Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
DOMNUL MANUEL CAMPOS SÁNCHEZ-BORDONA
prezentate la 30 martie 2023 [1]

Cauza C-162/22

A. G.
cu intervenția:
Lietuvos Respublikos generalinė prokuratūra

[cerere de decizie preliminară formulată de Lietuvos vyriausiasis administracinis teismas (Curtea Administrativă Supremă, Lituania)]

„Procedură preliminară – Telecomunicații – Prelucrarea datelor cu caracter personal – Directiva 2002/58/CE – Domeniu de aplicare – Articolul 15 alineatul (1) – Acces la datele stocate de furnizorii de servicii de comunicații electronice și colectate în cadrul urmăririi penale – Utilizare ulterioară a datelor cu ocazia unei cercetări privind un abuz în serviciu”

1. Prin prezenta trimitere preliminară se ridică în esență problema dacă anumite date cu caracter personal obținute în cursul unei cercetări penale pot fi utilizate ulterior în cadrul unei proceduri administrative disciplinare inițiate împotriva unui funcționar public.

2. Răspunsul la această întrebare oferă Curții o nouă ocazie să se pronunțe cu privire la domeniile de aplicare, pe de o parte, al Directivei 2002/58/CE [2] și, pe de altă parte, al Directivei (UE) 2016/680 [3] și al Regulamentului (UE) 2016/679 [4].

3. În ceea ce privește Directiva 2002/58, Curtea a elaborat o jurisprudență constantă cu privire la situațiile și la condițiile în care statele membre pot limita întinderea drepturilor și obligațiilor pe care le stabilește [5].

1 Limba originală: spaniola.

2 Directiva Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63).

3 Directiva Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO 2016, L 119, p. 89).

4 Regulamentul Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1, denumit în continuare „RGPD”).

5 Fără a fi exhaustive, printre principalele hotărâri de referință din această jurisprudență figurează Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238), Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții (C-203/15 și C-698/15, EU:C:2016:970), Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții (C-511/18, C-512/18 și C-520/18, EU:C:2020:791, denumită în continuare „Hotărârea La Quadrature du Net”), Hotărârea din 2 martie 2021, Prokuratuur (Condiții de acces la datele referitoare la comunicațiile electronice) (C-746/18, EU:C:2021:152), și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258, denumită în continuare „Hotărârea Commissioner of An Garda Síochána”).

I. Cadrul juridic

A. Dreptul Uniunii

1. Directiva 2002/58

4. Articolul 1 („Sfera de aplicare și scopul”) prevede:

„(1) Prezenta directivă armonizează dispozițiile statelor membre, lucru necesar în vederea asigurării unui nivel echivalent de protecție a drepturilor și libertăților fundamentale, mai ales a dreptului la confidențialitatea datelor personale, în domeniul prelucrării de date personale în sectorul comunicațiilor electronice și a liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Comunității.

(2) Prevederile prezentei directive precizează și completează Directiva 95/46/CE[6] în scopurile menționate la alineatul (1). Mai mult, acestea sunt menite a asigura protecția intereselor legitime ale abonaților persoane juridice.

(3) Prezenta directivă nu se aplică activităților care nu sunt cuprinse în domeniul de aplicare al [TFUE], 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.”

5. Articolul 5 („Confidențialitatea comunicațiilor”) alineatul (1) prevede:

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

6. Articolul 15 („Aplicarea anumitor dispoziții ale Directivei 95/46/CE”) prevede:

„(1) 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) din Directiva 95/46/CE. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest

[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).

alineat. Toate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale ale legislației comunitare, inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [TUE].

[…]

(2) Dispozițiile capitolului III cu privire la măsuri judiciare, responsabilitate și sancțiuni din Directiva 95/46/CE se aplică în privința dispozițiilor de drept intern adoptate în conformitate cu prezenta directivă și cu privire la drepturile individuale ce decurg din prezenta directivă.

[…]”

2. RGPD

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

„(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

(a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii

[…]

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

[…]”

8. Articolul 5 („Principii legate de prelucrarea datelor cu caracter personal”) prevede:

„(1) Datele cu caracter personal sunt:

[…]

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) («limitări legate de scop»);

[…]”

9. Articolul 6 („Legalitatea prelucrării”) prevede:

„(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

[…]

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

[…]

(3) Temeiul pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în:

(a) dreptul Uniunii sau

(b) dreptul intern care se aplică operatorului.

[…]

(4) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 23 alineatul (1), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

(a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;

(b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;

(c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu articolul 9, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu articolul 10;

(d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

[…]”

3. Directiva 2016/680

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

„Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii,

depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.”

11. Articolul 2 („Domeniul de aplicare”) alineatul (1) prevede:

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

12. Articolul 4 („Principii referitoare la prelucrarea datelor cu caracter personal”) prevede:

„(1) Statele membre garantează că datele cu caracter personal sunt:

[…]

(b) sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate într-un mod incompatibil cu aceste scopuri;

[…]

(2) Prelucrarea de către același operator sau de către un altul, în oricare dintre scopurile stabilite la articolul 1 alineatul (1), altele decât cele pentru care datele cu caracter personal au fost colectate, este permisă în măsura în care:

(a) operatorul este autorizat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu dreptul Uniunii sau cu dreptul intern și

(b) prelucrarea este necesară și proporțională în raport cu respectivul alt scop, în conformitate cu dreptul Uniunii sau cu dreptul intern.

[…]”

13. Articolul 9 („Condiții specifice de prelucrare”) alineatul (1) prevede:

„Datele cu caracter personal colectate de autoritățile competente în scopurile stabilite la articolul 1 alineatul (1) nu se prelucrează în alte scopuri decât cele stabilite la articolul 1 alineatul (1), cu excepția cazurilor în care o astfel de prelucrare este autorizată în temeiul dreptului Uniunii sau al dreptului intern. În cazurile în care datele cu caracter personal sunt prelucrate în alte scopuri, prelucrării respective i se aplică [RGPD], cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.”

B. Dreptul național

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. Articolul 65 alineatul 2 impune furnizorilor de servicii de comunicații electronice obligația de a stoca datele enumerate în anexa 1 la legea respectivă și, dacă este cazul, de a le pune la dispoziția autorităților competente pentru a fi utilizate în vederea combaterii infracționalității grave [8].

15. În conformitate cu articolul 77 alineatul 1, furnizorii de servicii de comunicații electronice trebuie să furnizeze autorităților competente informațiile pe care le dețin în mod legal și care sunt necesare în special pentru prevenirea, investigarea și urmărirea penală a infracțiunilor.

16. În conformitate cu articolul 77 alineatul 4, în cazul în care există o hotărâre judecătorească motivată sau un alt temei juridic prevăzut de lege, furnizorii de servicii de comunicații electronice trebuie să facă posibil din punct de vedere tehnic, în special pentru organele de cercetare penală și de urmărire penală, în conformitate cu procedurile prevăzute de dreptul procesual penal, controlul conținutului comunicațiilor transmise prin rețelele de comunicații electronice.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. În conformitate cu articolul 6 alineatul 3 punctul 1, în cazul în care sunt îndeplinite condițiile prevăzute de LIC și cu autorizarea prealabilă a parchetului sau a unui organ judiciar, organele de cercetare penală [10] pot colecta informații de la furnizorii de servicii de comunicații electronice.

18. În conformitate cu articolul 8 alineatele 1 și 3, organele de cercetare penală acționează de îndată ce dispun de informații privind pregătirea sau săvârșirea unei infracțiuni deosebit de grave, grave sau de o gravitate scăzută și inițiază imediat urmărirea penală în cazul în care cercetarea indică existența unei infracțiuni.

19. În conformitate cu articolul 19 alineatul 1 punctul 5, informațiile care provin din operațiuni de cercetare penală pot fi utilizate în cazurile prevăzute la alineatele 3 și 4 ale aceleiași dispoziții și în alte situații prevăzute de lege.

20. În conformitate cu articolul 19 alineatul 3, informațiile referitoare la un eveniment care prezintă caracteristicile unei infracțiuni legate de corupție pot fi declasificate, cu acordul parchetului, și utilizate în contextul unei cercetări privind abateri disciplinare sau în serviciu.

[7] Legea Republicii Lituania privind comunicațiile electronice, în versiunea Legii nr. IX-2135 din 15 aprilie 2004, astfel cum a fost modificată prin Legea nr. XIII-2172 din 6 iunie 2019, denumită în continuare „LCE”.

[8] Datele enumerate în anexa menționată („Categorii de date care trebuie protejate”) sunt cele necesare pentru a identifica originea și destinația unei comunicații, data efectuării ei, ora și durata, tipul și localizarea echipamentului de comunicație (inclusiv comunicații mobile) al utilizatorilor.

[9] Legea Republicii Lituania privind datele operative în materie penală, în versiunea Legii nr. XI-2234 din 2 octombrie 2012, astfel cum a fost modificată prin Legea nr. XIII-1837 din 20 decembrie 2018 (denumită în continuare „LIC”).

[10] Vom utiliza termenul de „servicii de informații”, iar nu „organe de culegere a datelor operative”, pentru a desemna serviciile care efectuează cercetările corespunzătoare.

3. Lietuvos Respublikos baudžiamojo proceso kodeksas [11]

21. În conformitate cu articolul 154 („Controlul, înregistrarea și stocarea informațiilor transmise prin intermediul rețelelor de comunicații electronice”) alineatul 1, un organ de anchetă poate, în temeiul deciziei pronunțate la cererea parchetului de un judecător specializat, să asculte, să înregistreze și să stocheze conversațiile transmise prin intermediul rețelelor de comunicații electronice, dacă există motive să creadă că s-ar putea obține informații despre o infracțiune deosebit de gravă sau gravă care este în curs de pregătire sau de săvârșire sau care a fost deja săvârșită ori despre o infracțiune de o gravitate scăzută sau care nu este gravă.

22. În conformitate cu articolul 177 („Interdicția de comunicare a datelor din cadrul cercetării penale”) alineatul 1, informațiile obținute în cursul urmăririi penale sunt confidențiale și, până la judecarea cauzei, pot fi divulgate numai cu autorizarea parchetului și numai în măsura în care se justifică [12].

II. Situația de fapt, litigiul și întrebarea preliminară

23. Lietuvos Respublikos generalinė prokuratūra (Parchetul General al Republicii Lituania, denumit în continuare „Parchetul General”) a efectuat o anchetă internă cu privire la acțiunile întreprinse de A. G., care, la momentul respectiv, deținea funcția de procuror în cadrul Apygardos prokuratūra (Parchetul Regional), ca urmare a existenței unor indicii cu privire la săvârșirea unui abuz în serviciu.

24. Comisia din cadrul Parchetului General a concluzionat că A. G. săvârșise un abuz în serviciu și a propus să i se aplice acestuia sancțiunea disciplinară a destituirii din funcție.

25. Abuzul în serviciu ar fi fost stabilit pe baza informațiilor obținute în cursul procedurii administrative prin intermediul acțiunilor serviciilor de informații în materie penală, pe baza explicațiilor date de alți funcționari și de recurent, precum și pe baza concluziilor a două proceduri de cercetare penală.

26. În concret, ar fi existat comunicații telefonice între A. G. și avocatul unui suspect, în cadrul unei cercetări penale efectuate de A. G., cu privire la cauze în care avocatul respectiv acționase în calitate de apărător [13].

27. Supravegherea și înregistrarea conținutului informațiilor transmise prin rețelele de comunicații electronice au fost autorizate prin hotărâri judecătorești.

28. Procurorul general i-a aplicat lui A. G. sancțiunea destituirii din funcție, pe care acesta a contestat-o la Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional din Vilnius, Lituania), solicitând anularea sa.

[11] Codul de procedură penală al Republicii Lituania din 14 martie 2002, în versiunea aplicabilă în litigiul principal, denumit în continuare „CEC”.

[12] În conformitate cu Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendajos (Recomandări privind furnizarea și utilizarea datelor din cadrul cercetării penale în alte scopuri decât cel al urmăririi penale, precum și protecția datelor pe parcursul cercetării penale), aprobate prin Ordinul nr. 1 279 al Procurorului General din 17 august 2017, astfel cum a fost modificat prin Ordinul nr. 1 211 din 25 iunie 2018, în special clauza 23, procurorul, după primirea unei cereri de acces la informațiile din cadrul urmăririi penale, decide dacă este cazul să le furnizeze. În caz afirmativ, acesta trebuie să precizeze în ce măsură pot fi furnizate.

[13] Astfel cum s-a arătat în ședință, împotriva lui A. G. și a avocatului respectiv sunt în curs de soluționare proceduri penale pentru aceste fapte.

29. Acțiunea a fost respinsă prin hotărârea din 16 iulie 2021, instanța de prim grad de jurisdicție constatând legalitatea atât a acțiunilor serviciilor de informații în materie penală, cât și a utilizării, în cadrul procedurii disciplinare, a datelor obținute de serviciile respective.

30. Împotriva hotărârii pronunțate în primă instanță, A. G. a declarat recurs la Lietuvos vyriausiasis administracinis teismas (Curtea Administrativă Supremă din Lituania), instanță care solicită Curții să se pronunțe cu privire la următoarea întrebare preliminară:

„Articolul 15 alineatul (1) din Directiva 2002/58/CE […] coroborat cu articolele 7, 8, și 11 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretat în sensul că interzice autorităților publice competente să utilizeze datele stocate de furnizorii de servicii de comunicații electronice, ce pot oferi informații privind datele unui utilizator al unui mijloc de comunicare electronică și comunicațiile efectuate de acesta, în cadrul unor investigații privind fapte de corupție legate de abuzul în serviciu, indiferent dacă accesul la aceste date a fost acordat, în cazul concret, în scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice?”

III. Procedura în fața Curții

31. Cererea de decizie preliminară a fost înregistrată la grefa Curții la 3 martie 2022.

32. Au prezentat observații scrise A. G., guvernele ceh, estonian, maghiar, irlandez, italian și lituanian, precum și Comisia Europeană.

33. La ședința din 2 februarie 2023 au participat A. G., guvernele francez, maghiar, irlandez și lituanian și Comisia.

IV. Analiză

A. Admisibilitate. Delimitarea răspunsului la întrebarea preliminară

34. Instanța de trimitere este o instanță de contencios administrativ, competentă să efectueze controlul jurisdicțional al deciziilor administrative. Aceasta este natura deciziei luate de Procurorul General, care a aplicat sancțiunea destituirii din funcție a unui funcționar din cadrul unui parchet teritorial pentru fapte ce constituie abateri în serviciu.

35. Prin urmare, litigiul principal nu se referă la decizii ale autorităților judiciare penale. Chiar dacă aceste decizii coexistă cu procedura administrativă (disciplinară) care a condus la destituirea din funcție[14], este important de subliniat că litigiul vizează numai destituirea din funcție.

36. Astfel, în decizia de trimitere se observă anumite inadvertențe în ceea ce privește situația de fapt din litigiu care stabilește contextul în care se înscrie întrebarea preliminară.

[14] A se vedea nota de subsol 13 din prezentele concluzii.

37. După cum au subliniat guvernul ceh și Comisia, nu se poate stabili cu certitudine pe baza deciziei de trimitere dacă autoritățile competente: a) s-au adresat furnizorilor de servicii de comunicații electronice pentru a obține datele în litigiu sau b) au obținut ele însele, în mod direct, datele respective.

38. Problema nu este deloc una minoră. De ea depinde identificarea reglementării Uniunii pe baza căreia se poate răspunde la întrebarea preliminară. În funcție de modalitatea de săvârșire a faptelor, va fi aplicabilă:

– fie Directiva 2002/58, în cazul în care datele obținute sunt rezultatul unei obligații de prelucrare impuse furnizorilor de servicii de comunicații electronice,

– fie Directiva 2016/680, în cazul în care datele au fost obținute direct de autoritatea publică, fără a impune obligații furnizorilor respectivi.

39. În al doilea caz, protecția datelor cu caracter personal ar fi reglementată de dreptul național, fără a se aduce atingere aplicării Directivei 2016/680[15]. Prin urmare, întrebarea preliminară ar fi formulată pe baza unei abordări necorespunzătoare prin punerea accentului pe Directiva 2002/58.

40. Guvernul maghiar, convins că datele cu caracter personal au fost obținute prin intermediul unor operațiuni de interceptare telefonică efectuate de serviciile de informații în materie penală, pune sub semnul întrebării admisibilitatea trimiterii preliminare, deoarece Directiva 2002/58 ar fi implicit inaplicabilă.

41. Totuși, potrivit Comisiei:

– Directiva 2016/680 ar fi aplicabilă în măsura în care datele cu caracter personal colectate și stocate direct de autorități în cadrul unei cercetări penale anterioare urmează să fie utilizate în cadrul unei cercetări ulterioare;

– Directiva 2002/58 ar fi aplicabilă în cazul în care, astfel cum a constatat instanța de trimitere[16], cel puțin o parte din date trebuiau să fie colectate și stocate în temeiul unei dispoziții naționale adoptate în conformitate cu articolul 15 alineatul (1) din aceasta. Directiva 2002/58 ar fi astfel relevantă pentru soluționarea litigiului.

42. Împărtășim abordarea Comisiei, singura de altfel care permite depășirea reticențelor (justificate) cu privire la admisibilitatea deciziei de trimitere.

43. Înțeleasă în acest fel întrebarea preliminară, relevanța Directivei 2002/58 pentru soluționarea sa:

– rezultă din prezumția inerentă tuturor trimiterilor preliminare în ceea ce privește necesitatea formulării lor, a cărei apreciere este de competența instanței care o propune[17];

[15] Hotărârea La Quadrature du Net, punctul 103: „atunci când statele membre pun în aplicare în mod direct măsuri care derogă de la confidențialitatea comunicațiilor electronice, fără a impune obligații de prelucrare furnizorilor de servicii de astfel de comunicații, protecția datelor persoanelor în cauză nu intră sub incidența Directivei 2002/58, ci exclusiv a dreptului național, sub rezerva aplicării [Directivei 2016/680]”.

[16] Punctul 37 din decizia de trimitere.

[17] A se vedea în special Hotărârea din 4 decembrie 2018, Minister for Justice and Equality și Commissioner of An Garda Síochána (C-378/17, EU:C:2018:979, punctul 26), și Hotărârea din 22 decembrie 2022, Airbnb Ireland și Airbnb Payments UK (C-83/21, EU:C:2022:1018, punctul 82).

– poate fi acceptată în măsura în care se solicită interpretarea Curții numai cu privire la Directiva 2002/58, pe care instanța o consideră esențială pentru soluționarea litigiului [18].

44. Astfel, potrivit instanței de trimitere, în procedura pe care trebuie să o soluționeze sunt relevante următoarele aspecte:

„i) accesul la *datele stocate de furnizorii de servicii de comunicații electronice*, nu doar în scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței public, și

ii) *utilizarea datelor stocate* obținute în scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice în cadrul cercetării unor fapte de corupție legate de abuzul în serviciu” [19].

45. Prin urmare, totul pare să indice că, în afară de eventuala existență a unor date cu caracter personal a căror prelucrare nu ar putea intra în domeniul de aplicare al Directivei 2002/58 (ci în cel al Directivei 2016/680), în cadrul cercetării care a condus la aplicarea sancțiunii au fost utilizate date cu caracter personal colectate de la furnizorii de servicii de comunicații electronice.

46. Răspunsul Curții trebuie să se limiteze la cererea instanței de trimitere, astfel cum este formulată. Prin urmare, aceasta trebuie să stabilească dacă datele cu caracter personal obținute și prelucrate în temeiul articolului 15 alineatul (1) din Directiva 2002/58 în cadrul cercetării penale pot fi utilizate ulterior cu ocazia unei proceduri disciplinare (administrative) inițiate împotriva unui funcționar public.

47. Astfel delimitați termenii trimiterii preliminare, considerațiile pe care tocmai le-am expus mai sus au ca revers faptul că următoarele chestiuni rămân neabordate în cuprinsul acesteia:

– în primul rând, cele referitoare la legalitatea *colectării inițiale* a datelor cu caracter personal în temeiul articolului 15 alineatul (1) din Directiva 2002/58. Întrebarea instanței de trimitere se limitează la *utilizarea ulterioară* a datelor respective în cadrul procedurii disciplinare, fără a pune în discuție legalitatea colectării lor inițiale [20];

– în al doilea rând, cele referitoare la utilizarea datelor obținute și prelucrate direct de autoritățile publice în cadrul unor cercetări penale anterioare. Nici cu privire la acest aspect, care intră în domeniul de aplicare al dreptului național și al Directivei 2016/680, instanța de trimitere nu are îndoieli.

[18] Trimiterea fără echivoc la Directiva 2002/58 în dispozitivul deciziei de trimitere și tăcerea cu privire la Directiva 2016/680 în motivarea în drept a acesteia sugerează același lucru. Situația este diferită în cazul în care Curtea, fără să depășească limitele întrebării, poate oferi instanței de trimitere indicații utile în vederea pronunțării, eventual prin trimitere la alte dispoziții de drept al Uniunii. A se vedea în acest sens Hotărârea din 18 septembrie 2019, VIPA (C-222/18, EU:C:2019:751, punctul 50 și jurisprudența citată).

[19] Punctul 35 din decizia de trimitere. Sublinierea noastră.

[20] Prin urmare, nu este necesară pronunțarea Curții cu privire la legalitatea unor astfel de operațiuni prealabile. În cazul în care ar face acest lucru, ar trebui să reafirme că se poate acorda *acces* la datele deținute de furnizorii de servicii de comunicații electronice numai dacă sunt *stocate* de aceștia în conformitate cu articolul 15 alineatul (1) din Directiva 2002/58. A se vedea în acest sens Hotărârea La Quadrature du Net, punctul 167. Dispoziția menționată, interpretată în lumina articolelor 7, 8, 11 și a articolului 52 alineatul (1) din cartă, se opune unor măsuri legislative care prevăd cu titlu preventiv stocarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare în astfel de scopuri (Hotărârea La Quadrature du Net, punctul 168).

48. În concluzie, în considerațiile cu privire la fondul cauzei pe care le vom prezenta în continuare va trebui să facem abstracție de interpretarea Directivei 2016/680 [21]. Acestea se vor limita, în ceea ce privește Directiva 2002/58, la utilizarea datelor cu caracter personal obținute în temeiul său prin intermediul unor prelucrări a căror legalitate inițială trebuie prezumată, în măsura în care nu este în discuție în litigiul principal.

B. Cu privire la fond

1. Recapitularea jurisprudenței Curții referitoare la aplicarea Directivei 2002/58

49. Din articolul 15 alineatul (1) prima teză din Directiva 2002/58 rezultă că statele membre pot adopta o măsură care derogă de la principiul confidențialității consacrat la articolul 5 alineatul (1) din aceeași directivă, atunci când aceasta este „o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice” și „strict” proporțională cu scopul urmărit [22].

50. În special, posibilitatea statelor membre de a justifica o restrângere a drepturilor și a obligațiilor prevăzute printre altele la articolele 5, 6 și 9 din Directiva 2002/58 trebuie să fie apreciată măsurând gravitatea ingerinței pe care o implică o asemenea restrângere și verificând dacă importanța obiectivului de interes general urmărit prin restrângerea respectivă se raportează la această gravitate [23].

51. „Pentru a îndeplini cerința proporționalității, o reglementare trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz. Această reglementare trebuie să aibă forță juridică obligatorie în dreptul intern și în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date […]” [24].

52. În ceea ce privește obiectivele de interes general care pot justifica o măsură adoptată în temeiul articolului 15 alineatul (1) din Directiva 2002/58, în conformitate cu principiul proporționalității, există o ierarhie a acestor obiective în funcție de importanța lor, iar importanța obiectivului urmărit de o asemenea măsură trebuie să se raporteze la gravitatea ingerinței [25].

53. În această ierarhie a obiectivelor, protecția securității naționale, interpretată în lumina articolului 4 alineatul (2) TUE, trece înaintea celorlalte obiective menționate la articolul 15 alineatul (1) din Directiva 2002/58, și anume apărarea, siguranța publică sau prevenirea,

[21] Ne vom referi totuși la ea, cu titlu subsidiar, în partea finală a prezentelor concluzii.

[22] Hotărârea La Quadrature du Net, punctul 129.

[23] Hotărârea La Quadrature du Net, punctul 131 și jurisprudența citată.

[24] Hotărârea Commissioner of An Garda Síochána, punctul 54.

[25] Hotărârea Commissioner of An Garda Síochána, punctul 56.

investigarea, depistarea și urmărirea penală a unor fapte penale ori a folosirii neautorizate a sistemelor de comunicații electronice. Obiectivul combaterii infracționalității în general, inclusiv a infracțiunilor grave, și al protejării siguranței publice se încadrează în a doua categorie [26].

54. Din această clasificare a obiectivelor rezultă că:

– obiectivul privind protejarea securității naționale, primul în ierarhia indicată de Curte, permite o ingerință la fel de gravă ca cea pe care o presupun măsurile legislative care permit să se impună furnizorilor de servicii de comunicații electronice obligația de a stoca în mod generalizat și nediferențiat datele de transfer și datele de localizare [27];

– următorul obiectiv în ordinea importanței, și anume cel al combaterii infracționalității grave, poate justifica ingerințe precum stocarea direcționată a datelor de transfer și a datelor de localizare sau a adreselor IP atribuite sursei unei conexiuni, pentru o perioadă limitată în timp la strictul necesar [28].

2. Aplicarea acestei jurisprudențe în prezenta trimitere preliminară

55. Potrivit instanței de trimitere, datele în cauză au fost obținute printr-o ingerință gravă în drepturile garantate de articolele 7, 8 și 11 din cartă [29].

56. Reiterăm faptul că în prezenta cauză nu este vorba despre examinarea legalității inițiale a obținerii acestor date, cu alte cuvinte despre a aprecia dacă intervenția a fost suficient de justificată având în vedere gravitatea infracțiunii a cărei combatere era avută în vedere.

57. Instanța de trimitere s-a pronunțat cu privire la ambele chestiuni (gravitatea ingerinței și gravitatea încălcării) în termeni care nu sunt contestați în procedura principală și care, prin urmare, nu sunt relevanți pentru prezenta trimitere preliminară.

58. Ceea ce este relevant în prezenta cauză, potrivit instanței de trimitere, este să se stabilească dacă acele date: a) pot fi utilizate și în cadrul unor cercetări ulterioare care vizează combaterea infracționalității în general (presupunând că această noțiune include comportamentul care face obiectul sancțiunii disciplinare în discuție) sau b) pot fi utilizate numai în cadrul cercetărilor care vizează combaterea infracționalității grave.

59. Guvernele ceh și irlandez au examinat dacă comportamentul analizat de instanța de trimitere poate fi sau nu calificat drept „infracțiune gravă” și au concluzionat că se integrează în noțiunea respectivă.

[26] Hotărârea La Quadrature du Net, punctele 135 și 136, în care se arată că securitatea națională este de competența exclusivă a fiecărui stat membru și că ea corespunde interesului primordial de a proteja funcțiile esențiale ale statului și interesele fundamentale ale societății în cazul unor activități susceptibile să destabilizeze grav structurile constituționale, politice, economice sau sociale fundamentale ale unei țări și în special să amenințe în mod direct societatea, populația sau statul în sine, cum ar fi activitățile de terorism. Astfel de amenințări se disting, prin natura și prin gravitatea lor deosebită, de riscul general de apariție a unor tensiuni sau a unor tulburări, chiar grave, care afectează siguranța publică. Obiectivul de protejare a securității naționale poate justifica, așadar, măsuri care presupun ingerințe mai grave în drepturile fundamentale decât cele pe care le-ar putea justifica celelalte obiective.

[27] Hotărârea Commissioner of An Garda Síochána, punctul 58.

[28] Hotărârea La Quadrature du Net, punctul 168.

[29] Astfel cum rezultă din punctul 46 din decizia de trimitere: în cuprinsul ei se face referire la datele care pot furniza informații cu privire la comunicațiile efectuate de un utilizator al unui mijloc de comunicație electronică sau la localizarea echipamentelor terminale pe care le utilizează și care permit tragerea unor concluzii precise în legătură cu viața privată a persoanelor vizate.

60. Totuși, în opinia noastră, aceasta este o chestiune în privința căreia Curtea nu este obligată să se pronunțe, fiind de competența instanței de trimitere să stabilească natura comportamentului.

61. Instanța de trimitere arată că, în cazul în care utilizarea datelor obținute printr-o ingerință gravă în drepturile fundamentale nu poate fi justificată decât în scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, astfel de date nu pot fi utilizate în vederea cercetării abaterilor disciplinare legate de fapte de corupție [30]. Cu alte cuvinte, în cadrul unor cercetări precum cea în discuție în prezenta cauză.

62. Pe baza acestei aprecieri, trebuie să se stabilească dacă abaterile disciplinare pentru a căror urmărire se dorește utilizarea anumitor date cu caracter personal trebuie, din perspectiva gravității lor, să fie echivalente calitativ cu abaterile care au justificat colectarea datelor respective [31].

63. În ședință, guvernul lituanian a recunoscut că destituirea din funcție a fost impusă ca urmare a unei abateri profesionale a procurorului sancționat. Verificarea aspectului dacă această abatere (scurgerea de informații privind o cercetare penală) poate fi asimilată unei infracțiuni grave sau dacă implică un risc grav pentru protejarea siguranței publice depinde de o serie de factori pe care numai instanța de trimitere este în măsură să îi analizeze [32].

64. În ședință, s-au făcut numeroase referiri la combaterea corupției, ca fenomen care stă la baza unor comportamente precum cel în discuție în cauză. Dezbaterea privind această chestiune ar necesita multe nuanțări, în vederea asigurării rigorii necesare în contextul tuturor manifestărilor puterii punitive ale statului. S-ar impune să se stabilească, de exemplu, dacă termenul de „corupție” este utilizat într-un sens generic sau dacă se referă la un tip specific de comportament în care, în abstract, ar fi poate excesiv să se includă simpla încălcare a obligației de păstrare a secretului, dacă nu este însoțită de un avantaj corelativ pentru funcționar [33].

65. În orice caz, în cazul în care instanța de trimitere consideră că încălcarea eticii sancționată în speță este mai puțin gravă decât infracțiunea a cărei cercetare a justificat măsura adoptată în temeiul articolului 15 din Directiva 2002/58, răspunsul la întrebarea sa preliminară poate fi dedus din următoarele aspecte reținute de Curte:

– „[A]ccesul la datele de transfer și la datele de localizare păstrate de furnizori în aplicarea unei măsuri adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, care trebuie să aibă loc cu respectarea deplină a condițiilor care rezultă din jurisprudența de interpretare a

[30] Decizia de trimitere, punctul 46 *in fine*.

[31] În Hotărârea Curții Europene a Drepturilor Omului (Curtea EDO) din 18 ianuarie 2022, Adomaitis împotriva Lituaniei (CE:ECHR:2022:0118JUD001483318, denumită în continuare „Hotărârea Curții EDO Adomaitis”), care se referea la interceptarea comunicațiilor electronice în cazul unui abuz de putere continuu din partea directorului unei închisori, oferă indicii pentru a aprecia această echivalență.

[32] În principiu, nu sunt comparabile, pe de o parte, un comportament sancționabil care face obiectul analizei în cadrul unui proces penal și, pe de altă parte, o abatere pur deontologică, care este sancționată în cadrul unei proceduri disciplinare. Procesul penal și procedura disciplinară se diferențiază, din punctul de vedere al obiectului lor, prin natura și gravitatea comportamentului analizat. Disparitatea procedurilor este, în aceste sens, un indiciu al gravității diferite a obiectelor lor.

[33] În convenția elaborată în temeiul articolului K.3 alineatul (2) litera (c) din Tratatul privind Uniunea Europeană, privind lupta împotriva corupției care implică funcționari ai Comunităților Europene sau funcționari ai statelor membre ale Uniunii Europene (JO 1997, C 195, p. 2, Ediție specială, 19/vol. 11, p. 196) se menționează situații de corupție pasivă („fapta săvârșită cu intenție, de către un funcționar, direct sau prin intermediul unui terț, de a pretinde sau a primi avantaje de orice natură, pentru sine sau pentru un terț, sau de a accepta o promisiune în acest sens, pentru a îndeplini sau pentru a se abține să îndeplinească, cu încălcarea îndatoririlor sale ca funcționar, un act în conformitate cu îndatoririle sale sau în exercițiul funcției sale”) și de corupție activă („fapta săvârșită cu intenție, de către orice persoană, de a promite sau de a da, direct sau prin intermediul unui terț, un avantaj de orice natură, pentru sine sau pentru un terț, unui funcționar, pentru ca acesta din urmă să îndeplinească sau să se abțină să îndeplinească, cu încălcarea îndatoririlor sale ca funcționar, un act în conformitate cu îndatoririle sale sau în exercițiul funcției sale”), care trebuie să fie calificate drept infracțiuni.

Directivei 2002/58, nu poate fi justificat, în principiu, decât prin obiectivul de interes general în vederea căruia această păstrare a fost impusă furnizorilor respectivi. Situația este diferită numai dacă importanța obiectivului urmărit prin acces o depășește pe cea a obiectivului care a justificat păstrarea”[34];

– „[Î]n special, […] accesul la astfel de date în scopul urmăririi penale și al sancționării unei infracțiuni [de drept comun] nu poate fi în niciun caz acordat atunci când stocarea acestora a fost justificată de obiectivul de combatere a infracționalității grave sau *a fortiori* de protejare a securității naționale”[35].

66. Prin urmare, în această privință, se aplică un fel de principiu al echivalenței între obiectivele de interes general care justifică *colectarea* datelor cu caracter personal, pe de o parte, și cele care justifică *utilizarea* ulterioară a acestora, pe de altă parte. Singura derogare de la principiul respectiv este posibilă, astfel cum tocmai am arătat, atunci când importanța obiectivului urmărit prin accesul la date o depășește pe cea a obiectivului care a justificat stocarea.

67. O interpretare diferită ar presupune denaturarea sistemului de garanții al Directivei 2002/58: drepturile pe care le protejează ar putea face obiectul unor ingerințe grave dincolo de situațiile prevăzute la articolul 15 din aceasta și de condițiile stabilite în jurisprudența Curții.

68. În special, periclitarea dreptului la confidențialitatea comunicațiilor este admisibilă în mod legitim numai în funcție de obiectivul specific de interes general pe care îl urmărește. Prin urmare, legitimitatea accesului la datele stocate trebuie verificată de la caz la caz, punând în balanță gravitatea pe care o implică, pe de o parte, și importanța obiectivului de interes general care trebuie îndeplinit prin această ingerință, pe de altă parte.

69. O interpretare inacceptabilă a Directivei 2002/58 este că, odată cu facilitarea accesului cu prima ocazie care îl justifică în mod valid, se deschide calea pentru un acces ulterior (în realitate, o reutilizare a datelor obținute) bazat pe un obiectiv ierarhic inferior celui corespunzător situației inițiale.

70. În acest sens, cerințele pentru acordarea accesului inițial (inclusiv cele impuse de Curte în vederea autorizării sale)[36] pot fi extrapolate la utilizarea ulterioară a acelorași date de alte autorități.

C. Cu titlu subsidiar: incidența Directivei 2016/680

71. Până aici, am prezentat aspectele pe care le considerăm cele mai adecvate pentru a răspunde la cererea de decizie preliminară în termenii în care a fost formulată, și anume prin facilitarea interpretării Directivei 2002/58, astfel cum a solicitat instanța de trimitere.

72. În ipoteza în care datele în discuție în prezenta cauză nu ar fi fost obținute în temeiul articolului 15 alineatul (1) din Directiva 2002/58, ci direct de către serviciile de informații în materie penală ale statului membru în cadrul unui proces penal, scenariul ar fi diferit.

[34] Hotărârea Commissioner of An Garda Síochána, punctul 98.

[35] Hotărârea La Quadrature du Net, punctul 166.

[36] Hotărârea Commissioner of An Garda Síochána, punctul 106, care citează Hotărârea Prokuratuur, punctul 51.

73. În această ipoteză, ar fi aplicabile normele dreptului național, fără a aduce atingere aplicării Directivei 2016/680 în ceea ce privește prelucrarea datelor cu caracter personal obținute în cadrul unei cercetări penale. Plecăm de la premisa că acțiunile serviciilor de informații în materie penală în astfel de situații intră în domeniul de aplicare al Directivei 2016/680. Acest lucru a fost confirmat în ședință.

74. Astfel cum am arătat în Concluziile prezentate în cauza Inspektor v Inspektorata kam Visshia sadeben savet (Scopurile prelucrării datelor cu caracter personal – Anchetă penală) [37], „GDPR și Directiva 2016/680 formează un sistem coerent în cadrul căruia:

– RGPD stabilește *normele generale* de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal;

– Directiva 2016/680 instituie *normele specifice* privind prelucrarea datelor respective în domeniul cooperării judiciare în materie penală și al cooperării polițienești [38].

75. Aminteam atunci [39] că:

– „Protecția oferită de regimul constituit de cele două dispoziții se bazează pe principiile legalității, echității, transparenței și, pentru ceea ce ne interesează aici, pe principiul limitării stricte a colectării și prelucrării datelor la scopurile prevăzute de lege.”

– „În concret, articolul 5 alineatul (1) litera (b) din RGPD prevede că datele sunt «colectate în scopuri determinate, explicite și legitime și *nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri*». Articolul 4 alineatul (1) litera (b) din Directiva 2016/680, care reprezintă *lex specialis*, are o formulare identică.”

– „Prin urmare, datele cu caracter personal nu pot fi colectate și prelucrate cu caracter general, ci numai în scopuri determinate și în condițiile de legalitate stabilite de legiuitorul Uniunii [40].”

– „Principiul legăturii stricte dintre colectarea și prelucrarea datelor, pe de o parte, și scopurile care trebuie îndeplinite de ambele operațiuni, pe de altă parte, nu are caracter absolut, deoarece atât RGPD, cât și Directiva 2016/680 permit o anumită flexibilitate […]”.

76. Or, conform interpretării date de Curte articolului 4 alineatul (2) din Directiva 2016/680 [41], este dificil de acceptat ca datele cu caracter personal colectate în cursul unui proces penal să fie utilizate *în același scop* în contextul unei proceduri disciplinare ulterioare împotriva unui funcționar public.

[37] C-180/21 (EU:C:2022:406), în continuare „Concluziile Inspektor v Inspektorata”.

[38] Concluziile Inspektor v Inspektorata, punctul 35.

[39] Concluziile Inspektor v Inspektorata, punctele 36-39.

[40] Cerința privind „legalitatea” este prevăzută la articolul 5 alineatul (1) litera (a) din RGPD [articolul 4 alineatul (1) litera (a) din Directiva 2016/680], iar condițiile sale sunt stabilite la articolul 6 din RGPD. În ceea ce privește prezenta cauză și în conformitate cu litera (e) a acestei din urmă dispoziții, prelucrarea trebuie să fie necesară pentru îndeplinirea unei sarcini de interes public sau pentru exercitarea autorității publice cu care este învestit operatorul de date (care efectuează prelucrarea propriu-zisă).

[41] Hotărârea din 8 decembrie 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Scopurile prelucrării datelor cu caracter personal – Anchetă penală), C-180/21 (EU:C:2022:967), denumită în continuare „Hotărârea Inspektor v Inspektorata”.

77. Ar trebui să reamintim însă că, în conformitate cu articolul 4 alineatul (2) din Directiva 2016/680, „prelucrarea de către același operator sau de către un altul, în oricare dintre scopurile stabilite la articolul 1 alineatul (1), altele decât cele pentru care datele cu caracter personal au fost colectate, este permisă în măsura în care:

– operatorul este autorizat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu dreptul Uniunii sau cu dreptul intern, și

– prelucrarea este necesară și proporțională în raport cu respectivul alt scop, în conformitate cu dreptul Uniunii sau cu dreptul intern”.

78. Pornind de la această premisă, instanța de trimitere trebuie să analizeze dacă scopul (*diferit*) al prelucrării ulterioare figurează sau nu printre cele prevăzute la articolul 1 alineatul (1) din Directiva 2016/680:

– în primul caz (reafectare *ad intra* a datelor), va fi necesar să se verifice dacă sunt îndeplinite cele două cerințe prevăzute la articolul 4 alineatul (2) din Directiva 2016/680;

– în al doilea caz (reafectare *ad extra* a datelor), este aplicabil articolul 9 alineatul (1) din Directiva 2016/680.

1. Utilizarea datelor în temeiul articolului 4 alineatul (2) din Directiva 2016/680

79. În ceea ce privește *prima* dintre cele două cerințe prevăzute de dispoziția menționată, aceasta este îndeplinită numai dacă legislația statului membru se reflectă într-o lege [42] care reglementează momentul la care operatorul este autorizat să prelucreze datele cu caracter personal. Această lege trebuie, în plus, să conțină norme obligatorii, clare și precise [43].

80. Aceasta este totuși o chestiune care, în mod normal, trebuie verificată de instanța de trimitere, în urma analizării articolului 177 din CEC, a articolului 19 alineatul (3) din LIC și a recomandărilor Parchetului General [44]. Pe baza acestor elemente, va trebui evaluat în ce măsură dreptul național permite ca informațiile obținute în cadrul proceselor penale să fie utilizate, în anumite condiții, în contextul cercetării abaterilor disciplinare. Considerentele Curții EDO din Hotărârea Adomaitis pot fi utile pentru această verificare [45].

81. În ceea ce privește *a doua* condiție, instanța de trimitere va trebui să aprecieze dacă, în cazul prelucrării datelor în discuție în prezenta cauză, ingerința era necesară și proporțională [46].

[42] Împărtășim opinia Comisiei potrivit căreia, întrucât utilizarea ulterioară a datelor cu caracter personal obținute în cursul unor cercetări penale reprezintă o ingerință în drepturile fundamentale garantate de articolele 7 și 8 din cartă, este inadmisibil, potrivit articolului 52 alineatul (1) din cartă, ca aceasta să fie prevăzută de lege.

[43] Punctul 51 din prezentele concluzii

[44] Nota de subsol 12 din prezentele concluzii.

[45] La punctul 83 din hotărâre, se consideră a fi suficientă garanția legalității ingerinței asigurate de dispozițiile legislative naționale și de jurisprudența constituțională lituaniană.

[46] Astfel cum observă Comisia, această cauză nu este foarte diferită de cea examinată în Hotărârea CEDO din 16 iunie 2016, Versini-Campinchi și Crasnianski împotriva Franței (CE:ECHR:2016:0616JUD004917611). Conform celor arătate la punctul 57 din aceasta, utilizarea, în cadrul unei proceduri disciplinare pentru încălcarea secretului profesional, a comunicațiilor interceptate în cadrul unui proces penal urmărește unul dintre scopurile legitime în sensul articolului 8 din CEDO. Întrepătrunderea materială strânsă între obiectivul procesului penal și cel al procedurii disciplinare conduce la împărtășirea legitimității scopurilor celor două.

82. După cum am arătat, aspectele reținute în Hotărârea Adomaitis pronunțată de Curtea EDO pot contribui la această apreciere:

– în ceea ce privește necesitatea, va trebui să se evalueze în ce măsură insuficiența dovezilor privind alte date disponibile în cursul procedurii disciplinare a făcut ca utilizarea datelor în litigiu să fie cu adevărat necesară pentru succesul cercetării în curs [47].

– în ceea ce privește proporționalitatea, trebuie evaluată gravitatea infracțiunii care a dat naștere procedurii disciplinare, dar ținând cont de faptul că, astfel cum a susținut guvernul lituanian și așa cum reiese din Hotărârea Adomaitis pronunțată de Curtea EDO [48], utilizarea datelor cu caracter personal este rezervată infracțiunilor pentru care este prevăzută cea mai severă sancțiune disciplinară, și anume destituirea.

2. Utilizarea datelor în temeiul articolului 9 din Directiva 2016/680

83. În conformitate cu articolul 9 alineatul (1) din Directiva 2016/680, datele cu caracter personal colectate de autoritățile competente în scopurile stabilite la articolul 1 alineatul (1) nu se prelucrează în alte scopuri decât cele stabilite la articolul 1 alineatul (1), cu excepția cazurilor în care o astfel de prelucrare este autorizată în temeiul dreptului Uniunii sau al dreptului unui stat membru. În această situație, se aplică RGPD, mai puțin în cazul în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii [49].

84. În cazul în care instanța de trimitere consideră că articolul 4 alineatul (2) din Directiva 2016/680 nu este aplicabil, va trebui să facă referire la RGPD. În temeiul acestui regulament, va trebui să stabilească dacă, pe lângă dispoziția legală, este îndeplinită cel puțin una dintre condițiile privind legalitatea prelucrării datelor cu caracter personal enumerate în mod exhaustiv la articolul 6 alineatul (1) din RGPD.

V. Concluzie

85. Având în vedere considerațiile care precedă, propunem Curții să răspundă Lietuvos vyriausiasis administracinis teismas (Curtea Administrativă Supremă, Lituania) 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) coroborat cu articolele 7, 8, 11 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene

trebuie interpretat în sensul că

[47] Hotărârea Curții EDO Adomaitis, punctul 85.

[48] Hotărârea Curții EDO Adomaitis, punctul 87.

[49] Această excepție a fost interpretată în sens strict în Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare), (C-439/19, EU:C:2021:504, punctul 66).

interzice autorităților publice competente să colecteze date stocate de furnizorii de servicii de comunicații electronice, ce pot oferi informații detaliate despre un utilizator, și să le folosească în cadrul unor investigații privind comportamente care constituie infracțiuni mai puțin grave decât cele a căror cercetare a putut la momentul respectiv să justifice accesul la acele date.

2. Cu caracter subsidiar:

Articolul 9 alineatul (1) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului coroborat cu articolele 6 și 10 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, în lumina articolelor 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene,

trebuie interpretat în sensul că

nu se opune utilizării, în cadrul unei proceduri administrative disciplinare, a datelor cu caracter personal obținute în mod legal și direct de autoritatea publică în cadrul unei investigații penale, cu condiția ca acea procedură și investigația respectivă să aibă, în conformitate cu norme de drept intern clare, precise și obligatorii, legătură între ele și în măsura în care utilizarea datelor urmărește un scop legitim și este necesară și proporțională, ceea ce trebuie stabilit de autoritatea judiciară.”