența printre altele să efectueze urmărirea penală împotriva unei persoane bănuite de săvârșirea unei infracțiuni în vederea aducerii acesteia în fața unei instanțe judecătorești. În această măsură, el trebuie considerat ca fiind o autoritate care participă la administrarea justiției penale⁶².

109. Astfel cum Curtea a arătat în legătură cu Procura della Repubblica (procurorul Republicii, Italia) și potrivit unei formulări care, în opinia noastră, poate fi transpusă în cadrul prezentei cauze, „funcția îndeplinită de [procuror] nu este de a soluționa cu independență totală un litigiu, ci de a-l supune, la rândul său, atenției instanței competente, ca parte la procedură ce exercită acțiunea penală”⁶³.

110. Astfel, deși Ministerul Public prezintă, în statutul său, în organizarea sa și în misiunile sale, trăsăturile specifice care îl disting de o instanță și care justifică calificarea sa drept „autoritate care participă la administrarea justiției penale în statele membre”, totuși, din punct de vedere funcțional, în cazul în care dreptul național prevede că autoritatea care exercită controlul prealabil al proporționalității accesului care este impus prin Hotărârea Tele2 Sverige și Watson și alții este

61 Cu privire la cele două aspecte ale cerinței de independență, a se vedea prin analogie, în legătură cu instanțele naționale care sunt chemate să statueze asupra unor chestiuni referitoare la interpretarea și la aplicarea dreptului Uniunii, Hotărârea din 5 noiembrie 2019, Comisia/Polonia (Independența instanțelor de drept comun) (C-192/18, EU:C:2019:924, punctele 108-110, precum și jurisprudența citată).

62 A se vedea în special Hotărârea din 27 mai 2019, PF (Procurorul general al Lituaniei) (C-509/18, EU:C:2019:457, punctele 39 și 40).

63 Hotărârea din 12 decembrie 1996, X (C-74/95 și C-129/95, EU:C:1996:491, punctul 19).

Ministerul Public, acesta din urmă trebuie, cu privire la acest aspect, să manifeste un grad de independență analog celui al unei instanțe. Astfel, exercitarea acestei funcții mai degrabă de o autoritate administrativă decât de o instanță nu trebuie să afecteze obiectivitatea, fiabilitatea și eficiența acestui control.

111. În această privință, trebuie amintit că, în conformitate cu articolul 90¹ alineatul (2) din Codul de procedură penală, autoritatea de investigare poate, în procedura de cercetare, cu autorizarea dată de Ministerul Public, sau în procedura judiciară, cu autorizarea dată de instanță, să solicite unei întreprinderi de comunicații electronice datele prevăzute la articolul 111¹ alineatele (2) și (3) din Legea privind comunicațiile electronice.

112. Pe de altă parte, din reglementarea estoniană reiese că Ministerul Public, în cadrul unei proceduri penale, conduce procedura de cercetare, al cărei obiectiv este colectarea elementelor de probă și crearea altor condiții necesare desfășurării unui proces. În plus, în cursul procedurii de cercetare, autoritatea de investigare și Ministerul Public examinează elementele incriminatoare sau dezincriminatoare colectate în privința suspectului sau a inculpatului. Dacă Ministerul Public este convins că au fost colectate toate probele necesare și dacă este cazul, acesta prezintă acuzațiile împotriva persoanei și, în acest caz, el este cel care susține acțiunea publică în cadrul procesului.

113. Instanța de trimitere observă de asemenea că, chiar dacă, în cadrul procedurii penale, Ministerul Public trebuie, pentru măsurile care constituie ingerințele cele mai grave în drepturile fundamentale, să solicite o autorizație de la un judecător de instrucție (de exemplu pentru majoritatea măsurilor de supraveghere și pentru detenție), Ministerul Public are de asemenea competența de a decide adoptarea unor acte de procedură care constituie o ingerință intensă în mai multe drepturi fundamentale⁶⁴.

114. Îndoilele exprimate de instanța de trimitere pentru a califica Ministerul Public drept „autoritate administrativă independentă” în sensul Hotărârii Tele2 Sverige și Watson și alții sunt datorate în principal faptului că, după procedura de cercetare, dacă Ministerul Public este convins că în cauza penală au fost colectate toate probele necesare și dacă este cazul, acestuia îi revine sarcina de a prezenta acuzațiile împotriva persoanei în cauză. În acest caz, Ministerul Public este cel care susține acțiunea publică în cadrul procesului și, prin urmare, este de asemenea participant la procedură. Astfel, în principal, din cauza calității sale de organ de urmărire penală, calificarea Ministerului Public drept „autoritate administrativă independentă” în sensul Hotărârii Tele2 Sverige și Watson și alții este pusă la îndoială de instanța de trimitere.

115. Prin urmare, formulate astfel, îndoilele exprimate de instanța de trimitere privesc mai precis imparțialitatea Ministerului Public în cadrul controlului proporționalității accesului la date al serviciilor de investigare pe care trebuie să îl efectueze înainte de a autoriza un asemenea acces.

116. Înainte de a aborda acest aspect referitor la imparțialitate, arătăm că articolul 1 alineatul 1¹ din Legea privind Ministerul Public prevede că acesta din urmă „îndeplinește misiunile care îi revin potrivit legii în mod independent”. În plus, în temeiul articolului 2 alineatul (2) din lege, „[p]rocurorul își îndeplinește misiunile în mod independent și își desfășoară activitatea numai în conformitate cu legea și cu propria convingere”⁶⁵.

117. În această privință, guvernul estonian arată că, deși Ministerul Public este o autoritate care ține de Ministerul Justiției, reglementarea estoniană îi refuză totuși acestuia din urmă orice posibilitate de a formula o apreciere cu privire la o procedură specifică sau de a interveni într-o procedură penală în curs. Acest guvern precizează că nerespectarea independenței Ministerului Public ar constitui o încălcare pasibilă de sancțiune.

⁶⁴ De exemplu, Ministerul Public dă o autorizație în vederea unei supravegheri discrete a unei persoane, a unui lucru sau a unui loc, precum și, în numeroase cazuri, în vederea unei percheziții.

⁶⁵ A se vedea de asemenea în același sens articolul 30 alineatul (2) din Codul de procedură penală.

118. În consecință, deși nu trebuie să existe îndoieli privind independența Ministerului Public în cadrul misiunilor care îi revin în temeiul reglementării estoniene, considerăm că aceasta este totuși de natură să suscite îndoieli legitime în ceea ce privește aptitudinea Ministerului Public de a exercita un control prealabil neutru și obiectiv cu privire la caracterul proporțional al accesului la date în cazul în care, în cadrul unei anumite cauze, trebuie să exercite în același timp misiuni care constau în a conduce investigația preliminară, a decide urmărirea penală sau a susține acțiunea publică în cursul procesului.

119. Este adevărat că mai multe elemente care figurează în reglementarea estoniană constituie garanții că Ministerul Public acționează, în cadrul misiunilor asumate, cu respectarea cerinței de imparțialitate.

120. Astfel, în temeiul articolului 211 alineatul (2) din Codul de procedură penală, Ministerul Public este obligat să examineze elementele incriminatoare și dezincriminatoare colectate în privința suspectului sau a inculpatului.

121. Pe de altă parte, astfel cum reiese din articolul 1 alineatul (1) din Legea privind Ministerul Public, acesta din urmă este obligat să asigure legalitatea procedurii de cercetare penală în privința căreia are misiunea de a o conduce. În plus, în conformitate cu articolul 1 alineatul (1¹) și cu articolul 2 alineatul (2) din aceeași lege, Ministerul Public trebuie să își exercite misiunile cu respectarea legilor. Acest lucru presupune că, atunci când conduce procedura de cercetare penală, Ministerul Public trebuie nu numai să aibă ca obiectiv asigurarea eficacității acesteia din urmă, ci și să garanteze că această procedură nu se desfășoară aducând o atingere disproporționată dreptului la viață privată al persoanelor în cauză. Astfel, se poate considera că autorizarea accesului la datele păstrate face parte integrantă din misiunea mai generală a Ministerului Public, care constă în a controla legalitatea mijloacelor puse în aplicare de serviciile de investigare, în special proporționalitatea actelor de investigare în raport cu natura și cu gravitatea faptelor.

122. În consecință, argumentul ar putea fi formulat în sensul că tocmai pentru că el conduce procedura de cercetare, Ministerul Public trebuie să evalueze dacă, în raport cu specificitatea fiecărei cauze, un acces la date păstrate de operatorii de telecomunicații este strict necesar, în lipsa unor elemente de probă alternative, pentru ca investigația cu privire la o presupusă infracțiune să avanseze.

123. Nu este mai puțin adevărat că, din punctul de vedere al persoanelor vizate de cererea de acces la date, împrejurarea că autoritatea administrativă care trebuie să verifice dacă acest acces este strict necesar în cadrul investigației este în același timp cea care este susceptibilă să le urmărească și să susțină acțiunea publică în cadrul unui eventual proces ulterior poate, în opinia noastră, să fie de natură să slăbească garanțiile de imparțialitate prevăzute de reglementarea estoniană. Din acest punct de vedere, poate exista un conflict potențial între aceste misiuni ale Ministerului Public, pe de o parte, și cerința de neutralitate și de obiectivitate a controlului prealabil al caracterului proporțional al accesului la date, pe de altă parte.

124. Astfel, în cadrul misiunilor sale, Ministerul Public este obligat să colecteze probe, să aprecieze relevanța acestora și să tragă concluziile cu privire la vinovăția persoanei în cauză. Revine acestei autorități a statului sarcina de a prezenta și de a susține dosarul acuzării în cadrul acțiunii publice pe care este însărcinată să o susțină în cadrul procesului, fiind, prin urmare, participant la procedură. Ca urmare a acestor misiuni, Ministerul Public este supus unei cerințe probatorii care poate părea, în opinia persoanelor suspectate de săvârșirea unei infracțiuni, ca fiind incompatibilă cu aptitudinea aceleiași autorități de a efectua, în mod neutru și obiectiv, un control prealabil al caracterului proporțional al accesului la date.

125. Astfel cum arată Comisia, ar putea exista riscul ca, din cauza cumulului de misiuni care îi revin, Ministerul Public să poată fi perceput de persoanele în cauză ca având un interes să acorde un acces larg la datele lor, indiferent dacă sunt incriminatoare sau dezincriminatoare. În plus, persoanele suspectate de săvârșirea unei infracțiuni pot avea îndoieli legitime cu privire la imparțialitatea Ministerului Public atunci când autorizează accesul la datele lor, din moment ce acesta poate acționa

împotriva lor în procedura ulterioară în calitate de organ de urmărire penală. Or, apreciem că cerința de imparțialitate a autorității administrative care este însărcinată să efectueze controlul prealabil impus prin Hotărârea Tele2 Sverige și Watson și alții presupune o anumită distanță și o neutralitate în raport cu interesele care se pot confrunța în cadrul procedurii de cercetare, și anume, pe de o parte, eficacitatea acesteia din urmă și, pe de altă parte, protecția datelor cu caracter personal ale persoanelor în cauză. Potrivit Comisiei, situația ar putea fi diferită dacă organizarea administrativă internă a Ministerului Public ar fi de asemenea natură încât procurorul care trebuie să se pronunțe cu privire la cererea de acces nu ar avea niciun rol în procedura de cercetare și nici în etapele ulterioare ale procedurii, inclusiv acțiunea publică.

126. În măsura în care, astfel cum s-a confirmat în ședință, în Republica Estonia parchetul este organizat în mod ierarhic, nu suntem siguri că această sugestie a Comisiei ar putea remedia inconvenientele născute din cumulul misiunilor pe care reglementarea estoniană le atribuie Ministerului Public. În orice caz, acest lucru nu lipsește de pertinență ideea care stă la baza acestei sugestii, și anume că controlul prealabil al caracterului proporțional al accesului la date ar trebui efectuat de o autoritate administrativă care, pe de o parte, nu este direct implicată în desfășurarea investigației penale în cauză și, pe de altă parte, are o poziție de neutralitate față de părțile din procedura penală. Unei astfel de autorități, detașate de interesele legate de investigație și de acțiunea publică în procedura în cauză, nu i s-ar putea reproșa că privilegiază interesele investigației în detrimentul celor referitoare la protecția datelor persoanelor în cauză. Astfel, autoritatea menționată ar fi în măsură să adopte, cu deplină imparțialitate, o decizie care limitează accesul la datele păstrate la ceea ce este strict necesar în vederea atingerii obiectivului urmărit, în conformitate cu cerințele impuse la articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost interpretat de Curte în Hotărârile din 8 aprilie 2014, Digital Rights Ireland și alții⁶⁶ și Tele2 Sverige și Watson și alții. În același timp, suntem conștienți de faptul că instituirea unei perspective externe intereselor legate de procedura în cauză nu trebuie să se facă cu prețul unei reduceri a eficacității investigării, urmăririi penale și reprimării infracțiunilor.

127. Pentru a respecta autonomia procedurală a statelor membre, Curtea nu ar trebui să intervină mai mult în organizarea generală a administrării justiției în statele membre și nici în organizarea internă a parchetelor. Revine statelor membre sarcina de a crea instrumente de natură să garanteze că controlul prealabil accesului la datele păstrate asigură un just echilibru între interesele legate de eficacitatea investigației penale și dreptul la protecția datelor al persoanelor vizate de acest acces.

128. Vom încheia precizând că, în opinia noastră, lipsa unui control prealabil efectuat de o autoritate administrativă „independentă” în sensul Hotărârii Tele2 Sverige și Watson și alții nu poate fi compensat de existența unui control jurisdicțional care poate fi efectuat după ce accesul a fost autorizat⁶⁷. În caz contrar, cerința caracterului prealabil al controlului și-ar pierde rațiunea de a fi, care constă în a împiedica autorizarea unui acces la datele păstrate care ar fi disproporționat în raport cu obiectivul care constă în investigarea, în urmărirea penală și în reprimarea infracțiunilor.

129. Având în vedere dezvoltările care precedă, propunem Curții să răspundă la a treia întrebare preliminară că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că cerința potrivit căreia accesul autorităților naționale competente la datele păstrate trebuie să fie supus unui control prealabil din partea unei instanțe sau a unei autorități administrative independente nu este îndeplinită atunci când reglementarea națională prevede că un asemenea control este efectuat de Ministerul Public, care are misiunea de a conduce procedura de cercetare, putând de asemenea să susțină acțiunea publică în cadrul procesului.

⁶⁶ C-293/12 și C-594/12, EU:C:2014:238.

⁶⁷ Potrivit elementelor care au fost furnizate Curții în ședință, în dreptul estonian, acest control jurisdicțional poate interveni la sfârșitul procedurii de cercetare, atunci când un suspect, căruia i s-a comunicat dosarul, decide să conteste un act din această procedură, sau în cadrul procesului.

V. Concluzie

130. În lumina considerațiilor de mai sus, propunem Curții să răspundă la întrebările adresate de Riigikohus (Curtea Supremă, Estonia) după cum urmează:

- „1) 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, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, trebuie interpretat în sensul că printre criteriile care permit să se evalueze gravitatea ingerinței în drepturile fundamentale pe care o constituie accesul autorităților naționale competente la date cu caracter personal pe care furnizorii de servicii de comunicații electronice sunt obligați să le păstreze în temeiul unei reglementări naționale figurează categoriile de date în cauză, precum și durata perioadei pentru care este solicitat acest acces. Revine instanței de trimitere sarcina de a aprecia, în funcție de gravitatea ingerinței, dacă accesul menționat era strict necesar pentru atingerea obiectivului de a asigura prevenirea, investigarea, detectarea și urmărirea penală a unor infracțiuni.
- 2) Articolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale, trebuie interpretat în sensul că cerința potrivit căreia accesul autorităților naționale competente la datele păstrate trebuie să fie supus unui control prealabil din partea unei instanțe sau a unei autorități administrative independente nu este îndeplinită atunci când reglementarea națională prevede că un asemenea control este efectuat de Ministerul Public, care are misiunea de a conduce procedura de cercetare, putând de asemenea să susțină acțiunea publică în cadrul procesului.”