Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
DOMNUL GIOVANNI PITRUZZELLA
prezentate la 27 ianuarie 2022[1]

Cauza C-817/19

Ligue des droits humains
împotriva
Consiliului de miniștri

[cerere de decizie preliminară formulată de Cour constitutionnelle (Curtea Constituțională, Belgia)]

„Trimitere preliminară – Protecția datelor cu caracter personal – Prelucrarea datelor din registrul cu numele pasagerilor (PNR) – Regulamentul (UE) 2016/679 – Domeniu de aplicare – Directiva (UE) 2016/681 – Validitate – Carta drepturilor fundamentale a Uniunii Europene – Articolele 7, 8 și 52 alineatul (1)”

Cuprins

[1] Limba originală: franceza.

I. Introducere

1. Prin intermediul prezentei cereri de decizie preliminară, Cour constitutionnelle (Curtea Constituțională, Belgia) adresează Curții de Justiție zece întrebări preliminare referitoare la interpretarea Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (denumit în continuare „RGPD”) [2], precum și la validitatea și interpretarea Directivei (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (denumită în continuare „Directiva PNR”) [3] și a Directivei 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii (denumită în continuare „Directiva API”) [4]. Aceste întrebări au fost adresate în cadrul unei acțiuni formulate de asociația non-profit Ligue des droits humains (denumită în continuare „LDH”), care urmărește anularea totală sau parțială a Legii din 25 decembrie 2016 privind prelucrarea datelor pasagerilor (denumită în continuare „Legea PNR”) [5], care transpune în dreptul belgian Directiva PNR, precum și Directiva API.

2. Întrebările asupra cărora Curtea trebuie să se pronunțe în prezenta cauză se înscriu în cadrul din uneia dintre principalele dileme ale constituționalismului liberal democratic contemporan: cum trebuie definit echilibrul dintre individ și colectivitate în era datelor, în condițiile în care tehnologiile digitale au permis colectarea, stocarea, prelucrarea și analiza unor cantități uriașe de date cu caracter personal în scopuri predictive? Algoritmii, analiza Big Data și inteligența artificială utilizate de autoritățile publice pot fi folosite pentru a promova și a proteja interesele fundamentale ale societății cu o eficiență de neimaginat până în prezent: de la protecția sănătății publice la sustenabilitatea mediului, de la combaterea terorismului la prevenirea criminalității, în special a infracțiunilor grave. În același timp, colectarea nediferențiată a datelor cu caracter personal și utilizarea tehnologiilor digitale de către autoritățile publice pot da naștere unui panoptic digital, cu alte cuvinte unei autorități publice care vede totul fără să fie văzută. O putere

2 JO 2016, L 119, p. 1.

3 JO 2016, L 119, p. 132.

4 JO 2004, L 261, p. 24, Ediție specială 19/vol. 7, p. 40.

5 *Moniteur belge* din 25 ianuarie 2017, p. 12905.

omniscientă, care poate monitoriza și prevedea comportamentul fiecăruia și poate lua măsurile necesare, până la rezultatul paradoxal, imaginat de Steven Spielberg în filmul Minority Report, de a-i lua preventiv libertatea autorului unei infracțiuni care încă nu a fost comisă. După cum știm, în unele țări, societatea primează în fața individului, iar utilizarea datelor cu caracter personal permite realizarea în mod legitim a unei supravegheri în masă eficiente pentru a proteja interese publice considerate fundamentale. În schimb, constituționalismul european – național și supranațional –, cu accent pe individ și pe libertățile sale, pune o barieră semnificativă în calea apariției unei societăți de supraveghere în masă, mai ales după recunoașterea drepturilor fundamentale la respectarea vieții private și la protecția datelor cu caracter personal. În ce măsură poate fi însă ridicată această barieră fără a aduce atingere în mod grav anumitor interese fundamentale ale societății – precum cele menționate mai sus cu titlu de exemplu – care pot avea totuși legături constituționale? Ne aflăm în miezul problemei privind relația dintre individ și colectivitate în societatea digitală. O problemă care necesită, pe de o parte, căutarea și punerea în aplicare a unor echilibre delicate între interesele colectivității și drepturile particularilor pornind de la importanța absolută pe care acestea din urmă o au în patrimoniul constituțional european și, pe de altă parte, instituirea unor garanții împotriva abuzurilor. Și în acest caz ne găsim în cadrul versiunii contemporane a unei teme clasice a constituționalismului, întrucât, așa cum s-a afirmat succint în *Federalist Papers*, oamenii nu sunt îngeri și, prin urmare, sunt necesare mecanisme legale pentru a limita și a controla puterea publică.

3. Acestea sunt problemele de ordin general care se înscriu în contextul prezentelor concluzii, care se pot limita numai la interpretarea dreptului Uniunii în lumina jurisprudenței anterioare a Curții, pe baza unor tehnici bine stabilite, printre care se numără cea a interpretării conforme. O tehnică la care vom recurge frecvent, în cazul în care este posibil din punct de vedere legal, în prezentele concluzii, pentru a găsi echilibrul necesar din punct de vedere constituțional între obiectivele publice care stau la baza sistemului de transfer, de colectare și de prelucrare a datelor din registrul cu numele pasagerilor (denumit în continuare „PNR”) și drepturile consacrate la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”).

II. Cadrul juridic

A. Dreptul Uniunii

1. Carta

4. Potrivit articolului 7 din cartă, „[o]rice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor”.

5. În sensul articolului 8 din cartă:

„(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

(2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.

(3) Respectarea acestor norme se supune controlului unei autorități independente.”

6. În conformitate cu articolul 52 alineatul (1) din cartă, „[o]rice restrângere a exercițiului drepturilor și libertăților recunoscute prin prezenta cartă trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți”.

2. RGPD

7. Articolul 2 alineatul (2) litera (d) din RGPD exclude din domeniul de aplicare al acestui regulament prelucrarea datelor cu caracter personal efectuată „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. În conformitate cu articolul 23 alineatul (1) litera (d) din RGPD:

„Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

[…]

(d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora.”

3. Directiva PNR

9. În continuare, vom oferi doar o scurtă prezentare a funcționării sistemului instituit prin Directiva PNR. Mai multe detalii cu privire la conținutul dispozițiilor din Directiva PNR relevantă pentru răspunsul la întrebările preliminare vor fi furnizate pe parcursul analizei juridice.

10. În conformitate cu articolul 1, Directiva PNR, adoptată în temeiul articolului 82 alineatul (1) litera (d) TFUE și al articolului 87 alineatul (2) litera (a) TFUE, organizează la nivelul Uniunii Europene un sistem pentru transferul de către transportatorii aerieni al datelor din PNR ale zborurilor extra-UE[6], precum și pentru colectarea, prelucrarea și stocarea acestor date de către autoritățile competente din statele membre în scopul combaterii terorismului și a infracțiunilor grave.

[6] În conformitate cu articolul 3 punctul 2 din Directiva PNR, prin „zbor extra-UE” se înțelege „orice zbor regulat sau neregulat al unui transportator aerian cu proveniența dintr-o țară terță și planificat să aterizeze pe teritoriul unui stat membru sau să decoleze de pe teritoriul unui stat membru și planificat să aterizeze într-o țară terță, inclusiv, în ambele cazuri, zboruri cu orice escală pe teritoriul statelor membre sau al țărilor terțe”.

11. În conformitate cu articolul 3 alineatul (5) din această directivă, „registrul cu numele pasagerilor" sau „PNR" este „un registru al cerințelor de călătorie ale fiecărui pasager, care conține informațiile necesare pentru a permite prelucrarea și controlul rezervărilor de către transportatorii aerieni care efectuează rezervările și de către cei participanți, pentru fiecare călătorie rezervată de către sau în numele oricărei persoane, indiferent că este conținut în sistemele de rezervare, în sistemele de control al plecărilor utilizat pentru verificarea pasagerilor la îmbarcarea în avion sau în sisteme echivalente care oferă aceleași funcționalități".

12. Anexa I la Directiva PNR (denumită în continuare „anexa I") enumeră datele din PNR, astfel cum au fost colectate de transportatorii aerieni, care fac obiectul unui transfer în sensul și potrivit modalităților prevăzute la articolul 8 din această directivă.

13. Anexa II la Directiva PNR (denumită în continuare „anexa II") conține lista infracțiunilor care constituie „infracțiuni grave" în sensul articolului 3 punctul 9 din această directivă.

14. Articolul 2 din Directiva PNR prevede posibilitatea ca statele membre să decidă să aplice această directivă și „zborurilor intra-UE"[7] sau unora dintre acestea, considerate „necesare" pentru urmărirea obiectivelor directivei menționate.

15. În conformitate cu articolul 4 alineatul (1) din Directiva PNR, „[f]iecare stat membru instituie sau desemnează o autoritate competentă pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave sau o filială a unei astfel de autorități, care să acționeze ca unitate de informații despre pasageri (UIP)". În conformitate cu alineatul (2) litera (a) al acestui articol 4, UIP este responsabilă în special de colectarea datelor din PNR de la transportatorii aerieni, de stocarea și prelucrarea acestor date, precum și de transferul datelor respective sau al rezultatului prelucrării acestora autorităților competente menționate la articolul 7 din Directiva PNR. În conformitate cu articolul 7 alineatul (2), aceste autorități sunt „autoritățile competente în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor de terorism sau a infracțiunilor grave"[8].

16. În conformitate cu articolul 6 alineatul (1) a doua teză din Directiva PNR, „[î]n cazul în care datele din PNR transferate de transportatorii aerieni includ date diferite față de cele enumerate în anexa I, UIP șterge aceste date imediat și definitiv la primirea lor". Alineatul (2) al acestui articol are următorul cuprins:

„(2) UIP prelucrează datele din PNR doar în următoarele scopuri:

(a) efectuarea unei evaluări a pasagerilor înainte de sosirea sau de plecarea programată a acestora din statul membru, în vederea identificării persoanelor care necesită o examinare suplimentară de către autoritățile competente menționate la articolul 7 și, după caz, de către Europol, în conformitate cu articolul 10, având în vedere faptul că respectivele persoane pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă;

[7] În conformitate cu articolul 3 alineatul (3) din Directiva PNR, constituie un „zbor intra-UE" „orice zbor regulat sau neregulat al unui transportator aerian cu proveniența de pe teritoriul unui stat membru și planificat să aterizeze pe teritoriul unuia sau mai multor state membre, fără escală pe teritoriul unei țări terțe".

[8] Articolul 7 alineatul (1) din Directiva PNR prevede că fiecare stat membru adoptă o listă a autorităților competente îndreptățite să solicite sau să primească date din PNR sau rezultatul prelucrării acestor datelor de la UIP în vederea examinării suplimentare a acestor informații sau a adoptării măsurilor necesare în vederea prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave. Această listă a fost publicată de Comisie în anul 2018 (JO 2018, C 194, p. 1; rectificare în JO 2020, C 366, p. 55).

(b) oferirea de răspunsuri, de la caz la caz, unei cereri temeinic justificate bazate pe motive suficiente din partea autorităților competente vizând furnizarea și prelucrarea datelor din PNR în cazuri specifice în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave și comunicarea rezultatelor acestei prelucrări autorităților competente sau, după caz, Europol; și

(c) analizarea datelor din PNR în vederea actualizării sau a definirii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în temeiul alineatului (3) litera (b) în scopul identificării oricăror persoane care pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă."

17. Articolul 12 din Directiva PNR conține dispozițiile privind păstrarea datelor din PNR.

18. Articolul 5 din Directiva PNR prevede că fiecare UIP numește un responsabil cu protecția datelor pentru monitorizarea prelucrării datelor din PNR și punerea în aplicare a garanțiilor relevante. În plus, fiecare stat membru trebuie, în conformitate cu articolul 15 din această directivă, să încredințeze autorității naționale de supraveghere menționate la articolul 25 din Decizia-cadru 2008/977/JAI [9], înlocuită prin 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 (denumită în continuare „Directiva privind poliția") [10], sarcina de a supraveghea aplicarea pe teritoriul său a dispozițiilor adoptate în temeiul directivei menționate. Această autoritate, care își îndeplinește sarcinile urmărind protejarea drepturilor fundamentale legate de prelucrarea datelor cu caracter personal [11], este în special responsabilă, pe de o parte, cu tratarea plângerilor depuse de orice persoană vizată, investigarea chestiunii și informarea persoanelor vizate cu privire la evoluția și la soluționarea plângerilor lor într-o perioadă de timp rezonabilă și, pe de altă parte, cu verificarea legalității prelucrării datelor, desfășurarea de investigații, inspecții și audituri în conformitate cu dreptul intern, fie din proprie inițiativă, fie pe baza unei plângeri [12].

4. Alte acte relevante de drept al Uniunii

19. Cadrul juridic al prezentei cauze este completat de Directiva API și de Directiva privind poliția. Din considerații de lizibilitate a prezentelor concluzii, conținutul dispozițiilor relevante din aceste acte va fi prezentat în măsura în care acest lucru este necesar pentru tratarea chestiunilor în cauză sau, într-un mod mai general, în scopul analizei juridice.

B. Dreptul belgian

20. În conformitate cu articolul 22 din Constituția Belgiei, „[o]rice persoană are dreptul la respectarea vieții sale private și de familie, cu excepția cazurilor și a condițiilor prevăzute de lege".

9 Decizia-cadru a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO 2008, L 350, p. 60).

10 JO 2016, L 119, p. 89. Articolul 25 din Decizia-cadru 2008/977/JAI a fost înlocuit de articolul 41 din Directiva privind poliția.

11 A se vedea articolul 15 alineatul (2) din Directiva PNR.

12 A se vedea articolul 15 alineatul (3) literele (a) și (b) din Directiva PNR.

21. Potrivit articolului său 2, Legea PNR transpune Directiva API și Directiva PNR, precum și, parțial, Directiva 2010/65/UE [13].

22. În conformitate cu articolul său 3 alineatul (1), Legea PNR „stabilește obligațiile transportatorilor și ale operatorilor de turism referitoare la transmiterea datelor pasagerilor care călătoresc spre, pleacă de pe sau tranzitează teritoriul național". Potrivit articolului 4 punctele 1 și 2 din această lege, prin „transportator" se înțelege „orice persoană fizică sau juridică care asigură, cu titlu profesional, transportul de persoane pe cale aeriană, maritimă, feroviară sau terestră", iar prin „operator de călătorie" se înțelege „orice organizator sau intermediar de călătorie în sensul legii din 16 februarie 1994 care gerează contractul de organizare a călătoriilor și contractul de intermediere a călătoriilor".

23. Articolul 8 din Legea PNR prevede:

„(1) Datele pasagerilor sunt prelucrate în scopul:

1. cercetării și urmăririi penale, inclusiv executarea pedepselor sau a măsurilor restrictive de libertate, referitoare la infracțiunile prevăzute la articolul 90 ter alineatul (2) punctele 7, 8, 11, 14, 17, 18 și 19 și alineatul (3) din Codul de procedură penală;

2. cercetării și urmăririi penale, inclusiv executarea pedepselor sau a măsurilor restrictive de libertate, referitoare la infracțiunile prevăzute la articolul 196, în ceea ce privește infracțiunile de fals în înscrisuri autentice și oficiale, la articolele 198, 199, 199bis, 207, 213, 375 și 505 din Codul penal;

3. prevenirii tulburărilor grave ale siguranței publice în cadrul radicalizării violente prin monitorizarea fenomenelor și a asocierilor în vederea săvârșirii de infracțiuni, în conformitate cu articolul 44/5 alineatul (1) punctele 2 și 3 și alineatul (2) din Legea din 5 august 1992 privind poliția;

4. monitorizării activităților prevăzute la articolul 7 punctele 1 și 3/1 și la articolul 11 alineatul (1) punctele 1-3 și 5 din Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate [14];

5. cercetării și urmăririi penale a infracțiunilor prevăzute la articolul 220 alineatul (2) din Legea generală privind taxele vamale și accizele din 18 iulie 1977 și la articolul 45 alineatul (3) din Legea din 22 decembrie 2009 privind regimul general al accizelor […].

(2) În condițiile prevăzute în capitolul 11, datele pasagerilor sunt prelucrate de asemenea în scopul îmbunătățirii controlului persoanelor la frontierele externe și al combaterii imigrației ilegale."

24. Articolul 9 din Legea PNR conține lista datelor care fac obiectul transferului. Aceste date corespund celor enumerate în anexa I.

13 Directiva Parlamentului European și a Consiliului din 20 octombrie 2010 privind formalitățile de raportare aplicabile navelor la sosirea în și/sau la plecarea din porturile statelor membre și de abrogare a Directivei 2002/6/CE (JO 2010, L 283, p. 1).

14 *Moniteur belge* din 18 decembrie 1998, p. 40312.

25. În conformitate cu articolul 18 din Legea PNR, „datele privind pasagerii sunt păstrate în banca de date privind pasagerii pentru o perioadă maximă de cinci ani începând de la înregistrarea lor. La finalul acestei perioade, ele sunt distruse.”

26. Articolul 19 din Legea PNR prevede că, „la expirarea unei perioade de șase luni de la înregistrarea datelor privind pasagerii în baza de date privind pasagerii, toate datele privind pasagerii sunt depersonalizate, prin ocultarea elementelor informative”.

27. Articolul 24 din Legea PNR prevede:

„(1) Datele pasagerilor sunt prelucrate în vederea efectuării unei evaluări prealabile a pasagerilor înainte de sosirea, plecarea sau tranzitul lor prevăzut pe teritoriul național, pentru a stabili care sunt persoanele care trebuie supuse unei examinări mai aprofundate.

(2) În contextul obiectivelor menționate la articolul 8 alineatul (1) punctele 1, 4 și 5 sau în legătură cu amenințările menționate la articolul 8 punctul 1 literele (a), (b), (c), (d), (f), (g) și la articolul 11 alineatul (2) din Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate, evaluarea prealabilă a pasagerilor se bazează pe o corespondență pozitivă, care rezultă dintr-o corelare a datelor pasagerilor cu:

1. bazele de date gestionate de serviciile competente sau care le sunt direct disponibile sau accesibile în contextul sarcinilor acestora sau cu liste de persoane întocmite de serviciile competente în contextul sarcinilor ce le revin.

2. criteriile de evaluare prestabilite de UIP, menționate la articolul 25.

(3) În contextul scopurilor menționate la articolul 8 alineatul (1) punctul 3, evaluarea prealabilă a pasagerilor se bazează pe o corespondență pozitivă, rezultată în urma corelării datelor pasagerilor cu bazele de date menționate la alineatul (2) punctul 1 […]”

28. Articolul 25 din Legea PNR reia conținutul articolului 6 alineatul (4) din Directiva PNR.

29. Capitolul 11 din Legea PNR conține dispozițiile care reglementează prelucrarea datelor pasagerilor în vederea îmbunătățirii controlului la frontiere și a combaterii imigrației ilegale. Aceste dispoziții constituie transpunerea în dreptul belgian a Directivei API.

30. Articolul 44 din Legea PNR prevede că UIP desemnează un responsabil cu protecția datelor în cadrul serviciului public federal de interne. Supravegherea punerii în aplicare a dispozițiilor Legii PNR este asigurată de Comisia pentru protecția vieții private.

31. Articolul 51 din Legea PNR modifică Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate prin introducerea articolului 16/3, formulat după cum urmează:

„(1) Serviciile de informații și de securitate pot decide, motivând corespunzător, să acceseze, în interesul exercitării misiunilor lor, datele pasagerilor prevăzute la articolul 7 din Legea [PNR].

(2) Decizia menționată la alineatul (1) este adoptată de șeful serviciului și comunicată în scris unității de informare a pasagerilor menționate la capitolul 7 din legea menționată anterior. Decizia se notifică Comitetului permanent R, împreună cu motivele acesteia.

Comitetul permanent R interzice serviciilor de informații și de securitate să exploateze datele colectate în condiții care nu respectă cerințele legale.

Decizia se poate referi la un set de date pentru o anumită investigație de informații. În acest caz, lista consultărilor privind datele referitoare la pasageri este comunicată o dată pe lună Comitetului permanent R."

C. Litigiul principal, întrebările preliminare și procedura în fața Curții

32. Printr-o cerere introductivă adresată către Cour constitutionnelle (Curtea Constituțională) la 24 iulie 2017, LDH a introdus o acțiune în anularea în tot sau în parte a Legii PNR. În susținerea acțiunii, aceasta a invocat două motive.

33. Prin intermediul primului motiv, invocat cu titlu principal și întemeiat pe încălcarea articolului 22 din Constituția Belgiei coroborat cu articolul 23 din RGPD, cu articolele 7, 8 și 52 alineatul (1) din cartă, precum și cu articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, semnată la Roma la 4 noiembrie 1950 (denumită în continuare „CEDO"), LDH consideră că legea atacată nu respectă principiul proporționalității în ceea ce privește domeniul său de aplicare și categoriile de date vizate, prelucrarea datelor pe care o introduce, obiectivele sale și durata conservării datelor. În special, aceasta susține că definiția datelor din PNR este prea largă și poate conduce la divulgarea unor date sensibile și că definiția noțiunii de „pasager" din această lege permite prelucrarea sistematică și neselectivă a datelor tuturor pasagerilor în cauză. În plus, LDH consideră că Legea PNR nu definește suficient de clar natura și modalitățile metodei de *pre-screening* al bazelor de date ale pasagerilor și ale criteriilor utilizate ca „indicatori de amenințare". În sfârșit, aceasta consideră că Legea PNR depășește limitele strictului necesar, întrucât urmărește obiective de prelucrare a datelor mai extinse decât cele permise de Directiva PNR, iar termenul de cinci ani pentru conservarea datelor din PNR este disproporționat. Prin intermediul celui de al doilea motiv, invocat în subsidiar și întemeiat pe încălcarea articolului 22 din Constituția Belgiei coroborat cu articolul 3 alineatul (2) TUE și cu articolul 45 din cartă, LDH contestă dispozițiile capitolului 11 din Legea PNR, care transpun Directiva API.

34. Consiliul de miniștri al Regatului Belgiei, în calitate de parte intervenientă la Cour constitutionnelle (Curtea Constituțională), se opune acțiunii asociației LDH, contestând atât admisibilitatea, cât și temeinicia celor două motive invocate în susținerea acesteia.

35. La rândul său, Cour constitutionnelle (Curtea Constituțională) prezintă următoarele considerații.

36. În ceea ce privește primul motiv, aceasta ridică, în primul rând, problema dacă definiția datelor din PNR, prevăzută în anexa I, este suficient de clară și precisă. Descrierea unora dintre aceste date are un caracter exemplificativ și neexhaustiv. În continuare, instanța menționată subliniază că definiția noțiunii de „pasager" de la articolul 3 alineatul (4) din această directivă determină colectarea, transferul, prelucrarea și stocarea datelor din PNR ale oricărei persoane transportate sau care urmează să fie transportată și înscrise pe lista pasagerilor, independent de existența unor motive serioase pentru a considera că persoana în cauză a săvârșit o infracțiune sau este pe punctul de a săvârși o infracțiune ori a fost considerată vinovată de săvârșirea unei infracțiuni. În ceea ce privește prelucrarea datelor din PNR, aceasta observă că ele fac în mod sistematic obiectul unei evaluări prealabile care implică confruntarea datelor din PNR ale tuturor pasagerilor cu baze de date sau cu criterii prestabilite, în vederea stabilirii unor corespondențe. Cu

toate acestea, Cour constitutionnelle (Curtea Constituțională) precizează că, deși criteriile trebuie să fie specifice, fiabile și nediscriminatorii, pare imposibil din punct de vedere tehnic să se definească în mod suplimentar criteriile prestabilite care vor fi utilizate pentru a determina profilurile de risc. În ceea ce privește perioada de păstrare a datelor din PNR prevăzută la articolul 12 alineatul (1) din Directiva PNR, potrivit căruia aceste date pot fi păstrate pentru o perioadă de cinci ani, instanța de trimitere consideră că datele din PNR sunt păstrate fără a se ține seama dacă s-a constatat sau nu în cadrul evaluării prealabile că pasagerii în cauză pot prezenta un risc pentru siguranța publică. În aceste condiții, instanța de trimitere ridică problema dacă, având în vedere jurisprudența derivată în special din Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții [15] și Avizul 1/15 (Acordul PNR Canada-UE) din 26 iulie 2017 [16], se poate considera că sistemul de colectare, transfer, prelucrare și păstrare a datelor din PNR stabilit de Directiva PNR nu depășește limitele strictului necesar. În acest context, instanța menționată solicită de asemenea să se stabilească dacă Directiva PNR se opune unei reglementări naționale precum cea rezultată din articolul 8 alineatul (1) punctul 4 din Legea PNR, care autorizează prelucrarea datelor din PNR în alte scopuri decât cele prevăzute de această directivă. În sfârșit, aceasta solicită să se stabilească dacă UIP poate fi considerată „o altă autoritate națională” care poate, în temeiul articolului 12 alineatul (3) litera (b) punctul (ii) din Directiva PNR, să autorizeze dezvăluirea tuturor datelor din PNR după o perioadă de șase luni. În ceea ce privește al doilea motiv, instanța de trimitere arată că acesta este îndreptat împotriva articolului 3 alineatul (1), articolului 8 alineatul (2), precum și articolelor 28-31 din Legea PNR, care reglementează colectarea și prelucrarea datelor pasagerilor în scopul combaterii imigrației ilegale și al îmbunătățirii controalelor la frontiere. Reamintind faptul că, potrivit primei dintre aceste dispoziții, legea menționată privește zborurile care călătoresc spre, pleacă de pe sau tranzitează teritoriul național, această instanță precizează că legiuitorul național a inclus zborurile „intra-UE” în domeniul de aplicare al acestei legi pentru a obține „o imagine mai completă a pasagerilor care reprezintă o amenințare potențială la adresa securității [în interiorul Uniunii] și naționale”, invocând posibilitatea prevăzută la articolul 2 din Directiva PNR coroborat cu considerentul (10) al acesteia.

37. În acest context, Cour constitutionnelle (Curtea Constituțională) a decis să suspende judecarea cauzei și a adresat Curții următoarele întrebări preliminare:

„1) Articolul 23 din [RGPD] coroborat cu articolul 2 alineatul (2) litera (d) din același regulament trebuie interpretat în sensul că se aplică unei legislații naționale precum Legea [PNR], care transpune Directiva [PNR], precum și Directiva [API] și Directiva [2010/65]?

2) Anexa I […] este compatibilă cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din [cartă] în măsura în care datele pe care aceasta le enumeră sunt foarte largi – în special datele prevăzute la punctul 18 din [această anexă], care depășesc datele prevăzute la articolul 3 alineatul (2) din Directiva [API] – și în sensul că, coroborate, acestea ar putea să intre sub incidența datelor sensibile și, astfel, să încalce limitele «strictului necesar»?

3) Punctele 12 și 18 din anexa I […] sunt compatibile cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din [cartă] în măsura în care, având în vedere termenul «inclusiv», datele pe care le vizează sunt menționate cu titlu exemplificativ, iar nu exhaustiv, astfel încât cerința preciziei și a clarității normelor care implică o ingerință în dreptul la respectarea vieții private și în dreptul la protecția datelor cu caracter personal nu ar fi respectată?

[15] C-203/15 și C-698/15, denumită în continuare „Hotărârea Tele2 Sverige”, EU:C:2016:970.

[16] Denumit în continuare „Avizul 1/15”, EU:C:2017:592.

4) Articolul 3 punctul 4 din Directiva [PNR] și anexa I […] sunt compatibile cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din [cartă] în măsura în care sistemul de colectare, de transfer și de prelucrare generalizate ale datelor pasagerilor pe care aceste dispoziții îl instituie privește orice persoană care utilizează mijlocul de transport respectiv, independent de orice element obiectiv care să permită să se considere că această persoană poate prezenta un risc pentru securitatea publică?

5) Articolul 6 din Directiva [PNR] coroborat cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din [cartă] trebuie interpretat în sensul că se opune unei legislații naționale precum legea atacată, care admite, ca scop al prelucrării datelor din PNR, monitorizarea activităților vizate de serviciile de informații și de securitate, integrând astfel acest scop în prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave?

6) Articolul 6 din Directiva [PNR] este compatibil cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din [cartă] în măsura în care evaluarea prealabilă organizată de acesta, printr-o corelare cu bănci de date și criterii prestabilite, se aplică în mod sistematic și generalizat datelor privind pasagerii, independent de orice element obiectiv care să permită să se considere că acești pasageri pot prezenta un risc pentru securitatea publică?

7) Noțiunea de «altă autoritate națională competentă», prevăzută la articolul 12 alineatul (3) din Directiva [PNR], poate fi interpretată în sensul că vizează UIP creată prin Legea [PNR], care ar putea, prin urmare, să autorizeze accesul la datele din PNR după o perioadă de șase luni, în cadrul unor cercetări care vizează informații specifice?

8) Articolul 12 din Directiva [PNR] coroborat cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din [cartă] trebuie interpretat în sensul că se opune unei legislații naționale precum legea atacată, care prevede un termen general de păstrare a datelor de cinci ani, fără a distinge dacă reiese, în cadrul evaluării prealabile, că pasagerii vizați pot sau nu să prezinte un risc pentru securitatea publică?

9) a) Directiva [API] este compatibilă cu articolul 3 alineatul (2) [TUE] și cu articolul 45 din [cartă] în măsura în care obligațiile pe care aceasta le instituie se aplică zborurilor din interiorul [Uniunii]?

   b) Directiva [API] coroborată cu articolul 3 alineatul (2) [TUE] și cu articolul 45 din [cartă] trebuie interpretată în sensul că se opune unei legislații naționale precum legea atacată, care, în scopul combaterii imigrației ilegale și al îmbunătățirii controlului la frontiere, autorizează un sistem de colectare și de prelucrare a datelor pasagerilor «care călătoresc spre, pleacă de pe sau tranzitează teritoriul național», ceea ce ar putea implica în mod indirect o restabilire a controalelor la frontierele interne?

10) În cazul în care, pe baza răspunsurilor date la întrebările preliminare care precedă, Cour constitutionnelle (Curtea Constituțională) ajunge la concluzia că legea atacată, care transpune printre altele Directiva [PNR], încalcă una sau mai multe dintre obligațiile care decurg din dispozițiile menționate în aceste întrebări, ar putea să mențină provizoriu efectele Legii [PNR] pentru a evita o insecuritate juridică și pentru a permite ca datele colectate și păstrate anterior să mai poată fi utilizate în scopurile prevăzute de [această] lege?”

38. Au prezentat observații scrise, în temeiul articolului 23 din Statutul Curții de Justiție a Uniunii Europene, LDH, guvernele belgian, ceh, danez, german, estonian, irlandez, spaniol, francez, cipriot, leton, neerlandez, austriac, polonez, finlandez, precum și Parlamentul European, Consiliul Uniunii Europene și Comisia Europeană. În conformitate cu articolul 24 din Statutul Curții de Justiție a Uniunii Europene, Comisia, Autoritatea Europeană pentru Protecția Datelor (AEPD) și Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA) au fost invitate să răspundă în scris la întrebările adresate de Curte. La 13 iulie 2021 a avut loc o ședință de audiere a pledoariilor.

III. Analiză

A. Cu privire la prima întrebare preliminară

39. Prin intermediul primei întrebări preliminare, instanța de trimitere solicită în esență Curții să stabilească dacă articolul 2 alineatul (2) litera (d) din RGPD trebuie interpretat în sensul că acest regulament, în special articolul 23 alineatul (1), în temeiul căruia dreptul Uniunii sau dreptul statelor membre pot restricționa, prin intermediul unor măsuri legislative, pentru motive enumerate în mod exhaustiv, întinderea obligațiilor și a drepturilor prevăzute de regulamentul respectiv, se aplică prelucrării datelor efectuate în temeiul unei reglementări naționale precum Legea PNR care transpune în dreptul intern Directiva PNR, precum și Directiva API și Directiva 2010/65.

40. Articolul 2 alineatul (2) din RGPD prevede excepții de la domeniului material de aplicare al acestui regulament, care are o definiție foarte largă [17], astfel cum este prevăzută la articolul 2 alineatul (1) [18]. Ca derogări de la aplicarea unei reglementări care guvernează prelucrarea datelor cu caracter personal care poate afecta libertățile fundamentale, aceste excepții trebuie să fie de strictă interpretare [19].

41. Articolul 2 alineatul (2) litera (d) din RGPD conține, printre altele, o clauză de excludere potrivit căreia acest regulament nu se aplică prelucrării datelor cu caracter personal „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”. Această clauză de excludere se bazează pe un criteriu dublu, subiectiv și obiectiv. Astfel, este exclusă din domeniul de aplicare al regulamentului menționat prelucrarea datelor efectuată, în primul rând, de către „autoritățile competente” și, în al doilea rând, în scopurile enumerate în această dispoziție. În consecință, trebuie evaluate diferitele tipuri de prelucrare a datelor reglementate de Legea PNR, în raport cu acest criteriu dublu.

17 A se vedea în acest sens Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504, punctul 61).

18 În conformitate cu articolul 2 alineatul (1) din RGPD, „[p]rezentul 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”.

19 A se vedea Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems (C-311/18, EU:C:2020:559, punctul 84), precum și Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504, punctul 62).

42. În ceea ce privește, în primul rând, prelucrările de date efectuate de transportatorii (aerieni, feroviari, tereștri și navali) către UIP sau de operatorii de turism *în scopul prestării de servicii sau în scopuri comerciale*, în măsura în care intră sub incidența legii menționate, rămân reglementate de RGPD, având în vedere că nu este îndeplinită nici componenta subiectivă și nici cea obiectivă a criteriului de excludere prevăzut la articolul 2 alineatul (2) litera (d) din acest regulament.

43. În ceea ce privește, în al doilea rând, *transferul de date din PNR de către transportatori sau operatorii de turism către UIP*, care constituie în sine o „prelucrare" în sensul articolului 4 punctul 2 din RGPD [20], includerea sa în domeniul de aplicare al RGPD este mai puțin evidentă.

44. Într-adevăr, pe de o parte, acest transfer nu este efectuat de o „autoritate competentă" în sensul articolului 3 punctul 7 din Directiva privind poliția, la care ar trebui să se facă trimitere prin analogie, în lipsa unei definiții a acestei noțiuni în RGPD [21]. Un operator economic, precum o companie de transport sau o agenție de turism, care are numai obligația legală de a transfera date cu caracter personal și căruia nu i-a fost încredințată nicio prerogativă de autoritate publică [22], nu poate fi considerat un organism sau o entitate în sensul articolului 3 punctul 7 litera (b) menționat [23].

45. Pe de altă parte, transferul de date din PNR de către companiile de transport și operatorii de turism este efectuat pentru a îndeplini o obligație impusă prin lege pentru a permite urmărirea obiectivelor enumerate la articolul 2 alineatul (2) litera (d) din RGPD.

46. Or, în opinia noastră, rezultă în mod clar din formularea acestei dispoziții că numai operațiunile de prelucrare care corespund atât componentei subiective, cât și celei obiective ale criteriului de excludere prevăzut de aceasta se situează în afara domeniului de aplicare al RGPD. În consecință, transferul de date din PNR către UIP impus de Legea PNR societăților de transport și operatorilor de turism intră sub incidența acestui regulament.

47. În ceea ce privește dispozițiile din Legea PNR care transpun Directiva PNR, această concluzie este susținută de articolul 21 alineatul (2) din directiva respectivă, care prevede că aceasta „nu aduce atingere aplicabilității Directivei 95/46/CE [24] în ceea ce privește prelucrarea datelor cu caracter personal de către transportatorii aerieni". În opinia noastră, trebuie respinsă

20 A se vedea în acest sens Hotărârea din 6 octombrie 2020, Privacy International (C-623/17, denumită în continuare „Hotărârea Privacy International", EU:C:2020:790, punctul 41 și jurisprudența citată). În conformitate cu articolul 4 punctul 2 din RGPD, constituie o „prelucrare" „orice operațiune […] efectuat[ă] asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal […] cum ar fi […] divulgarea prin transmitere […]".

21 A se vedea în acest sens Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504, punctul 69). În conformitate cu articolul 3 punctul 7 literele (a) și (b) din Directiva privind poliția, o „autoritate competentă" este „(a) orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau (b) orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice" în aceleași scopuri.

22 Nu rezultă niciun indiciu în acest sens din decizia de trimitere.

23 Nici un astfel de operator nu poate fi calificat drept „persoană împuternicită de operator" în sensul articolului 4 punctul 8 din RGPD sau al articolului 3 punctul 9 din Directiva privind poliția, acesta fiind mai degrabă „operator" în sensul articolului 4 punctul 7 a doua teză din RGPD. În conformitate cu articolul 4 punctul 8 din RGPD și cu articolul 3 punctul 9 din Directiva privind poliția, care sunt formulate în mod identic, „persoană împuternicită de operator" este „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului". În conformitate cu articolul 4 punctul 7 prima teză din RGPD, un „operator" este „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care […] stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal", a doua teză a acestei dispoziții precizează că, „atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern".

24 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). Această directivă a fost abrogată și înlocuită de RGPD; a se vedea articolul 94 din acest regulament.

interpretarea acestei dispoziții propusă în special de guvernul francez, potrivit căreia aceasta prevede numai că transportatorii rămân supuși obligațiilor prevăzute de RGPD pentru prelucrarea datelor care nu sunt prevăzute de Directiva PNR. Într-adevăr, având în vedere formularea sa, domeniul de aplicare al acestei „clauze de neprejudiciere" este unul extins și definit numai prin raportare la autorul prelucrării, fără a se face nicio mențiune cu privire la scopul prelucrării sau la cadrul în care aceasta se desfășoară, fie că este vorba despre exercitarea activității comerciale a transportatorului aerian sau despre îndeplinirea unei obligații legale. Observăm de asemenea că o clauză cu un conținut identic se regăsește la articolul 13 alineatul (3) din Directiva PNR, care face referire în mod specific la obligațiile transportatorilor aerieni în temeiul RGDP „de a lua măsuri tehnice și organizatorice adecvate pentru a proteja securitatea și confidențialitatea datelor cu caracter personal". Or, această dispoziție este prevăzută printre cele care organizează protecția datelor cu caracter personal prelucrate în temeiul Directivei PNR și urmează după articolul 13 alineatul (1) din această directivă, care supune, în mod general, orice prelucrare de date efectuată în temeiul acesteia dispozițiilor Deciziei-cadru 2008/977, care sunt menționate în aceasta. Contrar celor susținute de guvernul francez, un astfel de aranjament legislativ permite, pe de o parte, interpretarea articolului 13 alineatul (3) menționat drept o clauză care plasează sub incidența RGPD doar prelucrarea de date prevăzută de Directiva PNR, care nu este efectuată de „autoritățile competente" în sensul Directivei privind poliția, și, pe de altă parte, interpretarea referinței la respectarea obligațiilor impuse de acest regulament în materie de securitate și de confidențialitate a datelor drept o reiterare a garanțiilor care trebuie să însoțească în mod obligatoriu transferul de către transportatori al datelor din PNR către UIP.

48. Concluzia enunțată la punctul 46 din prezentele concluzii nu este repusă în discuție de considerentul (19) al RGPD și de considerentul (11) al Directivei privind poliția, la care fac referire, printre altele, guvernele german, irlandez și francez, pentru a susține caracterul de *lex specialis* al Directivei PNR. În această privință, este adevărat, desigur, că această directivă stabilește, pentru prelucrarea datelor cu caracter personal pe care o vizează, un cadru de protecție a acestor date care este autonom în raport cu cel al RGPD. Cu toate acestea, acest cadru specific se aplică numai prelucrării datelor din PNR efectuate de „autoritățile competente", în sensul articolului 3 punctul 7 din Directiva privind poliția, care include în special UIP-urile, în timp ce transferul de date din PNR către UIP-uri face în continuare obiectul cadrului general stabilit de RGPD, în temeiul, printre altele, al „clauzei de neprejudiciere" prevăzute la articolul 21 alineatul (2) din Directiva PNR.

49. În sprijinul afirmației acestora potrivit căreia RGPD nu se aplică transferului de către transportatorii și operatorii de turism al datelor din PNR către UIP, guvernele belgian, irlandez, francez și cipriot fac referire la Hotărârea din 30 mai 2006, Parlamentul/Consiliul și Comisia [25], în care Curtea a statuat că transferul de către transportatorii aerieni comunitari al datelor din PNR către autoritățile din Statele Unite ale Americii, în temeiul unui acord negociat între acest stat și Comunitatea Europeană, constituie o prelucrare de date cu caracter personal în sensul

[25] C-317/04 și C-318/04, denumită în continuare „Hotărârea Parlamentul/Consiliul", EU:C:2006:346. În cauzele în care a fost pronunțată această hotărâre, Parlamentul a solicitat, pe de o parte, anularea Deciziei 2004/496/CE a Consiliului din 17 mai 2004 privind încheierea unui acord între Comunitatea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor din PNR de către transportatorii aerieni către Biroul vamal și de protecție a frontierelor din cadrul Departamentului pentru Securitate Internă al Statelor Unite (JO 2004, L 183, p. 83, și rectificare în JO 2005, L 255, p. 168), și, pe de altă parte, anularea Deciziei 2004/535/CE a Comisiei din 14 mai 2004 privind nivelul adecvat de protecție a datelor cu caracter personal cuprinse în registrul cu numele pasagerilor transferat către Biroul vamal și de protecție a frontierelor din Statele Unite (JO 2004, L 235, p. 11).

articolului 3 alineatul (2) prima liniuță din Directiva 95/46 [26] și, prin urmare, nu se încadrează în domeniul de aplicare al acestei directive. Pentru a ajunge la această concluzie, Curtea a luat în considerare *scopul transferului*, precum și faptul că transferul „a făcut parte dintr-un cadru instituit de autoritățile publice", chiar dacă datele au fost colectate și transferate de operatori privați [27].

50. În această privință, este suficient să arătăm că în Hotărârea din 6 octombrie 2020, La Quadrature du Net și alții [28], Curtea a considerat în esență că Hotărârea Parlamentul/Consiliul nu poate fi transpusă în contextul RGPD [29].

51. Pe de altă parte, la punctul 102 din Hotărârea La Quadrature du Net [30], aplicând prin analogie raționamentul din Hotărârea Tele2 Sverige și din Hotărârea din 2 octombrie 2018, Ministerio Fiscal [31], Curtea a afirmat că, „deși [RGPD] precizează, la articolul 2 alineatul (2) litera (d), că acesta nu se aplică prelucrărilor efectuate «de către autoritățile competente» în scopul, printre altele, al prevenirii și depistării infracțiunilor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, din articolul 23 alineatul (1) literele (d) și (h) din același regulament reiese că prelucrările de date cu caracter personal efectuate de particulari în aceleași scopuri intră în domeniul de aplicare al acestuia" [32].

52. Pentru motivele deja dezvoltate, suntem convinși că concluzia potrivit căreia transferul de către societățile de transport și operatorii de turism al datelor din PNR către UIP intră sub incidența RGPD rezultă deja în mod clar din textul articolului 2 alineatul (2) litera (d) din RGPD, care face referire numai la operațiunile de prelucrare efectuate de „autoritățile competente", fără a fi nevoie să se facă referire la clauza de restricționare prevăzută la articolul 23 alineatul (1) din regulamentul menționat [33]. Cu toate acestea, afirmația de la punctul 102 din Hotărârea La Quadrature du Net constituie o luare de poziție clară a Curții în favoarea unei astfel de concluzii.

53. Întrucât transferul datelor din PNR de către companiile de transport și operatorii de turism intră în domeniul de aplicare al RGPD, o reglementare națională precum Legea PNR care obligă aceste companii și operatori să efectueze un astfel de transfer constituie o „măsură legislativă" în temeiul articolului 23 alineatul (1) litera (d) din RGPD și trebuie, în consecință, să îndeplinească condițiile prevăzute de această dispoziție [34].

26 Potrivit articolului 3 alineatul (2) prima liniuță din Directiva 95/46, această directivă nu se aplica prelucrării datelor cu caracter personal „puse în practică pentru exercitarea activităților din afara domeniului de aplicare al dreptului comunitar, cum ar fi cele prevăzute în titlurile V și VI din Tratatul privind Uniunea Europeană și, *în orice caz*, prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când aceste prelucrări sunt legate de probleme de securitate a statului) și activitățile statului în domeniul dreptului penal" (sublinierea noastră).

27 Cu privire la „abordarea teleologică" și „contextuală" a Curții în Hotărârea Parlamentul/Consiliul, a se vedea Concluziile avocatului general Campos Sánchez-Bordona prezentate în cauzele conexate La Quadrature du Net și alții (C-511/18 și C-512/18, EU:C:2020:6, punctele 47 și 62).

28 C-511/18, C-512/18 și C-520/18, denumită în continuare Hotărârea „La Quadrature du Net", EU:C:2020:791.

29 A se vedea Hotărârea La Quadrature du Net, punctele 100-102.

30 A se vedea în același sens Hotărârea Privacy International, punctul 47.

31 C-207/16, denumită în continuare „Hotărârea Ministerio Fiscal", EU:C:2018:788, punctul 34.

32 A se vedea prin analogie Hotărârea Tele2 Sverige, punctele 72-74, și Hotărârea Ministerio fiscal, punctul 34. Aceste hotărâri priveau interpretarea articolului 15 alineatul (1) prima teză 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) (JO 2002, L 201, p. 37, Ediție specială 13/vol. 36, p. 63), care prevede o clauză de limitare similară celei conținute la articolul 23 alineatul (1) literele (a)-(d) din RGPD.

33 O trimitere la articolul 15 alineatul (1) din Directiva 2002/58 a fost justificată în contextul acestei directive, având în vedere modul de redactare a clauzei de excludere de la articolul 1 alineatul (3) din aceasta, care face referire într-un mod general la „activități[e] statului în domeniul legii penale".

34 A se vedea prin analogie Hotărârea Privacy International, punctele 38 și 39.

54. În al treilea rând, în ceea ce privește prelucrarea datelor din PNR efectuată *de UIP și autoritățile naționale competente*, aplicabilitatea RGPD depinde, astfel cum rezultă din cele prezentate anterior, de obiectivele pe care aceste prelucrări le urmăresc.

55. Astfel, *primo*, prelucrările de date din PNR efectuată de UIP și de autoritățile naționale competente în scopurile enumerate la articolul 8 alineatul (1) punctele 1-3 și 5 din Legea PNR [35] sunt excluse din domeniul de aplicare al RGPD în măsura în care, astfel cum pare să fie cazul, scopurile menționate se numără printre cele acoperite de clauza de excludere de la articolul 2 alineatul (2) litera (d) din RGPD. Protecția datelor persoanelor vizate de aceste prelucrări ale datelor intră sub incidența dreptului național, sub rezerva aplicării Directivei privind poliția [36] și, în cadrul domeniului de aplicare al acesteia, a Directivei PNR.

56. Același lucru este valabil, *secundo*, în ceea ce privește prelucrarea datelor din PNR efectuată de UIP și de serviciile de securitate și de informații în contextul monitorizării activităților menționate în dispozițiile Legii organice privind serviciile de informații și de securitate enumerate la articolul 8 alineatul (1) punctul 4 din Legea PNR, în măsura în care acestea răspund scopurilor prevăzute la articolul 2 alineatul (2) litera (d) din RGPD, fapt a cărui apreciere revine instanței de trimitere.

57. Guvernul belgian susține că prelucrările efectuate în temeiul articolului 8 alineatul (1) punctul 4 din Legea PNR fac în orice caz obiectul clauzei de excludere prevăzute la articolul 2 alineatul (2) litera (a) din RGPD, precum și a celei prevăzute la articolul 2 alineatul (3) litera (a) din Directiva privind poliția, întrucât activitățile serviciilor de securitate și de informații nu intră în domeniul de aplicare al dreptului Uniunii.

58. În această privință, chiar dacă subliniem că Curtea nu este sesizată cu o chestiune privind interpretarea acestor dispoziții, observăm mai întâi că aceasta a statuat deja că o reglementare națională care impune operatorilor privați obligații de prelucrare intră în domeniul de aplicare al dispozițiilor dreptului Uniunii privind protecția datelor cu caracter personal, inclusiv atunci când vizează protecția securității naționale [37]. Rezultă că transferul de date din PNR la care sunt obligați prin Legea PNR transportatorii și operatorii de turism este, în principiu, reglementat de RGPD, chiar și atunci când este efectuat în temeiul articolului 8 alineatul (1) punctul 4 din această lege.

59. În continuare, observăm că, deși considerentul (16) al RGPD enunță că acesta nu se aplică „activității[or] privind securitatea națională”, iar considerentul (14) al Directivei privind poliția precizează că „activitățile privind securitatea națională, activitățile agențiilor sau ale unităților specializate pe probleme de securitate națională […] nu ar trebui să fie considerate activități care se încadrează în domeniul de aplicare al [acestei] directive”, criteriile pe baza cărora o prelucrare de date cu caracter personal efectuată de o autoritate, un serviciu sau o agenție publice ale unui stat membru intră în domeniul de aplicare al vreunui act de drept al Uniunii care organizează protecția persoanelor în cauză în ceea ce privește o astfel de prelucrare sau nu intră în domeniul de aplicare al dreptului respectiv au la bază un raționament legat atât de funcțiile atribuite autorității, serviciului sau agenției respective, cât și de scopurile prelucrării menționate. Astfel, Curtea a apreciat că articolul 2 alineatul (2) litera (a) din RGPD, interpretat în lumina considerentului (16) al acestui regulament, „trebuie considerat ca având ca unic obiectiv excluderea din domeniul de aplicare al regulamentului menționat a prelucrărilor de date cu caracter personal efectuate de autoritățile de stat în cadrul unei activități de apărare a securității

35 Este vorba despre prelucrările reglementate în capitolele 7-10 și 12 din Legea PNR.

36 A se vedea în acest sens Hotărârea La Quadrature du Net, punctul 103, și Hotărârea Privacy International, punctul 48.

37 A se vedea în special Hotărârea La Quadrature du Net.

naționale sau al unei activități care poate fi încadrată în aceeași categorie, astfel încât simplul fapt că o activitate este proprie statului sau unei autorități publice nu este suficient pentru ca această excepție să fie automat aplicabilă unei asemenea activități”[38]. Curtea a mai precizat că „activitățile care au ca scop apărarea securității naționale prevăzute la articolul 2 alineatul (2) litera (a) din RGPD cuprind în special […] activitățile care au ca obiect protejarea funcțiilor esențiale ale statului și a intereselor fundamentale ale societății”[39]. Rezultă de aici că, în cazul în care un stat membru ar încredința serviciilor sale de securitate și de informații sarcini în domeniile enumerate la articolul 3 punctul 7 litera (a) din Directiva privind poliția, prelucrarea datelor efectuată de serviciile respective pentru îndeplinirea acestor sarcini ar intra în domeniul de aplicare al acestei directive și, dacă este cazul, al Directivei PNR. Într-un mod mai general, observăm că, în cadrul interpretării articolului 4 alineatul (2) TUE, pe care se întemeiază, printre alții, guvernul belgian, Curtea a statuat în mod repetat că simplul fapt că o măsură națională a fost adoptată în vederea protejării securității naționale nu poate să determine inaplicabilitatea dreptului Uniunii și nici să absolve statele membre de necesitatea de a respecta acest drept[40], arătându-se astfel reticentă să excludă în mod automat și în bloc activitățile statelor membre legate de protecția securității naționale din domeniul de aplicare al dreptului Uniunii.

60. *Tertio*, în opinia tuturor părților interesate care au prezentat observații, cu excepția guvernului francez, este necesar să se considere că prelucrarea datelor din PNR efectuată de autoritățile competente belgiene în scopurile prevăzute la articolul 8 alineatul (2) din Legea PNR, și anume „îmbunătățir[ea] controlului persoanelor la frontierele externe și […] combater[ea] imigrației ilegale”[41], nu face obiectul clauzei de excludere prevăzute la articolul 2 alineatul (2) litera (d) din RGPD și nici al unei alte clauze de excludere prevăzute la acest articol și, prin urmare, intră în domeniul de aplicare al acestui regulament. Contrar celor susținute de guvernul francez, prelucrarea menționată nu poate fi reglementată nici de Directiva PNR, al cărei articol 1 alineatul (2) prevede că „[d]atele din PNR colectate în conformitate cu prezenta directivă pot fi prelucrate doar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave”, nici, în principiu, de Directiva privind poliția care, potrivit articolului 1 alineatul (1), se aplică numai prelucrării 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”. Astfel cum rezultă din decizia de trimitere, articolul 8 alineatul (2) și capitolul 11 din Legea PNR, care conțin dispozițiile privind prelucrarea datelor din PNR în vederea îmbunătățirii controlului la frontieră și a combaterii imigrației ilegale și care prevăd în acest scop transferul datelor respective de către UIP în special către serviciile de poliție responsabile cu controlul la frontieră, vizează transpunerea în dreptul belgian a Directivei API și a Directivei 2010/65. Or, aceste două directive impun autorităților competente să respecte dispozițiile Directivei 95/46 în ceea ce privește operațiunile de prelucrare pe care le prevăd[42]. Contrar celor susținute de guvernul francez, trimiterea la normele de protecție din această directivă trebuie interpretată în sensul că vizează toate prelucrările de date cu caracter personal efectuate în temeiul Directivei API și al Directivei 2010/65. Faptul că Directiva API este anterioară intrării în vigoare a Deciziei-cadru 2008/977 este irelevant în această privință, întrucât

38 A se vedea Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504, punctul 66).

39 A se vedea Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504).

40 A se vedea Hotărârea La Quadrature du Net, punctul 99 și jurisprudența citată.

41 Condițiile care încadrează această prelucrare a datelor sunt prevăzute în capitolul 11 din Legea PNR.

42 A se vedea considerentele (8), (9) și (12) și articolul 6 din Directiva API, precum și articolul 8 alineatul (2) din Directiva 2010/65.

decizia-cadru și Directiva privind poliția care a înlocuit-o vizează numai prelucrarea datelor cu caracter personal menționată la articolul 3 alineatul (1) din Directiva API, efectuată de autoritățile competente în scopul aplicării legii [43].

61. Pe baza tuturor considerațiilor menționate anterior, propunem Curții să răspundă la prima întrebare preliminară în sensul că articolul 23 din RGPD coroborat cu articolul 2 alineatul (2) litera (d) din acest regulament trebuie interpretat în sensul că:

– se aplică legislației naționale de transpunere a Directivei PNR în măsura în care această legislație reglementează prelucrarea datelor din PNR efectuată de transportatori și de alți operatori economici, inclusiv transferul datelor din PNR către UIP, prevăzut la articolul 8 din directiva menționată;

– nu se aplică legislației naționale de transpunere a Directivei PNR în măsura în care aceasta reglementează prelucrarea datelor efectuată în scopurile prevăzute la articolul 1 alineatul (2) din această directivă de către autoritățile naționale competente, inclusiv de UIP și, după caz, de serviciile de securitate și de informații ale statului membru în cauză;

– se aplică legislației naționale de transpunere a Directivei API și a Directivei 2010/65 în vederea îmbunătățirii controlului persoanelor la frontierele externe și în vederea combaterii imigrației ilegale.

B. Cu privire la a doua, a treia, a patra, a șasea și a opta întrebare preliminară

62. Prin intermediul celei de a doua, de a treia, de a patra și de a șasea întrebări preliminare, Cour constitutionnelle (Curtea Constituțională) solicită Curții să se pronunțe cu privire la validitatea Directivei PNR în raport cu articolele 7, 8 și 52 alineatul (1) din cartă. A opta întrebare preliminară, deși este formulată ca o întrebare de interpretare, urmărește, pe fond, tot pronunțarea de către Curte a unei hotărâri cu privire la validitatea acestei directive.

63. Aceste întrebări se referă la diferitele elemente ale sistemului de prelucrare a datelor din PNR instituit prin Directiva PNR și solicită, prin raportare la fiecare dintre aceste elemente, o apreciere a respectării condițiilor de legalitate a restricțiilor aduse exercitării drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă. Astfel, a doua și a treia întrebare preliminară vizează lista de date din PNR din anexa I, a patra întrebare privește definiția noțiunii de „pasager” menționată la articolul 3 punctul 4 din Directiva PNR, a șasea întrebare vizează utilizarea datelor din PNR în scopul evaluării prealabile în temeiul articolului 6 din această directivă, iar a opta întrebare se referă la termenul de păstrare a datelor din PNR prevăzut la articolul 12 alineatul (1) din această directivă.

1. Cu privire la drepturile fundamentale prevăzute la articolele 7 și 8 din cartă

64. Articolul 7 din cartă garantează dreptul oricărei persoane la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor. Articolul 8 alineatul (1) din cartă recunoaște în mod explicit dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc. Conform unei jurisprudențe constante, aceste drepturi, care se referă la orice informație privind

[43] Utilizarea informațiilor prealabile privind pasagerii (denumite în continuare „datele API”) de către autoritățile de aplicare a legii este prevăzută în mod expres la articolul 6 alineatul (1) ultimul paragraf din Directiva API.

o persoană fizică identificată sau identificabilă, sunt strâns legate, întrucât accesul la datele cu caracter personal ale unei persoane fizice în vederea stocării sau a utilizării lor afectează dreptul acestei persoane la respectarea vieții private [44].

65. Cu toate acestea, drepturile consacrate la articolele 7 și 8 din cartă nu sunt prerogative absolute, ci trebuie să fie luate în considerare în raport cu funcția lor în societate [45]. Astfel, articolul 8 alineatul (2) din cartă permite prelucrarea datelor cu caracter personal dacă sunt îndeplinite anumite condiții. Această dispoziție prevede că datele cu caracter personal trebuie prelucrate „în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege”.

66. Orice limitare a dreptului la protecția datelor cu caracter personal, precum și a dreptului la viață privată trebuie să respecte de asemenea cerințele articolului 52 alineatul (1) din cartă. Astfel, o asemenea limitare trebuie să fie prevăzută de lege, să respecte substanța acestor drepturi și, pentru a respecta principiul proporționalității, să fie necesară și să răspundă efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

67. Evaluarea unei măsuri de restrângere a acestor drepturi trebuie să țină seama și de importanța drepturilor consacrate la articolele 3, 4, 6 și 7 din cartă și de cea a obiectivelor de protejare a securității naționale și de combatere a infracționalității grave, contribuind la protecția drepturilor și libertăților celorlalți [46]. În această privință, articolul 6 din cartă consacră dreptul oricărei persoane nu numai la libertate, ci și la siguranță [47].

68. În plus, articolul 52 alineatul (3) din cartă urmărește să asigure coerența necesară între drepturile prevăzute de aceasta din urmă și drepturile corespunzătoare garantate de CEDO, care trebuie luate în considerare ca prag de protecție minimă [48]. Dreptul la respectarea vieții private și de familie, consacrat la articolul 7 din cartă, corespunde celui garantat la articolul 8 din CEDO și trebuie, în consecință, să i se recunoască același înțeles și aceeași întindere [49]. Rezultă din jurisprudența Curții Europene a Drepturilor Omului (denumită în continuare „Curtea EDO”) că o ingerință în drepturile garantate de acest articol poate fi justificată în temeiul alineatului (2) al articolului respectiv numai dacă este prevăzută de lege, dacă urmărește unul sau mai multe dintre scopurile legitime enumerate la alineatul respectiv și dacă este necesară într-o societate democratică pentru atingerea acestui scop sau a acestor scopuri [50]. De asemenea, măsura trebuie să fie compatibilă cu statul de drept, care este menționat în mod expres în preambulul CEDO și este inerent obiectului și scopului articolului 8 din aceasta [51].

44 A se vedea în acest sens în special Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems (C-311/18, EU:C:2020:559, punctul 170 și jurisprudența citată).

45 A se vedea în special Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems (C-311/18, EU:C:2020:559, punctul 172 și jurisprudența citată).

46 A se vedea în acest sens Hotărârea La Quadrature du Net, punctul 122.

47 A se vedea Hotărârea La Quadrature du Net, punctul 123.

48 A se vedea Hotărârea La Quadrature du Net, punctul 124 și jurisprudența citată.

49 A se vedea Hotărârea din 18 iunie 2020, Comisia/Ungaria (Transparența asociațiilor) (C-78/18, EU:C:2020:476, punctul 122 și jurisprudența citată).

50 A se vedea în special Curtea EDO, 4 decembrie 2015, Roman Zakharov împotriva Rusiei (CE:ECHR:2015:1204JUD004714306, punctul 227), Curtea EDO, 18 mai 2010, Kennedy împotriva Regatului Unit (CE:ECHR:2010:0518JUD002683905, punctul 130), și Curtea EDO, 25 mai 2021, Centrum för Rättvisa împotriva Suediei (CE:ECHR:2021:0525JUD003525208, punctul 246).

51 A se vedea Curtea EDO, 4 decembrie 2015, Roman Zakharov împotriva Rusiei, (CE:ECHR:2015:1204JUD004714306, punctul 228), Curtea EDO, 4 mai 2000, Rotaru împotriva României (CE:ECHR:2000:0504JUD002834195, punctul 52), Curtea EDO, 4 decembrie 2008, S. și Marper împotriva Regatului Unit (CE:ECHR:2008:1204JUD003056204, punctul 95), Curtea EDO, 18 mai 2021, Kennedy împotriva Regatului Unit (CE:ECHR:2010:0518JUD002683905, punctul 151), și Curtea EDO, 25 mai 2021, Centrüm för Rättvisa împotriva Suediei (CE:ECHR:2021:0525JUD003525208, punctul 246).

69. Acestea sunt principiile în lumina cărora trebuie examinate întrebările adresate de Cour constitutionnelle (Curtea Constituțională) privind aprecierea validității.

2. Cu privire la încălcarea drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă

70. Curtea a statuat deja că dispozițiile care impun sau permit comunicarea de date cu caracter personal ale unor persoane fizice unui terț precum o autoritate publică trebuie calificate, în lipsa consimțământului acestor persoane fizice și indiferent de utilizarea ulterioară a datelor în cauză, drept ingerințe în viața lor privată și, prin urmare, drept restrângere a dreptului fundamental garantat la articolul 7 din cartă, fără a aduce atingere eventualei lor justificări [52]. Acest lucru este valabil chiar în absența unor împrejurări care să permită calificarea unei astfel de ingerințe drept „gravă” și fără a fi relevant dacă informațiile vizate referitoare la viața privată au sau nu un caracter sensibil sau dacă persoanele interesate au suferit sau nu eventuale inconveniente ca urmare a acestei ingerințe [53]. Accesul autorităților publice la astfel de informații constituie de asemenea o ingerință în dreptul fundamental la protecția datelor cu caracter personal garantat la articolul 8 din cartă, întrucât constituie o prelucrare de date cu caracter personal [54]. În mod similar, păstrarea datelor referitoare la viața privată a unei persoane pentru o anumită perioadă reprezintă în sine o ingerință în drepturile garantate la articolele 7 și 8 din cartă [55].

71. Curtea a mai statuat deja că datele din PNR, precum cele enumerate în anexa I, conțin informații despre persoane fizice identificate, și anume pasagerii aerieni în cauză, și că, în consecință, diferitele modalități de prelucrare la care pot fi supuse aceste date afectează dreptul fundamental la respectarea vieții private, garantat la articolul 7 din cartă. Aceste modalități de prelucrare intră și în domeniul de aplicare al articolului 8 din cartă și, prin urmare, trebuie să îndeplinească în mod necesar cerințele de protecție a datelor prevăzute la acest articol [56].

72. Astfel, prelucrarea datelor din PNR permisă de Directiva PNR și în special, în măsura în care prezintă relevanță în prezenta cauză, transferul acestor date de către transportatorii aerieni către UIP, utilizarea lor de către aceste unități, transferul lor ulterior către autorități naționale competente, în sensul articolului 7 din această directivă, precum și păstrarea acestora constituie ingerințe în drepturile fundamentale garantate la articolele 7 și 8 din cartă.

73. În ceea ce privește gravitatea acestor ingerințe, trebuie amintit, în primul rând, că Directiva PNR prevede transferul *sistematic* și *continuu* către UIP al datelor din PNR, astfel cum este definit la articolul 3 punctul 4 din această directivă, ale oricărui pasager aerian care efectuează un zbor „extra-UE”, în sensul articolului 3 punctul 2 din directiva menționată. Un astfel de transfer presupune accesul general al UIP la toate datele din PNR comunicate [57]. Această constatare nu este repusă în discuție, contrar celor susținute de anumite state membre în prezenta procedură, prin faptul că, întrucât aceste date fac obiectul unei prelucrări automatizate, UIP vor avea acces

52 A se vedea printre altele Hotărârea din 18 iunie 2020, Comisia/Ungaria (C-78/18, EU:C:2020:476, punctele 124 și 126, precum și jurisprudența citată); a se vedea de asemenea Curtea EDO, 4 mai 2000, Rotaru împotriva României (CE:ECHR:2000:0504JUD002834195, punctul 48), Curtea EDO, 26 martie 1987, Leander împotriva Suediei (CE:ECHR:1987:0326JUD000924881, punctul 46), și Curtea EDO, 29 iunie 2006, Weber și Saravia împotriva Germaniei (CE:ECHR:2006:0629DEC005493400, punctul 79).

53 A se vedea printre altele Hotărârea Ministerio Fiscal, punctul 51 și jurisprudența citată.

54 A se vedea printre altele Hotărârea din 18 iunie 2020, Comisia/Ungaria (C-78/18, EU:C:2020:476, punctul 126), precum și Hotărârea Ministerio Fiscal, punctul 51 și jurisprudența citată.

55 A se vedea Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, denumită în continuare „Hotărârea Digital Rigts”, EU:C:2014:238, punctul 34).

56 A se vedea Avizul 1/15, punctele 121-123.

57 A se vedea prin analogie Hotărârea Privacy International, punctele 79 și 80, precum și jurisprudența citată.

în concret numai la datele a căror analiză a avut un rezultat pozitiv. Într-adevăr, pe de o parte, o astfel de împrejurare nu a împiedicat până în prezent Curtea să afirme, în contextul unor sisteme similare de prelucrare automatizată a datelor cu caracter personal colectate sau stocate „în bloc", caracterul general al accesului autorităților publice în cauză la astfel de date. Pe de altă parte, simpla punere la dispoziția autorităților publice a datelor cu caracter personal în vederea prelucrării și stocării lor de către aceste autorități implică *a priori* un acces general și complet al acestora la astfel de date și o ingerință în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal.

74. În al doilea rând, în conformitate cu articolul 2 alineatul (1) din Directiva PNR, statele membre pot decide să aplice această din urmă directivă zborurilor „intra-UE", în sensul articolului 3 punctul 3 din Directiva PNR. În această privință, observăm, pe de o parte, că Directiva PNR nu prevede doar opțiunea statelor membre de a extinde aplicarea sa la zborurile intra-UE, ci stabilește și condițiile formale și materiale care reglementează exercitarea acestei opțiuni [58] și precizează că, în cazul în care această opțiune este exercitată numai pentru anumite zboruri intra-UE, selectarea acestor zboruri trebuie să se facă ținând seama de obiectivele urmărite de directiva menționată [59]. Pe de altă parte, Directiva PNR stabilește consecințele exercitării unei astfel de opțiuni, prevăzând la articolul 2 alineatul (2) că, dacă un stat membru decide să aplice această directivă în cazul zborurilor intra-UE, toate dispozițiile directivei „se aplică zborurilor intra-UE ca și cum ar fi zboruri extra-UE și datelor din PNR de la zborurile intra-UE ca și cum ar fi date din PNR de la zboruri extra-UE".

75. În aceste împrejurări, considerăm, contrar opiniei mai multor guverne care au prezentat observații în prezenta procedură, că, deși aplicarea Directivei PNR în cazul zborurilor intra-UE depinde de alegerea statelor membre, temeiul juridic al ingerințelor în exercitarea drepturilor la respectarea vieții private și la protecția datelor cu caracter personal în legătură cu transferul, prelucrarea și păstrarea datelor din PNR referitoare la aceste zboruri îl constituie, în cazul în care se face o astfel de alegere, Directiva PNR.

76. Cu toate acestea, cu excepția Regatului Danemarcei, căruia nu îi este aplicabilă această directivă [60], aproape toate statele membre aplică regimul stabilit de directivă în cazul zborurilor „intra-UE" [61]. Rezultă că acest regim se aplică tuturor zborurilor având ca punct de sosire sau de plecare Uniunea și aproape tuturor zborurilor efectuate în interiorul Uniunii.

58 A se vedea articolul 2 alineatele (1)-(3) din Directiva PNR.

59 A se vedea articolul 2 alineatul (3) din Directiva PNR.

60 În conformitate cu articolele 1 și 2 din Protocolul (nr. 22) privind poziția Danemarcei, întrucât acest stat membru nu participă la adoptarea Directivei PNR, nu are obligații în temeiul acesteia și aceasta nici nu i se aplică [a se vedea considerentul (40) al acestei directive]. Cu toate acestea, rezultă din observațiile scrise depuse de guvernul danez că Regatul Danemarcei a adoptat în anul 2018 o lege privind colectarea, utilizarea și stocarea datelor din PNR, ale cărei dispoziții sunt în mare parte conforme cu cele ale Directivei PNR. În ceea ce privește Irlanda, rezultă din considerentul (39) al Directivei PNR că acest stat membru a notificat, în conformitate cu articolul 3 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, intenția sa de a participa la adoptarea și la aplicarea acestei directive.

61 Comisia a publicat o listă actualizată a statelor membre care au decis să aplice Directiva PNR în cazul zborurilor intra-UE menționate la articolul 2 din Directiva [PNR] (JO 2020, C 358, p. 7), rectificată în septembrie 2021 prin adăugarea Sloveniei și eliminarea trimiterii la Regatul Unit (JO 2021, C 360, p. 8). Irlanda și Austria nu sunt incluse în această listă. Raportul Comisiei către Parlamentul European și Consiliu referitor la revizuirea Directivei [PNR] din 24 iulie 2020, [COM(2020) 305 final, p. 11 (denumit în continuare „Raportul Comisiei din anul 2020")] menționează că toate statele membre, cu excepția unuia, au extins colectarea datelor din PNR în cazul zborurilor intra-UE.

77. În al treilea rând, în ceea ce privește datele din PNR care urmează să fie transferate, anexa I enumeră 19 rubrici care cuprind date biografice [62], detalii despre călătoria cu avionul [63] și alte date colectate în contextul contractului de transport aerian, cum ar fi numărul de telefon, adresa electronică, metodele de plată, agenția sau agentul de turism, informații privind bagajele și observații generale [64]. Or, astfel cum a afirmat Curtea la punctul 128 din Avizul 1/15, pronunțându-se cu privire la rubricile prevăzute în anexa la proiectul de Acord între Canada și Uniunea Europeană privind transferul și prelucrarea datelor din registrul cu numele pasagerilor (denumit în continuare „proiectul de Acord PNR Canada-UE"), care sunt formulate în linii mari în mod similar celor din anexa I, „chiar dacă anumite date din PNR, privite izolat, nu par să poată revela informații importante privind viața privată a persoanelor vizate, totuși, considerate în ansamblu, respectivele date pot revela, printre altele, un itinerar de călătorie complet, obiceiuri de călătorie, relațiile existente între două sau mai multe persoane, precum și informații privind situația financiară a pasagerilor aerieni, obiceiurile lor alimentare sau starea lor de sănătate și ar putea furniza chiar informații sensibile despre acești pasageri".

78. În al patrulea rând, potrivit articolului 6 din Directiva PNR, datele transferate de către transportatorii aerieni sunt menite a fi analizate de către UIP prin mijloace automatizate și aceasta *în mod sistematic*, altfel spus independent de aspectul dacă există cel mai mic indiciu că persoanele în cauză ar putea fi implicate în infracțiuni de terorism sau în infracțiuni grave. Mai exact, în contextul evaluării prealabile a pasagerilor prevăzute la articolul 6 alineatul (2) litera (a) din această directivă și în conformitate cu articolul 6 alineatul (3) din directivă, datele respective pot fi verificate confruntându-le cu baze de date „relevante" [articolul 6 alineatul (3) litera (a)] și prelucrate în raport cu anumite criterii prestabilite [articolul 6 alineatul (3) litera (b)]. Or, primul tip de prelucrare poate furniza informații suplimentare privind viața privată a persoanelor în cauză [65] și, în funcție de bazele de date utilizate pentru confruntare, poate chiar să facă posibilă elaborarea unui *profil exact* al acestor persoane. În aceste împrejurări, obiecția formulată de mai multe guverne, potrivit căreia Directiva PNR permite accesul numai la un set relativ limitat de date cu caracter personal, nu reflectă în mod adecvat amploarea potențială a ingerințelor pe care această directivă o implică în exercitarea drepturilor fundamentale protejate de articolele 7 și 8 din cartă, din punctul de vedere al sferei de date la care aceasta poate permite accesul. În ceea ce privește al doilea tip de prelucrare a datelor prevăzut la articolul 6 alineatul (3) litera (b) din Directiva PNR, reamintim că, la punctele 169 și 172 din Avizul 1/15, Curtea a subliniat că orice tip de analiză bazată pe criterii prestabilite conține în mod inerent o anumită marjă de eroare și în special un anumit număr de rezultate „fals pozitive". Conform cifrelor cuprinse în documentul de lucru al serviciilor Comisiei [66] (denumit în continuare „documentul de lucru din anul 2020"), anexat la raportul Comisiei din anul 2020, numărul cazurilor de rezultate pozitive care s-au dovedit a fi eronate în urma reexaminării individuale prevăzute la articolul 6 alineatul (5) din Directiva PNR este destul de substanțial și s-a ridicat, în anii 2018 și 2019, la cel puțin cinci din cele șase persoane identificate [67].

62 A se vedea în special punctele 4 și 18 din anexa I privind numele, sexul, data nașterii, cetățenia și documentele de identitate ale pasagerului.

63 A se vedea în special punctele 2, 3, 7, 13 și 18 din anexa I la Directiva PNR, care menționează, printre altele, numărul zborului, aeroporturile de plecare și de sosire, precum și datele și orele de plecare și de sosire.

64 A se vedea punctele 5, 6, 9, 12 și 16 din anexa I.

65 A se vedea în acest sens Avizul 1/15, punctul 131.

66 SWD(2020)128 final.

67 Documentul de lucru din anul 2020 (p. 28 și nota de subsol 55) menționează o rată de concordanțe pozitive de 0,59 % pentru anul 2019, din care numai 0,11 % au făcut obiectul unui transfer către autoritățile competente. Pentru anul 2018, procentele corespunzătoare au fost de 0,25 % și, respectiv, de 0,4 %.

79. În al cincilea rând, în conformitate cu articolul 12 alineatul (1) din Directiva PNR, datele din PNR sunt păstrate într-o bază de date la UIP pentru o perioadă de cinci ani după transferul lor către UIP a statului membru pe teritoriul căruia se situează punctul de sosire sau de plecare al zborului. Prin urmare, Directiva PNR permite ca informațiile privind viața privată a pasagerilor aerieni să fie disponibile o perioadă deosebit de lungă [68]. În plus, întrucât transferul de date din PNR vizează aproape toate zborurile având ca punct de plecare și de sosire Uniunea, precum și cele efectuate în cadrul acesteia, iar avionul a devenit un mijloc de transport destul de comun, datele personale ale unui număr semnificativ de pasageri aerieni ar putea fi practic păstrate permanent, pentru simplul fapt că se deplasează cu avionul de cel puțin două ori la fiecare cinci ani.

80. În sfârșit, la un nivel mai general, Directiva PNR prevede măsuri care, luate în considerare în ansamblu, vizează instituirea la nivelul Uniunii a unui sistem de supraveghere „nedirecționată", și anume care nu este declanșată pe baza unei suspiciuni privind una sau mai multe persoane anume, „masivă", în sensul că se exercită asupra datelor cu caracter personal ale unui număr mare de persoane [69], care acoperă în întregime aceeași categorie de persoane [70], și „proactivă", în măsura în care urmărește investigarea nu numai a amenințărilor cunoscute, ci și găsirea sau identificarea pericolelor necunoscute anterior [71]. Astfel de măsuri generează, prin însăși natura lor, ingerințe grave în exercitarea drepturilor fundamentale protejate la articolele 7 și 8 din cartă [72], legate în special de obiectivul lor preventiv și predictiv, care necesită evaluarea datelor cu caracter personal referitoare la segmente largi ale populației, scopul fiind acela de a „identifica" persoane care, în funcție de rezultatele acestei evaluări, ar trebui să facă obiectul unei examinări mai aprofundate din partea autorităților competente [73]. În plus, recurgerea tot mai răspândită la prelucrarea unor cantități mari de date cu caracter personal de diferite tipuri, colectate „în bloc", precum și corelarea și prelucrarea combinată a acestora, în scopul prevenirii anumitor infracțiuni grave, conduc la un „efect cumulativ" care amplifică gravitatea restricțiilor aduse drepturilor fundamentale la respectarea vieții private și la protecția datelor cu caracter personal și riscă să favorizeze un proces de alunecare treptată către o „societate de supraveghere" [74].

81. Pe baza tuturor considerațiilor menționate anterior, considerăm că ingerința pe care o are Directiva PNR în exercitarea drepturilor fundamentale protejate la articolele 7 și 8 din cartă trebuie calificată cel puțin ca fiind „gravă".

68 A se vedea Avizul 1/15, punctul 132.

69 Sistemul instituit de Directiva PNR putea să acopere, înainte de criza sanitară, până la un miliard de pasageri pe an, informații accesibile la adresa electronică https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table?lang=fr.

70 Și anume, orice persoană care se încadrează în noțiunea de „pasager", astfel cum este definită la articolul 3 punctul 4 din Directiva PNR, și care efectuează un „zbor extra-UE", precum și, *de facto*, un „zbor intra-UE".

71 Într-un studiu adoptat de Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția) în anul 2015, se consideră că astfel de măsuri se încadrează în noțiunea de „supraveghere strategică" și urmează o „tendință generală" de utilizare a „supravegherii proactive" a populației; a se vedea studiul *Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique*, adoptat de Comisia de la Veneția în cadrul celei de a 102-a sesiuni plenare (Veneția, 20 și 21 martie 2015), https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-f, punctul 61.

72 În ceea ce privește articolul 8 din CEDO, a se vedea Hotărârea Curții EDO, 25 mai 2021, Big Brother Watch și alții împotriva Regatului Unit (CE:ECHR:2021:0525JUD005817013, punctul 325, denumită în continuare „Hotărârea Big Brother Watch"), cu privire la măsurile de interceptare în masă, în care Curtea EDO afirmă că intensitatea ingerinței în exercitarea dreptului la viață privată a acestor măsuri crește pe măsură ce sunt depășite diferitele etape ale procesului, și anume interceptarea și păstrarea inițială a comunicațiilor și a datelor asociate, prelucrarea automatizată prin aplicarea unor elemente de selectare, examinarea de către analiști și păstrarea ulterioară a datelor, precum și utilizarea „produsului final".

73 A se vedea în acest sens considerentele (6) și (7) ale Directivei PNR; a se vedea, pentru o analiză aprofundată a scopului și a implicațiilor asupra vieții private și a protecției datelor cu caracter personal, raportul intitulat *Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards*, elaborat de Korff, D., cu contribuția lui Georges, M., https://rm.coe.int/16806a601b (denumit în continuare „Raportul Korff").

74 După cum se arată în raportul Korff, „PNR is not an isolated issue, but a new symptom of a much wider disease" [„PNR nu este o problemă izolată, ci un nou simptom al unei boli mult mai extinse"].

82. Este adevărat, astfel cum susține în special Comisia, că ansamblul de garanții și măsuri de protecție pe care îl prevede Directiva PNR, în special pentru a evita utilizarea abuzivă a datelor din PNR, poate reduce intensitatea sau gravitatea acestor ingerințe. Nu este mai puțin adevărat că orice regim care prevede accesul la datele cu caracter personal și prelucrarea acestora de către autoritățile publice prezintă un nivel de gravitate, din punctul de vedere al protecției drepturilor fundamentale afectate, care este inerent caracteristicilor sale obiective. În opinia noastră, acest nivel de gravitate trebuie determinat înainte de a trece, în contextul aprecierii proporționalității respectivelor ingerințe, la evaluarea suficienței și a caracterului adecvat al garanțiilor prevăzute de acest regim. Considerăm că acesta este modul în care Curtea a procedat până în prezent.

83. Pentru a fi compatibile cu carta, ingerințele în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal pe care le implică Directiva PNR trebuie să îndeplinească condițiile prevăzute la punctele 65 și 66 din prezentele concluzii, care vor fi examinate în continuare în limitele aspectelor care au fost supuse atenției Curții de către instanța de trimitere.

3. Cu privire la justificarea ingerinței care rezultă din Directiva PNR

84. În timp ce a treia întrebare vizează respectarea condiției prevăzute la articolul 52 alineatul (1) prima teză din cartă, potrivit căreia orice ingerință într-un drept fundamental trebuie să fie „prevăzută de lege”, a doua, a patra, a șasea și a opta întrebare preliminară ridică Curții în special problema respectării principiului proporționalității menționat în a doua teză a acestei dispoziții.

a) Cu privire la respectarea cerinței ca orice limitare a exercitării unui drept fundamental prevăzut de cartă să fie prevăzută de lege

85. Potrivit unei jurisprudențe constante a Curții[75], care se bazează pe jurisprudența Curții EDO[76], cerința ca orice restrângere a exercitării unui drept fundamental să fie „prevăzută de lege” nu se referă numai la originea „legală” a ingerinței – care nu este în discuție în prezenta cauză –, ci implică de asemenea ca temeiul juridic care permite această ingerință să definească el însuși întinderea ingerinței într-un mod *clar* și *exact*. Acest al doilea aspect al expresiei „prevăzută de lege”, atât în sensul articolului 52 alineatul (1) din cartă, cât și al articolului 8 alineatul (2) din cartă și al articolului 8 din CEDO, care vizează „calitatea legii” și, prin urmare, accesibilitatea și previzibilitatea măsurii în cauză[77], are ca scop nu doar asigurarea respectării principiului legalității și o protecție adecvată împotriva arbitrariului[78], ci răspunde de asemenea unui

75 A se vedea printre altele Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems (C-311/18, EU:C:2020:559, punctul 175), Hotărârea din 8 septembrie 2020, Recorded Artists Actors Performers (C-265/19, EU:C:2020:677, punctul 86 și jurisprudența citată), precum și Hotărârea Privacy International, punctul 65.

76 A se vedea printre altele Hotărârea Curții EDO din 8 iunie 2006, Lupsa împotriva României, (CE:ECHR:2006:0608JUD001033704, punctele 32 și 33), și Hotărârea Curții EDO din 15 decembrie 2020, Piskìn împotriva Turciei (CE:ECHR:2020:1215JUD003339918, punctul 206); a se vedea de asemenea Hotărârea Big Brother Watch, punctul 333. Cu privire la necesitatea de a da sintagmei „prevăzută de lege” de la articolul 52 alineatul (1) din cartă aceeași interpretare precum cea reținută de Curtea EDO, a se vedea Concluziile avocatului general Wathelet prezentate în cauza WebMindLicenses (C-419/14, EU:C:2015:606, punctele 134-143).

77 A se vedea în ultimul rând Hotărârea Big Brother Watch, punctul 333.

78 A se vedea Hotărârea din 17 decembrie 2015, WebMindLicenses (C-419/14, EU:C:2015:832, punctul 81); a se vedea de asemenea Curtea EDO, 1 iulie 2008, Liberty și alții împotriva Regatului Unit (CE:ECHR:2008:0701JUD005824300, punctul 69), precum și Hotărârea Big Brother Watch, punctul 333.

imperativ de securitate juridică. Această cerință este menționată și în Avizul din 19 august 2016 al Comitetului consultativ privind Convenția 108 [79] referitor la implicațiile prelucrării datelor pasagerilor asupra protecției datelor (denumit în continuare „Avizul din 19 august 2016”) [80].

86. Prin adoptarea Directivei PNR, legiuitorul Uniunii a limitat el însuși drepturile consacrate la articolele 7 și 8 din cartă. Prin urmare, ingerințele în exercitarea acestor drepturi permise de directiva menționată nu pot fi considerate ca fiind consecința unei opțiuni a statelor membre [81], în pofida marjei de apreciere de care acestea au putut beneficia la momentul transpunerii directivei în dreptul național, ci își are temeiul juridic chiar în Directiva PNR. În aceste condiții, îi revenea legiuitorului Uniunii sarcina de a adopta norme clare și exacte care să definească atât întinderea, cât și aplicarea măsurilor care implică ingerințele menționate, pentru a se conforma jurisprudenței amintite la punctul 86 din prezentele concluzii, precum și „standardelor ridicate” de protecție a drepturilor fundamentale cuprinse în special în cartă și în CEDO, la care face trimitere considerentul (15) al Directivei PNR.

87. Deși prin a treia întrebare preliminară instanța de trimitere ridică în mod expres problema respectării acestei obligații în raport cu punctele 12 și 18 din anexa I, analiza celei de a doua, a celei de a patra și a celei de a șasea întrebări preliminare, prin care instanța de trimitere exprimă îndoieli cu privire la caracterul necesar al ingerințelor pe care le implică Directiva PNR în exercitarea drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă, va necesita de asemenea o luare de poziție cu privire la caracterul suficient de clar și de precis al dispozițiilor în cauză din Directiva PNR.

88. Chiar dacă această analiză are legătură, astfel cum am arătat la punctul 85 din prezentele concluzii, cu legalitatea ingerinței, în sensul articolului 52 alineatul (1) prima teză din cartă, o vom realiza în contextul examinării proporționalității sale, menționată în a doua teză a acestui alineat, în conformitate cu abordarea urmată atât de Curte, cât și de Curtea EDO în cauzele care implică măsuri ce au ca obiect prelucrarea datelor cu caracter personal [82].

b) Cu privire la respectarea substanței drepturilor prevăzute la articolele 7 și 8 din cartă

89. În conformitate cu articolul 52 alineatul (1) prima teză din cartă, orice restrângere adusă exercitării drepturilor fundamentale trebuie să aibă nu numai un temei juridic suficient de exact, ci să respecte de asemenea *substanța* acestor drepturi.

[79] Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981 și ratificată de toate statele membre, cunoscută mai curând sub numele de „Convenția 108”. În anul 2018 a fost elaborat un protocol de modificare a acestei convenții în vederea modernizării sale. Prin Decizia (UE) 2019/682 a Consiliului din 9 aprilie 2019 (JO 2019, L 115, p. 7), statele membre au fost autorizate să ratifice, în interesul Uniunii, protocolul de modificare menționat anterior, în măsura în care dispozițiile acestuia țin de competența exclusivă a Uniunii. În continuare în prezentele concluzii, vom face referire și la textul Convenției 108 modernizate, care, deși nu a fost ratificată încă de toate statele membre și nu a intrat încă în vigoare, prevede, după cum reiese din Decizia 2019/682, garanții bazate pe aceleași principii precum cele prevăzute de RGPD și de Directiva privind poliția.

[80] https://rm.coe.int/t-pd-2016-18rev-avis-pnr-fr/16807b6c09, p. 3 și 5. Raportul explicativ care însoțește Protocolul de modificare a Convenției 108 (denumit în continuare „Raportul explicativ privind Convenția 108 modernizată”) pune de asemenea accentul pe cerința ca măsura care prevede o ingerință în exercitarea dreptului la respectarea vieții private și la protecția datelor cu caracter personal să fie „accesibilă”, „previzibilă”, „suficient de detaliată” și „formulată în mod clar”; a se vedea punctul 91 din acest raport explicativ https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

[81] A se vedea *a contrario* Hotărârea din 3 decembrie 2019, Republica Cehă/Parlamentul și Consiliul (C-482/17, EU:C:2019:1035, punctul 135).

[82] A se vedea printre altele Hotărârea La Quadrature du Net, punctul 132 și jurisprudența citată; a se vedea de asemenea Curtea EDO, Hotărârea Big Brother Watch, punctul 334.

90. Astfel cum am explicat la punctul 66 din prezentele concluzii, această cerință – care este încorporată în constituțiile diferitelor state membre [83] și care, chiar dacă nu este recunoscută în mod expres de CEDO, este totuși bine ancorată în jurisprudența Curții EDO [84] – este consacrată la articolul 52 alineatul (1) din cartă [85]. Recunoscută de Curte cu mult înainte de codificarea sa [86], o astfel de cerință a fost constant reiterată în jurisprudența instanțelor Uniunii, chiar și după intrarea în vigoare a Tratatului de la Lisabona.

91. Rezultă în special din Hotărârea din 6 octombrie 2015, Schrems [87], că nerespectarea substanței unui drept fundamental de către un act al Uniunii atrage *în mod automat* nulitatea sau invaliditatea acestuia, fără a fi necesară o punere în balanță a intereselor aflate în joc. Astfel, Curtea recunoaște că orice drept fundamental are un „nucleu dur”, care garantează fiecărei persoane o sferă de libertate aflată la adăpost de orice ingerință din partea autorităților publice și care nu poate face obiectul unor limitări [88], cu excepția cazului în care sunt puse în discuție principiile democrației, statului de drept și respectării demnității umane, care stau la baza protecției drepturilor fundamentale. În plus, reiese atât din textul articolului 52 alineatul (1) din cartă, cât și din jurisprudența Curții și în special din Hotărârea Schrems I că aprecierea existenței unei ingerințe în substanța dreptului fundamental în cauză trebuie să fie anterioară și independentă de aprecierea proporționalității măsurii în cauză. Este vorba, cu alte cuvinte, de un test care are propria autonomie.

92. Cu toate acestea, faptul de a determina ceea ce constituie „substanța” și, prin urmare, conținutul intangibil al unui drept fundamental a cărui exercitare poate fi limitată este o operațiune extrem de complexă. Chiar dacă, pentru a-și îndeplini funcția, această noțiune ar trebui să poată fi definită în termeni absoluți, având în vedere caracteristicile esențiale ale dreptului fundamental în cauză, interesele subiective și obiective pe care urmărește să le protejeze și, în general, funcția sa într-o societate democratică bazată pe respectarea demnității umane [89], în practică, o astfel de operațiune se dovedește a fi aproape imposibilă, cel puțin fără a lua în considerare criteriile utilizate în mod obișnuit pentru a examina proporționalitatea ingerinței în exercitarea dreptului în cauză, cum ar fi gravitatea acestei ingerințe, amploarea sau dimensiunea sa temporală, și, prin urmare, fără a lua în considerare particularitățile fiecărui caz concret.

93. În ceea ce privește îndeosebi dreptul fundamental la respectarea vieții private, trebuie să se țină seama nu numai de importanța pe care o are, pentru sănătatea mentală și fizică a oricărei persoane, pentru bunăstarea, autonomia, dezvoltarea personală și capacitatea sa de a construi și de a cultiva relații sociale, faptul de a dispune de o sferă privată de dezvoltare interioară personală, ci și de rolul pe care acest drept îl joacă în salvgardarea altor drepturi și libertăți, cum ar fi în special libertatea de gândire, de conștiință, de religie, de exprimare și de informare, a căror deplină exercitare presupune recunoașterea unei sfere de intimitate. În general, trebuie să se țină seama de funcția pe care o îndeplinește respectarea dreptului la viață privată într-o

83 A se vedea în această privință Tridimas, T., Gentile, G., „The essence of Rights: an unreliable Boundary?”, *German Law Journal*, 2019, p. 796; Lenaerts, K., „Limits on limitations: The Essence of Fundamental Rights in the EU”, *German Law Journal*, 2019, 20, p. 779 și urm.

84 Pornind de la Hotărârea Curții EDO din 24 octombrie 1979, Winterwerp împotriva Țărilor de Jos (CE:ECHR:1979:1024JUD000630173, punctul 60).

85 A se vedea Explicațiile cu privire la Carta drepturilor fundamentale (JO 2007, C 303, p. 17, în special „Explicațiile cu privire la articolul 52”, p. 32, denumite în continuare „Explicațiile cu privire la cartă”).

86 A se vedea deja în acest sens în special Hotărârea din 14 mai 1974, Nold/Comisia (4/73, EU:C:1974:51, punctul 14), și Hotărârea din 13 decembrie 1979, Hauer (44/79, EU:C:1979:290, punctul 23).

87 C-362/14, denumită în continuare „Hotărârea Schrems I”, EU:C:2015:650, punctele 94-98.

88 A se vedea Lenaerts, K., *op. cit.*, p. 781, Tridimas, T., Gentile, G., *op. cit.*, p. 803.

89 Explicațiile cu privire la cartă recunosc expres că „demnitatea persoanei face parte din substanța drepturilor înscrise în […] cartă” și „[c]arta trebuie, prin urmare, respectată, chiar în cazul restrângerii unui drept”.

societate democratică [90]. Curtea pare să aprecieze existența unei ingerințe în substanța acestui drept prin luarea în considerare atât a *intensității*, cât și a *amplorii* ingerinței, ceea ce conduce la opinia că o astfel de ingerință este definită mai mult cantitativ decât calitativ. Astfel, pe de o parte, în Hotărârea Digital Rights, Curtea a considerat în esență că obligația de păstrare a datelor impusă de Directiva 2006/24/CE [91] nu a atins un asemenea nivel de gravitate încât să aibă un impact asupra substanței dreptului la respectarea vieții private, întrucât nu permitea „cunoașterea conținutului comunicațiilor electronice ca atare” [92]. Pe de altă parte, în Avizul 1/15, Curtea a considerat în esență că o limitare cantonată numai la anumite aspecte ale vieții private a persoanelor în cauză nu poate genera o ingerință în substanța acestui drept fundamental [93].

94. În ceea ce privește dreptul fundamental la protecția datelor cu caracter personal, Curtea pare să considere că substanța acestui drept este protejată atunci când măsura care stabilește ingerința limitează scopurile prelucrării și prevede norme care să asigure securitatea datelor în cauză, în special împotriva distrugerii accidentale sau ilegale, a pierderii sau a modificării accidentale [94].

95. În prezenta cauză, chiar dacă instanța de trimitere nu s-a referit în mod explicit la cerința respectării substanței drepturilor prevăzute la articolele 7 și 8 din cartă, problema respectării acestei cerințe este, în opinia noastră, subiacentă celei de a patra și celei de a șasea întrebări preliminare. Din acest motiv, propunem Curții să se aplece asupra ei.

96. În această privință, reamintim că, la punctul 150 din Avizul 1/15, deși admite că datele din PNR „pot să reveleze, dacă este cazul, informații foarte prețioase cu privire la viața privată a unei persoane” [95] și că aceste informații pot dezvălui, direct sau indirect, date sensibile ale persoanei în cauză [96], Curtea a concluzionat totuși, în ceea ce privește proiectul de Acord PNR Canada-UE, că, întrucât „natura acestor informații e[ra] limitată la anumite aspecte ale acestei vieți private, referitoare în special la călătoriile pe calea aerului între Canada și Uniune”, încălcarea dreptului fundamental la respectarea vieții private nu era de natură să afecteze substanța acestui drept.

97. Or, în afară de împrejurarea că datele din PNR avute în vedere de proiectul de Acord PNR Canada-UE trebuiau transferate către un stat terț și că prelucrarea lor ulterioară trebuia efectuată de autoritățile acestui stat terț pe teritoriul său, ingerințele în exercitarea dreptului fundamental la respectarea vieții private care rezultă din acest proiect de acord și cele prevăzute de Directiva PNR coincid în mare măsură sub aspectul naturii lor. Acest lucru este valabil, printre altele, în ceea ce privește datele din PNR în cauză, caracterul sistematic și generalizat al transferului și al prelucrării acestor date, caracterul automatizat al acestuia, precum și păstrarea acestor date. În schimb, ceea ce diferențiază cele două cauze este, dacă se poate spune astfel, „acoperirea geografică” a acestor ingerințe. Într-adevăr, după cum am indicat la punctul 77 din prezentele concluzii, operațiunile de prelucrare a datelor în discuție în prezenta cauză nu se limitează la legăturile aeriene cu o singură țară terță, astfel cum a fost cazul în Avizul 1/15, ci acoperă practic toate zborurile având ca punct de sosire și de plecare Uniunea și care sunt efectuate în interiorul acesteia. Prin urmare,

90 Facem referire în această privință la considerațiile cuprinse în opinia comună parțial concurentă a judecătorilor Lemmens, Vehabović și Bošniak exprimată în Hotărârea Big Brother Watch, punctele 3-10.

91 Directiva Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO 2006, L 105, p. 54, Ediție specială 13/vol. 53, p. 51).

92 A se vedea Hotărârea Digital Rights, punctul 39; a se vedea de asemenea, în ceea ce privește Directiva 2002/58, Hotărârea Tele2 Sverige, punctul 101.

93 A se vedea Avizul 1/15, punctul 150.

94 A se vedea în acest sens în special Hotărârea Digital Rights, punctul 40.

95 A se vedea în același sens Avizul 1/15, punctul 128.

96 A se vedea Avizul 1/15, punctele 164 și 165.

în comparație cu proiectul de Acord PNR Canada-UE, Directiva PNR impune prelucrarea sistematică a unui număr semnificativ mai mare de pasageri aerieni care călătoresc pe calea aerului în interiorul și în exteriorul Uniunii. În plus, dată fiind creșterea volumului de date prelucrate și a frecvenței cu care acestea sunt colectate, prelucrarea lor este probabil susceptibilă să furnizeze informații mai exacte, dar și mai ample despre viața privată a persoanelor în cauză (obiceiuri de călătorie, relații personale, situații financiare etc.).

98. Nu este mai puțin adevărat că, la fel ca în cazul Avizului 1/15, aceste informații, apreciate în mod izolat, se referă doar la anumite aspecte ale vieții private, legate de călătoriile cu avionul. Or, având în vedere necesitatea de a defini noțiunea de „substanță" a drepturilor fundamentale într-o manieră restrictivă, astfel încât aceasta să își păstreze funcția de bastion împotriva atacurilor asupra substanței înseși a acestor drepturi, considerăm că concluzia la care Curtea a ajuns la punctul 150 din Avizul 1/15 poate fi transpusă în prezenta cauză.

99. În Avizul 1/15, Curtea a exclus inclusiv o încălcare a substanței dreptului la protecția datelor cu caracter personal [97]. În opinia noastră, această concluzie poate fi de asemenea transpusă în împrejurările din prezenta cauză. Într-adevăr, la fel ca în cazul proiectului de Acord PNR Canada-UE, Directiva PNR limitează la articolul 1 alineatul (2) scopurile în care pot fi prelucrate datele din PNR. În plus, această directivă, precum și celelalte acte ale Uniunii la care aceasta face trimitere, în special RGPD și Directiva privind poliția, conțin dispoziții specifice menite să asigure îndeosebi securitatea, confidențialitatea și integritatea acestor date, precum și să le protejeze împotriva accesului și prelucrării ilicite. Chiar dacă nu se poate considera că o reglementare precum cea prevăzută de Directiva PNR afectează substanța drepturilor fundamentale protejate la articolele 7 și 8 din cartă, totuși aceasta trebuie să facă obiectul unui control strict și riguros al proporționalității sale.

c) Cu privire la respectarea cerinței ca ingerința să răspundă unui obiectiv de interes general

100. Directiva PNR urmărește cu precădere să asigure securitatea internă a Uniunii și să protejeze viața și siguranța persoanelor fizice prin transferul de date din PNR către autoritățile competente ale statelor membre pentru a fi utilizate în combaterea terorismului și a infracțiunilor grave [98].

101. În mod deosebit, rezultă din articolul 1 alineatul (2) din Directiva PNR coroborat cu considerentele (6) și (7) ale acesteia, precum și din propunerea Comisiei care a condus la adoptarea acestei directive (denumită în continuare „propunerea de Directivă PNR") [99] că, în cadrul unui astfel de obiectiv, datele din PNR sunt utilizate în moduri diferite de către autoritățile de aplicare a legii [100]. În primul rând, aceste date sunt utilizate pentru a identifica persoanele implicate sau suspectate de a fi implicate în infracțiuni de terorism și în infracțiuni grave care au fost deja săvârșite, pentru a colecta probe și, dacă este cazul, pentru a identifica complicii infractorilor și pentru a destructura rețelele infracționale (utilizare în „mod reactiv"). În al doilea rând, datele din PNR pot fi evaluate înainte de sosirea sau de plecarea pasagerilor pentru a preveni săvârșirea unei infracțiuni și pentru a identifica persoanele care nu au fost suspectate anterior de implicare în infracțiuni de terorism sau în infracțiuni grave și care, pe baza

97 A se vedea Avizul 1/15, punctul 150.

98 A se vedea în special considerentele (5), (6), (15) și (22) ale Directivei PNR.

99 Propunerea Comisiei din 2 februarie 2011 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave [COM(2011) 32 final, p. 4].

100 Din motive de simplificare, vom utiliza în prezentele concluzii sintagma „autorități de aplicare a legii" pentru a ne referi, într-un mod general, la orice autoritate cu atribuții în depistarea, prevenirea, urmărirea penală sau investigarea terorismului sau a infracțiunilor grave reglementate de Directiva PNR.

rezultatului acestei evaluări, ar trebui să fie supuse unei examinări mai aprofundate de către autoritățile de aplicare a legii (utilizare în „mod real"). În sfârșit, datele din PNR sunt utilizate în scopul definirii criteriilor de evaluare care pot fi aplicate ulterior la evaluarea riscului prezentat de pasageri înainte de sosirea și înainte de plecarea lor (utilizare în „mod proactiv"). O astfel de utilizare proactivă a datelor din PNR ar trebui să permită autorităților de aplicare a legii să contracareze amenințarea reprezentată de marea infracționalitate și de terorism sub un unghi diferit de cel permis de prelucrarea altor categorii de date cu caracter personal [101].

102. Rezultă din jurisprudența Curții că obiectivul de protecție a siguranței publice, care acoperă în special prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, constituie un obiectiv de interes general al Uniunii, în sensul articolului 52 alineatul (1) din cartă, care poate justifica o ingerință, chiar și gravă, în exercitarea drepturilor fundamentale consacrate la articolele 7 și 8 din cartă [102].

103. Curtea a admis de asemenea că obiectivele de menținere a securității publice și de combatere a infracțiunilor grave contribuie la protecția drepturilor și libertăților celorlalți [103]. Astfel, cât privește evaluarea comparativă între aceste obiective și drepturile fundamentale consacrate la articolele 7 și 8 din cartă [104], trebuie să se țină seama și de importanța drepturilor consacrate la articolele 3, 4, 6 și 7 din cartă. În acest sens, chiar dacă în Hotărârea La Quadrature du Net, Curtea a considerat că articolul 6 din cartă „nu poate fi interpretat în sensul că impune autorităților publice o obligație de a adopta măsuri specifice în vederea sancționării anumitor infracțiuni" [105], în schimb, în ceea ce privește îndeosebi combaterea efectivă a infracțiunilor ale căror victime sunt mai ales minorii și celelalte persoane vulnerabile, aceasta a subliniat că obligațiile pozitive ale autorităților publice pot decurge atât din articolul 7 din cartă, în vederea adoptării de măsuri legale pentru protejarea vieții private și de familie, cât și din articolele 3 și 4 din cartă, în ceea ce privește protecția integrității fizice și psihice a persoanelor, precum și interzicerea torturii și a tratamentelor inumane și degradante [106].

104. În sfârșit, Curtea a considerat că importanța obiectivului de menținere a *securității naționale* o depășește pe cea a obiectivelor de combatere a infracționalității în general, chiar gravă, precum și de protejare a siguranței publice și acesta poate justifica, așadar, măsuri care presupun ingerințe mai grave în exercitarea drepturilor fundamentale decât cele pe care le-ar putea justifica celelalte obiective [107]. Întrucât activitățile de terorism pot constitui amenințări la adresa securității naționale a statelor membre, sistemul pus în aplicare prin Directiva PNR, în măsura în care servește drept instrument de combatere a unor astfel de activități, contribuie la obiectivul de menținere a securității naționale a statelor membre.

101 A se vedea considerentul (7) al Directivei PNR. A se vedea de asemenea propunerea de Directivă PNR, p. 5.

102 A se vedea în acest sens Avizul 1/15, precum și Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele referitoare la comunicațiile electronice) (C-746/18, denumită în continuare „Hotărârea Prokuratuur", EU:C:2021:152, punctul 33 și jurisprudența citată).

103 A se vedea în acest sens Avizul 1/15, punctul 149 și jurisprudența citată, precum și Hotărârea La Quadrature du Net.

104 A se vedea mai jos analiza privind proporționalitatea ingerinței.

105 A se vedea Hotărârea La Quadrature du Net, punctul 125.

106 A se vedea Hotărârea La Quadrature du Net, punctul 126 și jurisprudența citată.

107 A se vedea Hotărârea La Quadrature du Net, punctul 136.

d) Cu privire la respectarea principiului proporționalității

105. În conformitate cu articolul 52 alineatul (1) teza a doua din cartă, pentru respectarea principiului proporționalității, pot fi impuse restrângeri în exercitarea unui drept fundamental recunoscut de cartă numai în cazul în care sunt necesare și numai dacă răspund efectiv unor obiective de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

106. În această privință, trebuie amintit că principiul proporționalității impune, potrivit unei jurisprudențe constante a Curții, ca actele instituțiilor Uniunii să fie de natură să atingă obiectivele legitime urmărite de reglementarea în cauză și să nu depășească limitele a ceea ce este adecvat și necesar pentru realizarea acestor obiective [108].

107. Conform jurisprudenței constante a Curții, protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele *strictului necesar*. În plus, un obiectiv de interes general nu poate fi urmărit fără a se ține seama de faptul că acesta trebuie conciliat cu drepturile fundamentale avute în vedere de măsura respectivă, prin realizarea unei evaluări comparative între, pe de o parte, obiectivul interesului general și, pe de altă parte, drepturile în cauză [109]. Mai precis, proporționalitatea unei limitări a drepturilor consacrate la articolele 7 și 8 din cartă 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 [110].

108. Rezultă din jurisprudența Curții că, pentru a îndeplini cerința privind proporționalitatea, Directiva PNR, ca temei juridic care presupune ingerințe în exercitarea drepturilor fundamentale consacrate la articolele 7 și 8 din cartă, descrise la punctele 70-83 din prezentele concluzii, trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurilor care implică astfel de ingerințe și să impună o serie de cerințe minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces ilicit și a oricărei utilizări ilicite a acestor date [111]. Necesitatea de a dispune de astfel de garanții este cu atât mai importantă atunci când, precum în prezenta cauză, datele cu caracter personal sunt supuse unei prelucrări automatizate și atunci când în joc este protecția acestei categorii speciale de date cu caracter personal pe care o reprezintă datele sensibile [112].

109. În ceea ce privește întinderea controlului jurisdicțional al respectării cerințelor care decurg din principiul proporționalității, având în vedere rolul important pe care îl are protecția datelor cu caracter personal în raport cu dreptul fundamental la respectarea vieții private și ingerința în exercitarea acestor drepturi pe care o implică Directiva PNR, puterea de apreciere a legiuitorului Uniunii se dovedește a fi redusă, astfel încât este necesară efectuarea unui control strict [113].

108 A se vedea Hotărârea Digital Rights, punctul 46 și jurisprudența citată.

109 A se vedea Avizul 1/15, punctul 140, precum și Hotărârea La Quadrature du Net, punctul 130 și jurisprudența citată. Cerința ca prelucrarea datelor cu caracter personal să reflecte, în fiecare etapă, „un just echilibru între toate interesele implicate, indiferent că sunt publice sau private, precum și drepturile și libertățile aflate în joc” este prevăzută de asemenea la articolul 5 din Convenția 108.

110 A se vedea în acest sens Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punctul 55 și jurisprudența citată), precum și Hotărârea La Quadrature du Net, punctul 131, și Hotărârea Prokuratuur, punctul 32.

111 A se vedea în acest sens Hotărârea Digital Rights, punctul 54, Hotărârea Schrems I, punctul 91, precum și Avizul 1/15, punctul 141.

112 A se vedea Avizul 1/15, punctul 141 și jurisprudența citată.

113 A se vedea în acest sens Hotărârea Digital Rights, punctul 48.

1) Cu privire la caracterul adecvat al prelucrării datelor din PNR menționate în Directiva PNR în raport cu obiectivul urmărit

110. La punctul 153 din Avizul 1/15, Curtea a afirmat, în ceea ce privește proiectul de Acord PNR Canada-UE, că se poate considera că transferul datelor din PNR către Canada și prelucrările lor ulterioare sunt apte să garanteze realizarea obiectivului privind protecția securității și a siguranței publice. Considerăm că această adecvare, care a fost recunoscută de mult timp atât la nivelul Uniunii, cât și la nivel mondial [114], nu poate fi contestată în ceea ce privește colectarea și prelucrarea ulterioare ale datelor din PNR în ceea ce privește zborurile extra-UE și cele intra-UE [115].

111. În aceste condiții, eficacitatea sistemului de prelucrare a datelor din PNR instituit prin directivă poate fi evaluată numai în mod concret, prin evaluarea rezultatelor aplicării sale [116]. În acest sens, este esențial ca o astfel de eficacitate să fie evaluată în mod continuu pe baza unor date statistice cât mai exacte și mai fiabile [117]. În această privință, Comisia ar trebui să efectueze, la intervale regulate, o revizuire similară celei deja prevăzute la articolul 19 din Directiva PNR.

2) Cu privire la caracterul strict necesar al ingerinței

112. Chiar dacă Cour constitutionnelle (Curtea Constituțională) nu a ridicat în mod explicit îndoieli cu privire la faptul că Directiva PNR conține norme clare, exacte și limitate la strictul necesar în ceea ce privește delimitarea scopurilor în care pot fi prelucrate datele din PNR [118], analiza proporționalității sistemului prevăzut de această directivă, solicitată de instanța de trimitere, nu poate, în opinia noastră, să omită abordarea acestei chestiuni [119].

i) Cu privire la delimitarea scopurilor prelucrării datelor din PNR

113. O delimitare clară a scopurilor pentru care este permis accesul autorităților competente la datele cu caracter personal, precum și utilizarea ulterioară a acestora de către autoritățile respective constituie o cerință esențială a oricărui sistem de prelucrare a datelor, în special în scopul aplicării legii. Îndeplinirea acestei cerințe este de altfel necesară pentru a permite Curții să evalueze proporționalitatea măsurilor în cauză, prin aplicarea testului privind gravitatea ingerinței în raport cu importanța obiectivului urmărit, identificat în jurisprudența sa [120].

114. Curtea a subliniat importanța unei delimitări clare a scopurilor măsurilor care implică limitări ale drepturilor fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, în special în Hotărârea Digital Rights, în care a declarat nevalidă Directiva 2006/24. La punctul 60 din acea hotărâre, Curtea a observat că directiva menționată nu prevedea „niciun criteriu obiectiv care să permită delimitarea accesului autorităților naționale competente la date

114 A se vedea în acest sens punctele 201-203 din prezentele concluzii.

115 În acest sens, facem referire la datele conținute în documentul de lucru 2020.

116 A se vedea în acest sens Avizul din 19 august 2016, p. 5.

117 Cu privire la importanța statisticilor pentru evaluarea eficacității sistemului instituit prin Directiva PNR, a se vedea în special Avizul 1/2011 din 14 iunie 2011 privind propunerea de Directivă PNR, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_FR.pdf, punctul 2.1.2.1 (denumit în continuare „Avizul 1/2011 al FRA”).

118 Această întrebare este în schimb adresată în mod clar de Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania), în cauza pendinte C-215/20.

119 Comisia a fost invitată să își prezinte observațiile în acest sens printr-o întrebare la care s-a solicitat un răspuns scris. Celelalte părți interesate au avut posibilitatea de a lua poziție în ședință.

120 A se vedea punctul 107 in fine din prezentele concluzii.

și utilizarea lor ulterioară în scopul prevenirii, detectării sau urmăririi penale în legătură cu infracțiuni care, având în vedere amploarea și gravitatea ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă, pot fi considerate ca fiind suficient de grave pentru a justifica o astfel de ingerință” și că, dimpotrivă, aceasta se limita „la a face trimitere în general, la articolul 1 alineatul (1), la infracțiunile grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern”.

115. Articolul 1 alineatul (2) din Directiva PNR enunță un criteriu general de limitare a scopului, conform căruia „[d]atele din PNR colectate în conformitate cu prezenta directivă pot fi prelucrate doar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave”. Cu toate acestea, spre deosebire de Directiva 2006/24, Directiva PNR nu se limitează la o astfel de enunțare, ci definește la articolul 3 punctele 8 și 9 atât noțiunea de „infracțiuni de terorism”, cât și pe cea de „infracțiuni grave”, prima noțiune, prin trimitere la articolele 1-4 din Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO 2002, L 164, p. 3, Ediție specială, 19/vol. 3, p. 252) [înlocuită de Directiva (UE) 2017/541] [121], iar a doua, pe de o parte, prin enumerarea, în anexa II, a categoriilor de infracțiuni care corespund acestei noțiuni și, pe de altă parte, prin stabilirea unui prag de gravitate legat de durata maximă a pedepsei cu închisoarea sau a măsurii de siguranță aplicabile în cazul acestor infracțiuni.

116. În timp ce referirea la dispozițiile relevante din Directiva 2017/541 face posibilă caracterizarea într-un mod suficient de clar și de exact a actelor care pot fi calificate drept infracțiuni de terorism în temeiul articolului 3 punctul 8 din Directiva PNR și evaluarea gravității acestora în scopul de a face o analiză comparativă a importanței obiectivului privind protecția siguranței publice urmărit de această directivă și a gravității ingerinței pe care o implică în exercitarea drepturilor fundamentale consacrate la articolele 7 și 8 din cartă, aceeași concluzie nu se impune cu aceeași evidență în ceea ce privește toate infracțiunile enumerate în anexa II.

117. La punctul 177 din Avizul 1/15, Curtea a apreciat că proiectul de Acord PNR Canada-UE definește cu claritate și cu precizie nivelul de gravitate al infracțiunilor vizate de noțiunea de „infracțiune transnațională gravă”, impunând ca acestea să fie „sancționate cu o pedeapsă privativă de libertate de cel puțin patru ani sau cu o pedeapsă mai severă”, făcând referire „la infracțiunile definite de dreptul canadian” și stabilind „diferitele ipoteze în care o infracțiune este considerată ca fiind de natură transnațională”.

118. În comparație cu reglementarea examinată de Curte în acel aviz, Directiva PNR, în primul rând, nu ia în considerare, la definirea infracțiunilor vizate, caracterul lor transnațional, în al doilea rând, prevede o listă exhaustivă de infracțiuni care, prin natura lor, sunt considerate infracțiuni grave, cu condiția ca acestea să atingă pragul minim al pedepsei maxime prevăzut la articolul 3 punctul 9 din această directivă, în al treilea rând, reduce, în principiu, pragul de gravitate, adoptând un criteriu bazat pe nivelul pedepsei maxime și stabilind acest prag la trei ani.

119. În ceea ce privește, în primul rând, lipsa unui criteriu de limitare bazat pe caracterul transnațional, este desigur adevărat că limitarea domeniului material de aplicare al Directivei PNR doar la infracționalitatea „transfrontalieră” gravă ar fi permis să se vizeze infracțiuni care, prin natura lor, pot avea, cel puțin potențial, o legătură obiectivă cu călătoriile aeriene și, prin

[121] Directiva Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO 2017, L 88, p. 6).

urmare, cu categoriile de date colectate și prelucrate în conformitate cu Directiva PNR [122]. Cu toate acestea, împărtășim, în principiu, opinia exprimată de Comisie potrivit căreia, spre deosebire de contextul unui acord internațional, relevanța și necesitatea unui astfel de criteriu sunt mai puțin evidente în ceea ce privește un mecanism de combatere a criminalității al cărui obiectiv este protejarea securității interne a Uniunii. În plus, după cum afirmă de fiecare dată Comisia, inexistența unor elemente transfrontaliere nu este în sine un indiciu care să permită excluderea gravității unei infracțiuni.

120. În ceea ce privește, în al doilea rând, criteriul care stabilește pragul de gravitate al infracțiunilor vizate – care, pentru a permite o apreciere *ex ante* a acestei gravități, trebuie interpretat în sensul că se referă la durata maximă a pedepsei cu închisoarea sau a măsurii de siguranță prevăzute de lege, iar nu la cea care ar putea fi efectiv aplicată într-un caz concret – acest criteriu, chiar dacă se bazează pe minimul pedepsei maxime și nu pe minimul pedepsei minime, nu este în sine inadecvat pentru identificarea unui nivel suficient de gravitate care să poată justifica ingerința în exercitarea drepturilor fundamentale consacrate la articolele 7 și 8 din cartă prin operațiunile de prelucrare a datelor prevăzute de Directiva PNR. Totuși, în opinia noastră, acesta trebuie interpretat ca un criteriu care identifică un nivel „minim” de gravitate. Prin urmare, deși un astfel de criteriu interzice statelor membre să califice drept „infracțiuni grave” infracțiuni menționate în anexa II pentru care dreptul lor penal intern prevede o pedeapsă cu închisoarea sau o măsură de siguranță cu o durată mai mică de trei ani, acesta nu le obligă însă să recunoască în mod automat o astfel de calificare pentru toate infracțiunile care pot fi incluse în anexa II menționată și care sunt pasibile de o pedeapsă care atinge pragul prevăzut la articolul 3 punctul 9 din Directiva PNR, în cazul în care, având în vedere caracteristicile specifice ale sistemelor lor penale, o astfel de recunoaștere ar conduce la utilizarea regimului prevăzut de Directiva PNR în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de drept comun, contrar obiectivelor urmărite de această directivă.

121. În ceea ce privește, în al treilea rând, lista din anexa II, trebuie remarcat mai întâi că enumerarea exhaustivă din Directiva PNR a infracțiunilor care se încadrează în definiția „infracțiunii grave” constituie o garanție formală și materială fundamentală pentru a asigura legalitatea sistemului instituit prin Directiva PNR și securitatea juridică a pasagerilor. Cu toate acestea, trebuie remarcat că această listă include atât infracțiuni care, prin natura lor, au în mod incontestabil un nivel de gravitate ridicat – precum, de exemplu, traficul de ființe umane, exploatarea sexuală a copiilor și pornografia infantilă, traficul de arme, de materiale nucleare sau radioactive, sechestrarea ilicită a aeronavelor/navelor, infracțiunile grave de competența Curții Penale Internaționale, omorul, violul, răpirea, lipsirea de libertate în mod ilegal și luarea de

[122] Subliniem, în această privință, că noțiunea de „infracțiune cu caracter transnațional”, astfel cum este definită, de exemplu, în proiectul de Acord PNR Canada-UE, a fost suficient de largă pentru a include și infracțiuni comise într-o singură țară și în cazul cărora infractorul „se află sau intenționează să călătorească în altă țară”; a se vedea articolul 3 alineatul (3) litera (e) din proiectul de Acord PNR Canada-UE, a cărui formulare este reprodusă la punctul 30 din Avizul 1/15. De asemenea, observăm că, în Avizul său 1/2011 (punctele 2.2.3.1 și 3.7), FRA a sugerat limitarea sistemului PNR al Uniunii numai la infracțiunile transnaționale grave. În schimb, propunerea de Directivă PNR prevedea o prelucrare automată diferențiată pentru infracțiunile transnaționale și pentru cele care nu au acest caracter [a se vedea articolul 4 alineatul (2) litera (a) din această propunere].

ostateci [123] –, cât și infracțiuni pentru care un astfel de nivel de gravitate este mai puțin evident, precum, de exemplu, frauda, contrafacerea și pirateria produselor, falsificarea de documente administrative și uzul de fals, precum și traficul de autovehicule furate [124]. În plus, printre infracțiunile incluse în anexa II, unele sunt mai susceptibile decât altele să aibă, prin însăși natura lor, un caracter transnațional, precum traficul de ființe umane, traficul de stupefiante sau de arme, exploatarea sexuală a copiilor, facilitarea intrării și șederii neautorizate, sechestrarea ilicită a aeronavelor și să aibă astfel o legătură cu transportul aerian de pasageri.

122. În ceea ce privește caracterul suficient de clar și de precis al rubricilor prevăzute în anexa II, și în acest caz nivelul este foarte variabil. Astfel, chiar dacă lista cuprinsă în această anexă trebuie considerată exhaustivă, mai multe dintre rubricile sale au un caracter „deschis” [125], iar altele se referă la noțiuni generice, care pot include un număr foarte mare de infracțiuni de o gravitate variabilă, cu toate că se încadrează întotdeauna în limita pragului maxim prevăzut la articolul 3 punctul 9 din Directiva PNR [126].

123. În această privință, observăm, pe de o parte, că directivele de armonizare adoptate în domeniile prevăzute la articolul 83 alineatul (1) TFUE, menționate la nota de subsol 123 din prezentele concluzii, oferă elemente relevante pentru identificarea cel puțin a unora dintre infracțiunile grave care pot fi încadrate la rubricile corespunzătoare din anexa II. Astfel, în special, Directiva 2013/40 definește, la articolele 3-8, diferite infracțiuni care se încadrează în conceptul de „criminalitate cibernetică” menționat la punctul 9 din această anexă II, având grijă, în fiecare caz, să excludă faptele care constituie „cazuri minore” [127]. În mod similar, Directiva 2019/713 definește anumite tipologii de infracțiuni frauduloase, iar Directiva 2017/1371 definește elementele constitutive ale unei „fraude îndreptate împotriva intereselor financiare ale Uniunii”. În acest context, merită menționată și Directiva 2008/99/CE, adoptată în temeiul articolului 175

[123] În plus, observăm că unele dintre infracțiunile menționate în anexa II se încadrează în domenii ale criminalității descrise ca fiind „de o gravitate deosebită” la articolul 83 alineatul (1) primul paragraf TFUE și enumerate în al doilea paragraf al aceluiași alineat. Este vorba în special despre traficul de persoane, exploatarea sexuală a copiilor, traficul ilicit de droguri, traficul ilicit de arme, spălarea banilor, corupția, contrafacerea mijloacelor de plată, criminalitatea informatică și criminalitatea organizată. În mai multe dintre aceste domenii, legiuitorul Uniunii a adoptat, în temeiul articolului 83 alineatul (1) TFUE, directive care stabilesc „norme minime cu privire la definirea infracțiunilor și a sancțiunilor”; a se vedea în special Directiva 2011/36/UE a Parlamentului European și a Consiliului din 5 aprilie 2011 privind prevenirea și combaterea traficului de persoane și protejarea victimelor acestuia, precum și de înlocuire a Deciziei-cadru 2002/629/JAI a Consiliului (JO 2011, L 101, p. 1), Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO 2011, L 335, p. 1), Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO 2013, L 218, p. 8), Directiva (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului (JO 2019, L 123, p. 18), Directiva (UE) 2017/1371 a Parlamentului European și a Consiliului din 5 iulie 2017 privind combaterea fraudelor îndreptate împotriva intereselor financiare ale Uniunii prin mijloace de drept penal (JO 2017, L 198, p. 29), și Directiva (UE) 2018/1673 a Parlamentului European și a Consiliului din 23 octombrie 2018 privind combaterea prin măsuri de drept penal a spălării banilor (JO 2018, L 284, p. 22).

[124] Cu toate acestea, observăm că toate infracțiunile enumerate în anexa I, cu excepția „spionajului industrial”, se regăsesc la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO 2002, L 190, p. 1, Ediție specială 19/vol. 6, p. 3). Deși nu sunt calificate în mod explicit ca fiind grave, acestea determină totuși predarea pe baza unui mandat european de arestare, fără verificarea dublei incriminări a faptei, atunci când ating același prag al pedepsei privative de libertate ca cel prevăzut la articolul 3 punctul 9 din Directiva PNR. Aproape toate infracțiunile menționate, cu excepția „sabotajului”, a „sechestrării ilicite a aeronavelor” și a „spionajului industrial”, sunt menționate și în anexa I la Regulamentul (UE) 2018/1727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului (JO 2018, L 295, p. 138), care enumeră lista „formelor grave de criminalitate” care intră în sfera de competență a Eurojust.

[125] Este vorba în special despre punctele 7, 8, 10 și 16.

[126] Acesta este, de exemplu, cazul „fraudei” (punctul 7), al „corupției” (punctul 6), al „infracțiunilor informatice și criminalității cibernetice” (punctul 9) și al „infracțiunilor împotriva mediului” (punctul 10). Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden), în cauza pendinte C-215/20, are în vedere în special infracțiunile de fraudă.

[127] Articolul 9 din această directivă precizează de altfel durata minimă a pedepsei maxime cu închisoarea pentru astfel de infracțiuni, care poate ajunge la trei ani numai în anumite împrejurări.

alineatul (1) CE privind protecția mediului prin intermediul dreptului penal [128], care definește, la articolul 3, o serie de infracțiuni grave împotriva mediului care pot fi incluse la rubrica 10 din anexa II, inclusiv acțiuni calificabile drept „trafic ilicit de specii de animale pe cale de dispariție și trafic de specii și soiuri de plante pe cale de dispariție", cu excepția tuturor faptelor care au un impact neglijabil asupra bunurilor protejate. În sfârșit, reamintim Directiva 2002/90/CE [129], care definește facilitarea intrării, tranzitului și șederii neautorizate, precum și Decizia-cadru 2002/946/JAI [130], vizând consolidarea cadrului penal pentru sancționarea acestor infracțiuni, Decizia-cadru 2003/568/JAI [131], care definește infracțiunile calificate drept „corupție activă și pasivă în sectorul privat", și Decizia-cadru 2008/841/JAI [132], care definește infracțiunile legate de participarea la o organizație criminală.

124. Pe de altă parte, observăm, astfel cum a subliniat în mod întemeiat Comisia, că, în lipsa unei armonizări depline a dreptului penal material, nu se poate reproșa legiuitorului Uniunii că nu a detaliat mai mult infracțiunile menționate în anexa II. Astfel, spre deosebire de ceea ce se va observa ulterior în prezentele concluzii cu privire la lista de date din PNR din anexa I, transpunerea în dreptul intern a listei de infracțiuni din anexa II impune în mod necesar ca statele membre să definească, în funcție de particularitățile sistemelor lor naționale de drept penal, infracțiunile care pot fi vizate. Totuși, această operație trebuie efectuată cu respectarea deplină a criteriului conform căruia orice ingerință în exercitarea drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă trebuie să fie limitată la strictul necesar. Astfel, de exemplu, nu este exclus, în opinia noastră, ca statele membre să prevadă ca, pentru anumite infracțiuni, precum, de exemplu, cele menționate la punctele 7, 16, 17, 18, 25 din anexa II, utilizarea datelor din PNR să se limiteze la cazurile în care aceste infracțiuni au un caracter transfrontalier sau sunt săvârșite în cadrul unei organizații infracționale ori conțin anumite circumstanțe agravante. Va reveni instanțelor judecătorești din statele membre, sub controlul Curții, sarcina de a interpreta dispozițiile naționale care transpun în dreptul intern lista menționată, în conformitate atât cu Directiva PNR, cât și cu carta, astfel încât prelucrarea datelor din PNR să rămână, pentru fiecare rubrică, limitată la infracțiunile care ating nivelul ridicat de gravitate prevăzut de această directivă, precum și la infracțiunile pentru care o astfel de prelucrare se dovedește relevantă [133].

125. Sub rezerva precizărilor de la punctele 120 și 124 din prezentele concluzii, considerăm că articolul 3 punctul 9 din Directiva PNR, precum și lista de infracțiuni din anexa II la aceasta îndeplinesc cerințele de claritate și precizie și nu depășesc limitele strictului necesar.

126. Cu toate acestea, trebuie admis că soluția ilustrată la punctul 124 din prezentele concluzii nu este pe deplin satisfăcătoare. Într-adevăr, pe de o parte, aceasta lasă o marjă largă de apreciere statelor membre, astfel încât domeniul material de aplicare al prelucrării datelor din PNR poate varia semnificativ de la un stat membru la altul, compromițând în acest fel obiectivul de armonizare urmărit de legiuitorul Uniunii [134]. Pe de altă parte, aceasta presupune ca verificarea proporționalității unui element esențial al sistemului, cum ar fi limitarea scopurilor acestei prelucrări, să fie efectuată mai curând *ex post* cu privire la măsurile naționale de transpunere

128 Directiva Parlamentului European și a Consiliului din 19 noiembrie 2008 (JO 2008, L 328, p. 28).

129 Directiva Consiliului din 28 noiembrie 2002 de definire a facilitării intrării, tranzitului și șederii neautorizate (JO 2002, L 328, p. 17, Ediție specială 19/vol. 6, p. 33).

130 Decizia-cadru a Consiliului din 28 noiembrie 2002 privind consolidarea cadrului penal pentru a preveni facilitarea intrării, tranzitului și șederii neautorizate (JO 2002, L 328, p. 1, Ediție specială 19/vol. 6, p. 30).

131 Decizia-cadru a Consiliului din 22 iulie 2003 privind combaterea corupției în sectorul privat (JO 2003, L 192, p. 54, Ediție specială 19/vol. 6, p. 122).

132 Decizia-cadru a Consiliului din 24 octombrie 2008 privind lupta împotriva crimei organizate (JO 2008, L 300, p. 42).

133 A se vedea în special considerentele (7) și (22) ale Directivei PNR.

134 A se vedea considerentul (35) al Directivei PNR.

decât *ex ante* cu privire la însăși Directiva PNR. Prin urmare, ar fi preferabil, în ipoteza în care Curtea ar decide, astfel cum propunem, să considere articolul 3 punctul 9 din Directiva PNR, precum și lista de infracțiuni din anexa II la aceasta ca fiind conforme cu articolele 7, 8 și 52 alineatul (1) din cartă, ca aceasta să atragă atenția legiuitorului Uniunii asupra faptului că o astfel de evaluare este doar provizorie și determină din partea legiuitorului o verificare, în lumina transpunerii de către statele membre a acestei dispoziții și a listei respective și pe baza datelor statistice menționate la articolul 20 din Directiva PNR, necesitatea: (i) de a preciza pe viitor, prin restrângerea domeniului de aplicare al acestei liste, categoriile de infracțiuni menționate în lista respectivă; (ii) de a elimina din cadrul acestuia infracțiunile pentru care prelucrarea datelor din PNR se dovedește fie disproporționată, fie irelevantă sau ineficientă și (iii) de a ridica pragul de gravitate al infracțiunilor menționate la articolul 3 punctul 9 din Directiva PNR[135]. În această privință, observăm că, deși articolul 19 alineatul (2) litera (b) din Directiva PNR prevede că Comisia trebuie să revizuiască toate elementele Directivei PNR, acordând o atenție deosebită „necesității și proporționalității colectării și prelucrării datelor din PNR pentru fiecare dintre scopurile prevăzute" de această directivă, nici Raportul Comisiei din anul 2020, nici documentul de lucru din anul 2020 care îl însoțește nu conțin, în opinia noastră, o revizuire satisfăcătoare cu privire la acest aspect.

ii) Cu privire la categoriile de date din PNR menționate în Directiva PNR (a doua și a treia întrebare preliminară)

127. Directiva PNR prevede transferul către UIP a 19 categorii de date din PNR colectate de transportatorii aerieni în scopul rezervării zborurilor. Aceste categorii, enumerate în anexa I, corespund celor care apar în sistemele de rezervări ale companiilor aeriene și celor enumerate în anexa I la Orientările privind datele din registrele cu numele pasagerilor, adoptate de Organizația Aviației Civile Internaționale (OACI) în anul 2010[136] (denumite în continuare „Orientările OACI").

128. Prin intermediul celei de a doua întrebări preliminare, instanța de trimitere ridică întrebări cu privire la validitatea anexei I în raport cu articolele 7, 8 și 52 alineatul (1) din cartă, având în vedere, pe de o parte, amploarea datelor cu caracter personal enumerate în această anexă – și în special a datelor API menționate la punctul 18 din aceasta, în sensul că acestea depășesc datele enumerate la articolul 3 alineatul (2) din Directiva API – și, pe de altă parte, posibilitatea ca aceste date, luate în considerare împreună, să dezvăluie informații sensibile și să încalce astfel limitele „strictului necesar". Prin intermediul celei de a treia întrebări preliminare – care, după cum am avut deja ocazia să subliniem, se referă la respectarea primei dintre cele trei condiții prevăzute la articolul 52 alineatul (1) din cartă, potrivit căreia orice ingerință în exercitarea unui drept fundamental trebuie să fie „prevăzută de lege" –, Cour constitutionnelle (Curtea Constituțională) solicită în schimb Curții să se pronunțe cu privire la validitatea punctelor 12 și 18 din anexa I, având în vedere mai ales caracterul „deschis" al acestora.

129. Întrucât analiza care trebuie efectuată în contextul celei de a doua întrebări preliminare presupune să se examineze dacă categoriile de date cu caracter personal menționate în anexa I sunt suficient de clare și precise, vom aborda mai întâi a treia întrebare preliminară.

135 A se vedea prin analogie Hotărârea din 16 decembrie 2008, Arcelor Atlantique și Lorraine și alții (C-127/07, EU:C:2008:728, punctele 61 și 62), precum și Hotărârea din 17 octombrie 2013, Schaible (C-101/12, EU:C:2013:661, punctele 91 și 94).

136 A se vedea documentul 9944, aprobat de secretarul general al OACI și publicat sub autoritatea acestuia. Versiunea în limba franceză a acestui document este disponibilă pe site-ul: https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_fr.pdf. În conformitate cu punctul 9.22 din anexa 9 (Facilități) la Convenția privind aviația civilă internațională, semnată la Chicago la 7 decembrie 1944 (denumită în continuare „Convenția de la Chicago"), statele contractante la convenția respectivă care solicită datele din PNR trebuie să își alinieze cerințele privind datele și prelucrarea acestor date, printre altele, la aceste orientări.

– Cu privire la caracterul suficient de clar și de precis al punctelor 12 și 18 din anexa I (a treia întrebare preliminară)

130. Cu titlu preliminar, trebuie remarcat că amploarea și gravitatea ingerinței în exercitarea drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă pe care le are o măsură care introduce restricții în exercitarea acestor drepturi depinde, înainte de toate, de întinderea și de natura datelor cu caracter personal care fac obiectul prelucrării. Prin urmare, identificarea acestor date constituie o operațiune esențială pe care orice temei juridic care introduce o astfel de măsură trebuie să o realizeze cât mai clar și mai precis posibil.

131. Avizul 1/15 a recunoscut această cerință în ceea ce privește prelucrarea datelor din PNR. Pronunțându-se cu privire la rubricile din anexa la proiectul de Acord PNR Canada-UE, care conține lista datelor din PNR vizate de acordul avut în vedere, Curtea a considerat, în acest aviz, mai ales că utilizarea unor categorii generale de informații care nu determină în mod suficient întinderea datelor care urmează să fie transferate, precum și utilizarea unor liste ilustrative de date care nu stabilesc nicio limită în ceea ce privește natura și amploarea informațiilor care pot fi incluse în rubrica în cauză, nu îndeplinesc cerințele de claritate și de precizie.

132. A treia întrebare preliminară trebuie examinată în lumina acestor principii.

133. Punctul 12 din anexa I la aviz are următorul cuprins:

„Mențiuni cu caracter general [inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele și sexul minorului, vârsta, limba (limbile) vorbită (vorbite), numele și datele de contact ale persoanei care îl însoțește la plecare și relația sa cu minorul, numele și datele de contact ale persoanei care îl așteaptă la sosire și relația sa cu minorul, agentul prezent la plecare și la sosire].”

134. În măsura în care se referă la „mențiuni cu caracter general”, acest punct constituie, la fel ca rubrica 17 din anexa la proiectul de Acord Canada-UE privind PNR, o rubrică denumită „text liber”, care poate include toate informațiile colectate de transportatorii aerieni în cursul activităților lor de prestare de servicii, în plus față de cele enumerate în mod expres la celelalte puncte din anexa I. Or, trebuie constatat, astfel cum a făcut-o Curtea la punctul 160 din Avizul 1/15, că o rubrică de acest tip „nu furnizează nicio indicație privind natura și întinderea informațiilor care trebuie transmise și pare susceptibilă chiar să înglobeze informații fără nicio legătură cu finalitatea transferului datelor din PNR”. În plus, întrucât precizarea dintre paranteze existentă în textul punctului 12 din anexa I, referitoare la informațiile privind minorii neînsoțiți, este furnizată numai cu titlu de exemplu, după cum o dovedește utilizarea termenului „inclusiv”, această rubrică nu stabilește nicio limită în privința naturii și a întinderii informațiilor care pot să figureze în cuprinsul său [137].

135. În aceste condiții, punctul 12 din anexa I nu poate fi considerat ca fiind delimitat cu suficientă claritate și precizie.

136. Deși Comisia și Parlamentul par să împărtășească această concluzie, statele membre care au prezentat observații cu privire la a treia întrebare preliminară, precum și Consiliul i se opun pe baza unor argumente care se suprapun în mare măsură.

[137] În același sens, a se vedea Avizul 1/15, punctul 160.

137. În primul rând, o primă serie de argumente vizează, în termeni generali, contestarea posibilității de a transpune în prezenta cauză concluziile la care a ajuns Curtea în Avizul 1/15.

138. În această privință, admițând diferența de context dintre cele două cauze, ne vom limita aici la a observa că concluzia la care a ajuns Curtea la punctul 160 din Avizul 1/15 în ceea ce privește rubrica 17 din anexa la proiectul de Acord PNR Canada-UE s-a bazat pe o interpretare exclusiv semantică și structurală a acestei rubrici. Or, o astfel de interpretare poate fi transpusă întocmai în cazul punctului 12 din anexa I, al cărui text este, în ceea ce privește partea neexemplificativă, identic cu cel al rubricii menționate și are o structură similară. În plus, după cum se va vedea mai detaliat în continuare, cele două norme în discuție se înscriu în același context de reglementare multilaterală, format în special din Orientările OACI, la care Curtea a făcut de altfel referire în mod expres la punctul 156 din Avizul 1/15. În aceste condiții, nu numai că nimic nu se opune ca, în ceea ce privește punctul 12 din anexa I, să urmăm aceeași interpretare precum cea adoptată de Curte la punctul 160 din Avizul 1/15 pentru rubrica 17 din anexa la proiectul de Acord PNR Canada-UE, dar mai ales nu există niciun motiv pentru a ne abate de la aceasta.

139. În al doilea rând, numeroase state membre subliniază că diferitele puncte din anexa I, inclusiv punctul 12, corespund rubricilor din anexa I la Orientările OACI, pe care transportatorii aerieni le cunosc bine și cărora sunt perfect capabili să le atribuie un conținut precis. Acest punct 12 ar corespunde în special ultimelor două rubrici din anexa menționată, intitulate „Mențiuni cu caracter general” și, respectiv, „Text liber/Câmpuri de cod în OSI [Other Supplementary Information], SSR [Special Service Request], SSI [Special Service Information], Observații/Istoric” și care se referă la „informații suplimentare” sau „referitoare de serviciile solicitate” [138].

140. În această privință, observăm mai întâi că corespondența dintre, pe de o parte, rubricile din anexa I la proiectul de Acord PNR Canada-UE și, pe de altă parte, rubricile din anexa I la Orientările OACI nu a împiedicat Curtea să declare în Avizul 1/15 că unele dintre rubricile prevăzute în anexa I la proiectul de acord menționat nu îndeplineau cerințele de claritate și de precizie pe care trebuie să le îndeplinească o măsură de restrângere a exercițiului drepturilor fundamentale. În continuare, observăm că o trimitere, care de altfel nu este explicită [139], la Orientările OACI nu permite, contrar a ceea ce par să aprecieze unele state membre, să se precizeze mai mult natura și întinderea informațiilor care pot fi menționate la punctul 12 din anexa I. Dimpotrivă, interpretarea acestor orientări întărește concluzia că o rubrică de tip „text liber”, precum punctul 12 menționat, include un număr nelimitat de informații de natură diversă, în plus față de cele care sunt incluse din oficiu în PNR [140].

141. În al treilea rând, unele guverne susțin că este de competența statelor membre să precizeze, prin intermediul unor măsuri legislative interne și cu respectarea limitelor impuse de articolele 7, 8 și 52 alineatul (1) din cartă, informațiile care pot fi prevăzute la punctul 12 din anexa I. Într-adevăr, ar fi chiar în natura unei directive să lase statelor membre o marjă de apreciere în ceea ce privește mijloacele necesare pentru punerea în aplicare a dispozițiilor pe care aceasta le prevede.

138 A se vedea punctele 2.1.2 și 2.1.5 din Orientările OACI.

139 Singura referire la Orientările OACI din Directiva PNR se regăsește în considerentul (17) al acesteia și se referă numai la „formatel[e] de date compatibile […] aplicabile transferurilor de date [din PNR] de la transportatorii aerieni către statele membre”.

140 Astfel, punctul 2.1.5 din orientările amintite menționează „informații suplimentare” sau „referitoare la serviciile solicitate”, care pot viza „cereri de asistență medicală sau mese speciale, ale «minorilor care călătoresc singuri», cereri de asistență etc.”. La rândul său, punctul 2.1.6 precizează că „domeniul «observații generale»” poate conține de asemenea „anumite informații, cum ar fi corespondența internă sau comunicațiile interne dintre personalul companiilor aeriene și agenții de rezervare”.

142. În această privință, astfel cum am precizat deja la punctul 86 din prezentele concluzii, considerăm că, în cazul în care măsurile care implică o ingerință în exercitarea drepturilor fundamentale consacrate de cartă își au sursa într-un act legislativ al Uniunii, revine legiuitorului Uniunii obligația să stabilească, cu respectarea criteriilor de claritate și precizie menționate anterior, precum și a principiului proporționalității, întinderea exactă a acestor ingerințe. Rezultă că, atunci când instrumentul ales de acest legiuitor este o directivă, nu este posibil, în opinia noastră, să se delege statelor membre, la transpunerea directivei în dreptul intern, sarcina de a stabili elementele esențiale care definesc întinderea ingerinței, cum ar fi, în cazul restricțiilor privind drepturile fundamentale prevăzute la articolele 7 și 8 din cartă, natura și întinderea datelor cu caracter personal care fac obiectul prelucrării.

143. În al patrulea rând, unele state membre subliniază că punctul 12 din anexa I trebuie interpretat în sensul că vizează numai informații care au o legătură cu prestarea de servicii de transport. Astfel interpretat, acest punct ar fi compatibil cu articolele 7, 8 și 52 alineatul (1) din cartă.

144. Considerăm că nici acest argument nu este convingător. Mai întâi, într-adevăr, informațiile care pot fi incluse într-o rubrică denumită „mențiuni cu caracter general” și sub codurile OSI, SSI și SSR sunt de natură foarte eterogenă (asistență medicală, mese speciale sau preferințe alimentare, orice cerere de asistență, informații privind minorii care călătoresc singuri etc.) [141] și toate acestea sunt legate de serviciul de transport în sensul că sunt destinate, printre altele, să permită transportatorului aerian să adapteze prestarea serviciului la cerințele fiecărui pasager. Un criteriu de interpretare bazat pe relevanța informațiilor în raport cu serviciul de transport nu ar permite, așadar, o clarificare mai bună a domeniului de aplicare al acestui punct 12. În continuare, observăm că, deși Curtea a utilizat acest criteriu la punctul 159 din Avizul 1/15 pentru a interpreta o rubrică diferită din anexa la proiectul de Acord PNR Canada-UE într-un mod conform cu cerințele de claritate și precizie, aceasta a exclus totuși posibilitatea de a proceda astfel în ceea ce privește rubrica 17 din anexa respectivă, care corespunde punctului 12 din anexa I.

145. În al cincilea rând, unele state membre au subliniat că informațiile menite a fi vizate la punctul 12 din anexa I sunt furnizate în mod voluntar transportatorilor aerieni de pasagerii înșiși care sunt informați în mod corespunzător cu privire la transferul ulterior al acestor date către autoritățile publice. Ideea care stă la baza unui astfel de argument este, în opinia noastră, aceea că există un fel de consimțământ implicit din partea pasagerului în cauză ca datele pe care le furnizează companiilor aeriene să fie ulterior transferate autorităților publice.

146. În această privință, Curtea a avut deja ocazia să afirme că nu se poate vorbi de „consimțământ” în cazul în care persoana vizată nu se poate opune în mod liber prelucrării datelor sale cu caracter personal [142]. Or, pentru o mare parte din informațiile care se pot regăsi la punctul 12 din anexa I, pasagerul în cauză nu dispune de o alegere reală, ci este obligat să le furnizeze pentru a putea beneficia de serviciul de transport. Acesta este cazul în special al persoanelor cu handicap sau cu mobilitate redusă ori al persoanelor care necesită îngrijiri medicale sau chiar al minorilor neînsoțiți. În plus, reamintim că la punctele 142 și 143 din Avizul 1/15, Curtea a afirmat în mod clar că prelucrarea datelor din PNR de către autoritățile publice

[141] A se vedea punctele 2.1.5 și 2.1.6 din Orientările OACI.

[142] A se vedea Hotărârea din 17 octombrie 2013, Schwarz (C-291/12, EU:C:2013:670, punctul 32), referitoare la cazul unui solicitant de pașaport căruia i se cere să se supună prelevării amprentelor sale digitale pentru a obține un document care să îi permită să călătorească într-o țară terță.

într-un scop diferit de cel pentru care aceste date sunt colectate de transportatorii aerieni nu poate fi considerată ca întemeindu-se pe vreo formă de consimțământ acordat de pasageri pentru această colectare.

147. În sfârșit, majoritatea statelor membre susțin că prelucrarea datelor prevăzută de Directiva PNR este încadrată de numeroase garanții, printre care, în ceea ce privește transferul de date către UIP, obligația ce le revine acestora de a șterge datele care nu sunt prevăzute în anexa I, precum și datele care pot dezvălui originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, starea de sănătate, viața sexuală sau orientarea sexuală ale unei persoane.

148. În această privință, precizăm de la bun început că, în opinia noastră, evaluarea caracterului suficient de clar și precis al normelor care definesc întinderea și natura datelor care pot fi transferate către autoritățile publice, în sensul că vizează să asigure faptul că o măsură care implică o ingerință în exercitarea drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă respectă principiile legalității și securității juridice, trebuie efectuată fără a ține seama de garanțiile care însoțesc prelucrarea la care vor fi supuse datele de către autoritățile menționate, întrucât aceste garanții intră în discuție doar atunci când este examinată proporționalitatea măsurii în cauză. Acesta este de altfel modul în care Curtea a procedat, la punctele 155-163 din Avizul 1/15, la aprecierea rubricilor din proiectul de Acord PNR Canada-UE. Într-un mod mai general, adăugăm că ar trebui să se acorde o atenție deosebită necesității de a menține o distincție clară între diferitele etape pe care le presupune examinarea unei măsuri care implică o ingerință în exercitarea drepturilor fundamentale, întrucât un amalgam al acestor etape diferite va fi, în opinia noastră, întotdeauna în detrimentul unei protecții eficiente a acestor drepturi.

149. Acestea fiind spuse, ne limităm în acest punct la a arăta că obligația care revine UIP, în conformitate cu articolul 6 alineatul (1) din Directiva PNR, de a șterge alte date decât cele enumerate în anexa I are utilitate numai dacă această anexă conține o listă clară și închisă de date care urmează să fie transferate. Același lucru este valabil și pentru obligația pe care o are UIP, potrivit articolului 13 alineatul (4) din Directiva PNR, de a șterge așa-numitele date „sensibile”[143]. Într-adevăr, o definiție prea vagă, inexactă sau deschisă a informațiilor care trebuie transmise crește atât probabilitatea ca astfel de date să fie transferate în mod indirect, cât și riscul ca acestea să nu fie identificate și șterse imediat. Cu alte cuvinte, garanțiile menționate mai sus își pot îndeplini în mod util funcția numai dacă normele care definesc natura și întinderea datelor din PNR pe care transportatorii aerieni sunt solicitați să le transfere către UIP sunt suficient de clare și precise și dacă lista acestor date are un caracter închis și exhaustiv.

150. Pe baza tuturor considerațiilor care precedă și astfel cum am anticipat la punctul 135 din prezentele concluzii, considerăm că punctul 12 din anexa I, în măsura în care include „mențiunile cu caracter general” printre datele pe care transportatorii aerieni sunt obligați să le transfere către UIP în temeiul Directivei PNR, nu îndeplinește cerințele de claritate și de precizie impuse de articolul 52 alineatul (1) din cartă, astfel cum a fost interpretat de Curte[144], și, în consecință, în această măsură, ar trebui să fie declarat nevalid.

[143] Vom reveni asupra acestei categorii de informații ulterior în prezentele concluzii.

[144] În acest sens s-a exprimat FRA în Avizul său 1/2011, p. 13. În avizul său din 25 martie 2011 privind propunerea de Directivă PNR (https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_en.pdf, punctul 47) (denumit în continuare „Avizul CEPD din 25 martie 2011”), CEPD a propus să se excludă rubrica „Mențiuni cu caracter general” din lista din anexa I.

151. În observațiile lor scrise, Comisia și Parlamentul au propus Curții să utilizeze mai degrabă o „interpretare conformă” a punctului 12 din anexa I, apreciind că acesta se referă numai la informațiile privind minorii menționate în mod explicit între paranteze. Recunoaștem că avem dificultăți în a considera că o astfel de interpretare respectă limitele unei simple interpretări conforme. Desigur, este adevărat că, potrivit unui principiu general de interpretare, un act al Uniunii trebuie interpretat, în măsura posibilului, într-un mod care să nu repună în discuție validitatea acestuia și în conformitate cu dreptul primar în ansamblul său și în special cu dispozițiile cartei [145]. Este la fel de adevărat că, în cazul Directivei PNR, posibilitatea unei astfel de interpretări este favorizată de accentul pus în special de multe dintre considerentele acestei directive pe respectarea deplină a drepturilor fundamentale, a dreptului la viață privată, precum și a principiului proporționalității [146]. Cu toate acestea, rezultă tot dintr-o jurisprudență constantă că o interpretare conformă este permisă numai atunci când textul de drept derivat al Uniunii poate primi mai multe interpretări și este posibil, în consecință, să prevaleze mai curând acea interpretare care conferă dispoziției conformitatea cu dreptul primar decât cea care conduce la constatarea incompatibilității sale cu acesta [147].

152. Or, în opinia noastră, punctul 12 din anexa I nu poate fi interpretat astfel cum sugerează Comisia și Parlamentul decât dacă este interpretat „*contra legem*”. Într-adevăr, după cum am explicat mai sus, acest punct se referă la o categorie largă de date de diferite tipuri, neidentificabile *a priori*, față de care datele privind minorii reprezintă doar o subcategorie. A interpreta acest punct în sensul că se referă numai la această subcategorie nu doar că ar ignora o parte din formularea sa, dar ar submina ordinea logică a afirmației pe care o conține acest punct. O astfel de operațiune, care constă în esență în eliminarea părții din textul punctului 12 din anexa I care ar fi considerată neconformă cu cerințele de claritate și precizie, nu poate fi efectuată, în opinia noastră, decât prin declararea nulității parțiale.

153. În ceea ce privește restul punctului 12 din anexa I, care enumeră o serie de date privind minorii neînsoțiți, considerăm că acesta îndeplinește cerințele de claritate și precizie, cu condiția să fie interpretat în sensul că acoperă numai informațiile privind minorii neînsoțiți care sunt direct legate de zbor și care sunt menționate în mod expres la acest punct.

154. Punctul 18 din anexa I este redactat după cum urmează:

„Orice date API colectate (inclusiv tipul, numărul, țara de emitere și data expirării oricărui document de identitate, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării, data sosirii, aeroportul de plecare, aeroportul de sosire, ora plecării și ora sosirii).”

155. Acest punct are o structură similară cu cea a punctului 12 din anexa I. Acesta menționează de asemenea o categorie generală de date, și anume informațiile prealabile cu privire la pasageri (Advance Passenger Information – API), urmată, între paranteze, de o listă de date considerate a fi incluse în această categorie generală, care este furnizată doar cu titlu exemplificativ, după cum reiese din utilizarea expresiei „inclusiv”.

[145] A se vedea în special Hotărârea din 19 noiembrie 2009, Sturgeon și alții (C-402/07 și C-432/07, EU:C:2009:716, punctul 47 și jurisprudența citată), Hotărârea din 19 septembrie 2013, Reexaminare Comisia/Strack (C-579/12 RX-II, EU:C:2013:570, punctul 40), precum și Hotărârea din 14 mai 2019, M și alții (Revocarea statutului de refugiat) (C-391/16, C-77/17 și C-78/17, EU:C:2019:403, punctul 77 și jurisprudența citată).

[146] A se vedea în special considerentele (5), (7), (11), (15), (16), (20), (22), (23), (25), (27), (28), (31), (36) și (37) ale Directivei PNR.

[147] A se vedea Hotărârea din 26 iunie 2007, Ordre des barreaux francophones et germanophone și alții (C-305/05, EU:C:2007:383, punctul 28), precum și Hotărârea din 14 mai 2019, M și alții (Revocarea statutului de refugiat) (C-391/16, C-77/17 și C-78/17, EU:C:2019:403, punctul 77).

156. Cu toate acestea, spre deosebire de punctul 12 din anexa I, punctul 18 din această anexă se referă la o categorie de date care sunt mai ușor de identificat atât în ceea ce privește natura acestora, cât și întinderea lor. Într-adevăr, din considerentul (4) al Directivei PNR rezultă că, atunci când directiva se referă la această categorie de date, aceasta vizează informațiile care, potrivit Directivei API la care acest considerent face trimitere expresă, sunt transmise de transportatorii aerieni autorităților naționale competente în vederea îmbunătățirii controalelor la frontieră și a combaterii imigrației ilegale. Datele respective sunt enumerate la articolul 3 alineatul (2) din această ultimă directivă.

157. În plus, rezultă din considerentul (9)[148] al Directivei PNR, precum și din articolul 3 alineatul (2) din Directiva API și din lista exemplificativă conținută la punctul 18 din anexa I că datele API menționate la acest punct sunt, pe de o parte, date biografice care permit verificarea identității pasagerului aerian și, pe de altă parte, date referitoare la zborul rezervat. Mai exact, în ceea ce privește prima categorie, cea referitoare la datele biografice, informațiile enumerate la articolul 3 alineatul (2) din Directiva API și la punctul 18 din anexa I acoperă datele generate la înregistrare care pot fi extrase din partea lizibilă pe calculator a unui pașaport (sau a altui document de călătorie)[149].

158. Astfel, punctul 18 din anexa I, interpretat în lumina considerentelor (4) și (9) ale Directivei PNR, identifică, în principiu, suficient de clar și de precis cel puțin natura datelor pe care le vizează.

159. În ceea ce privește întinderea acestora, trebuie constatat, pe de o parte, că și articolul 3 alineatul (2) din Directiva API este redactat într-o manieră „deschisă”, lista de informații pe care o enumeră fiind precedată de expresia „[a]ceste informații includ următoarele”[150], și, pe de altă parte, că în categoria de date API, astfel cum este definită în instrumentele multilaterale de armonizare în domeniu, figurează de asemenea alte date decât cele menționate în Directiva API și la punctul 18 din anexa I[151].

148 Referitor la ceea ce este relevant în context, considerentul (9) are următorul cuprins: „[u]tilizarea datelor din PNR împreună cu datele API conferă valoare adăugată asistenței oferite statelor membre pentru verificarea identității unei persoane, consolidând, prin aceasta, valoarea rezultatului respectiv în ceea ce privește aplicarea legii și reducând la minimum riscul de a efectua verificări și cercetări cu privire la persoane nevinovate”.

149 În acest sens, a se vedea de asemenea propunerea de Directivă PNR, p. 7, punctul 1. Aceleași date sunt prevăzute de directivele privind informațiile prealabile privind pasagerii (RPCV) elaborate de Organizația Mondială a Vămilor (OMD), de Asociația privind transportul aerian internațional (IATA) și de OACI, http://www.wcoomd.org/~/media/wco/public/en/pdf/pdf/topics/facilitation/instruments-and-tools/api-guidelines-and-pnr-doc/api-guidelines-_e.pdf?db=web [(denumite în continuare „directivele RPCV”, punctul 8.1.5, litera (a)], ca fiind „principalele elemente de informații care pot fi incluse în zona lizibilă pe calculator a documentelor oficiale de călătorie”.

150 Articolul 3 alineatul (2) din Directiva API are următorul conținut: „[a]ceste informații includ următoarele: numărul și tipul documentului de călătorie utilizat; cetățenia; numele complet; data nașterii; punctul de trecere a frontierei utilizat pentru a intra pe teritoriul statelor membre; codul transportului; ora de plecare și ora de sosire a transportului; numărul total de persoane transportate; punctul inițial de îmbarcare”. Subliniem că, în programul său de lucru pentru anul 2022, COM(2021) 645 final, p. 9, Comisia a avut în vedere o actualizare a Directivei API. În septembrie 2020, Comisia a publicat o evaluare a acestei directive care era baza viitoarei sale revizuiri, SWD(2020) 174 final (denumit în continuare „documentul de lucru din anul 2020 cu privire la Directiva API”). În documentul menționat, Comisia subliniază, printre altele, că lista de informații cuprinsă la articolul 3 alineatul (2) din Directiva API nu este conformă cu standardele internaționale privind datele API, în special prin faptul că nu include toate datele existente în partea lizibilă pe calculator a documentelor de identitate (a se vedea în special p. 48).

151 A se vedea directivele RPCV, punctele 8.1.5, literele (b) și (c).

160. În aceste condiții, pentru ca punctul 18 din anexa I să îndeplinească cerințele de claritate și de precizie necesare pentru temeiurile juridice care implică o ingerință în articolele 7 și 8 din cartă, acesta trebuie interpretat în sensul că se referă numai la acele date API care sunt enumerate în mod expres la acest punct și la articolul 3 alineatul (2) din Directiva API și care au fost colectate de transportatorii aerieni în cadrul activităților lor obișnuite [152].

161. În această etapă, este oportun să trecem succint în revistă celelalte puncte din anexa I care, având în vedere modul lor de redactare, au de asemenea un caracter „deschis” sau nu sunt suficient de precise, chiar dacă instanța de trimitere nu a solicitat în mod expres Curții să se pronunțe cu privire la acestea [153].

162. Mai întâi, în ceea ce privește punctul 5 din anexa I, care menționează „adresă și informații de contact (număr de telefon, adresă de e-mail)”, deși trebuie considerat că acesta vizează numai datele de contact menționate în mod expres între paranteze și că are, prin urmare, un caracter exhaustiv, el nu precizează totuși, precum în cazul rubricii corespunzătoare din proiectul de Acord PNR Canada-UE [154], dacă aceste coordonate se referă numai la călător sau la terții care au făcut rezervarea zborului pentru pasagerul aerian, la terții prin intermediul cărora poate fi contactat un pasager aerian sau chiar la terții care trebuie informați în caz de urgență [155]. Întrucât interpretarea punctului 5 din anexa I în sensul că vizează și categoriile de terți menționate mai sus ar extinde ingerința cuprinsă în Directiva PNR la alți subiecți decât pasagerii aerieni în sensul articolului 3 alineatul (4) din Directiva PNR, propunem Curții, în lipsa unor date precise care să permită să se considere că dobândirea sistematică și generalizată a datelor acestor terți constituie un element strict necesar pentru eficacitatea sistemului de prelucrare a datelor din PNR instituit prin această directivă, să interpreteze acest punct în sensul că vizează numai datele menționate în mod expres în această directivă și care privesc pasagerul aerian în numele căruia se face rezervarea. Desigur, Directiva PNR nu exclude posibilitatea ca și datele cu caracter personal ale altor subiecți decât pasagerii aerieni să facă obiectul transferului către UIP [156]. Cu toate acestea, este esențial să se indice în mod clar și explicit cazurile în care acest lucru este posibil, cum este cazul agenților de turism, menționați la punctul 9 din anexa I, sau al tutorilor minorilor care călătoresc singuri, menționați la punctul 12 din anexa respectivă. Într-adevăr, numai dacă această condiție este îndeplinită, se poate considera că decizia de a include aceste date printre cele care urmează să fie transferate către UIP a făcut obiectul unei evaluări comparative între diferitele interese aflate în joc, în sensul considerentului (15) al Directivei PNR, și că terții în cauză pot fi informați în mod corespunzător cu privire la prelucrarea datelor lor cu caracter personal.

163. În ceea ce privește apoi punctul 6 din anexa I, care se referă la „[t]oate informațiile privind forma de plată, inclusiv adresa de facturare”, astfel cum a statuat Curtea la punctul 159 din Avizul 1/15, cu privire la rubrica corespunzătoare din anexa la proiectul de Acord PNR Canada-UE, pentru a îndeplini cerințele de claritate și precizie punctul respectiv trebuie să fie interpretat în sensul că „nu vizează decât informațiile privind modalitățile de plată și facturarea biletului de avion, fiind exclusă orice altă informație care nu are o legătură directă cu zborul”. Prin urmare,

152 O interpretare similară a rubricii corespunzătoare din proiectul de Acord PNR Canada-UE se regăsește la punctul 161 din Avizul 1/15.

153 Menționăm că, în prezent, Curtea este sesizată cu o serie de întrebări preliminare referitoare în special la caracterul suficient de precis al mai multor puncte din anexa I și în special al punctelor 4, 8, 12 și 18 (a se vedea cauza pendinte C-215/20).

154 A se vedea Avizul 1/15, punctul 158.

155 Observăm că informațiile privind agenția sau agentul de voiaj sunt deja menționate la punctul 5 din anexa I.

156 A se vedea definiția datelor din PNR de la articolul 3 punctul 5 din Directiva PNR.

aceste informații nu pot include, de exemplu, informațiile privind modalitățile de plată pentru alte servicii care nu sunt direct legate de zbor, cum ar fi închirierea unui autovehicul la sosire [157].

164. În ceea ce privește punctul 8, referitor la „[i]nformațiile din profilul «client fidel»”, acesta este definit de standardele OACI ca fiind legat de numărul de cont și de statutul clientului fidel [158]. Interpretat în acest sens, acest punct îndeplinește cerințele de claritate și precizie.

165. În ceea ce privește punctul 10 din anexa I, care vizează „[s]ituația de călătorie a pasagerului, inclusiv confirmările, situația înregistrării pentru zbor, informații privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare fără rezervare prealabilă”, și punctul 13 din anexa menționată, referitor la „[i]nformații despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu, câmpurile aferente furnizării automate a prețului unui bilet de călătorie”, în pofida formulării lor deschise, aceste puncte fac referire numai la informații foarte precise și clar identificabile legate direct de zbor. Același lucru este valabil și în ceea ce privește punctul 14 din anexa I, care face referire la „[n]umărul locului și alte informații privind locul”, și punctul 16 din această anexă, care vizează „[t]oate informațiile cu privire la bagaje”.

– *Cu privire la întinderea datelor enumerate în anexa I (a doua întrebare preliminară)*

166. Printre elementele pe care Curtea le ia în considerare atunci când evaluează proporționalitatea unei măsuri care implică ingerințe în exercitarea drepturilor consacrate la articolele 7 și 8 din cartă se numără caracterul adecvat, relevant și neexcesiv al datelor cu caracter personal prelucrate (principiul „minimizării datelor”) [159]. Același test este prevăzut în jurisprudența Curții EDO [160] și susținut de Convenția 108 [161].

167. Rezultă din considerentul (15) al Directivei PNR că lista datelor din PNR care urmează să fie transmise către UIP a fost stabilită cu scopul de a reflecta cerințele legitime ale autorităților publice din domeniul combaterii terorismului și a infracțiunilor grave, dar și de a proteja drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal prin aplicarea unor „standarde ridicate” în conformitate cu carta, Convenția 108 și CEDO. Același considerent precizează că datele din PNR ar trebui, printre altele, să conțină doar detalii privind rezervările pasagerilor și itinerariile călătoriilor, care permit autorităților competente să-i identifice pe acei pasageri ai curselor aeriene care reprezintă o amenințare pentru securitatea internă.

168. În ceea ce privește, în primul rând, caracterul adecvat și relevant al datelor din PNR prevăzute în anexa I, diferitele puncte din această anexă, inclusiv punctele 5, 6, 8 și 18, astfel cum propunem să fie interpretate [162], precum și punctul 12, cu excepția părții pentru care propunem

157 În acest sens, a se vedea de asemenea Concluziile avocatului general Mengozzi prezentate în Avizul 1/15 [(Acordul PNR Canada-UE), EU:C:2016:656], punctul 218.

158 A se vedea rubrica corespunzătoare din apendicele I la Orientările OACI.

159 A se vedea în acest sens în special Hotărârea Digital Rights, punctul 57. Cu privire la cerința privind limitarea categoriilor de date vizate de o măsură de acces la ceea ce este strict necesar pentru obiectivul urmărit, a se vedea în ultimă instanță Hotărârea Prokuratuur, punctul 38. Principiul reducerii la minimum a datelor este prevăzut, printre altele, la articolul 5 alineatul (1) litera (c) din RGPD și la articolul 4 alineatul (1) litera (c) din Directiva privind poliția.

160 A se vedea în special Curtea EDO, 18 aprilie 2013, M. K. împotriva Franței, (CE:ECHR:2013:0418JUD001952209, punctul 35).

161 A se vedea raportul explicativ privind Convenția 108 din anul 1981 (https://rm.coe.int/16800ca471), articolul 5, punctul 40, precum și Raportul explicativ privind Convenția 108 modernizată, articolul 5, punctul 51.

162 A se vedea punctele 154-158 și 162-164 din prezentele concluzii.

declararea nevalidității [163], vizează numai date care furnizează informații legate în mod direct de călătoriile aeriene care intră în domeniul de aplicare al Directivei PNR. Aceste date au în plus o legătură obiectivă cu scopurile urmărite de această directivă. În special, datele API pot fi utilizate în special într-un „mod reactiv", pentru a identifica o persoană deja cunoscută autorităților de aplicare a legii, de exemplu, pentru că este suspectată de implicare în infracțiuni de terorism sau în infracțiuni grave care au fost deja săvârșite sau este suspectată a fi pe punctul de a comite o astfel de infracțiune, în timp ce datele din PNR pot fi utilizate mai degrabă într-un „mod real sau proactiv", pentru a identifica amenințări care provin de la persoane care nu sunt încă cunoscute de serviciile de aplicare a legii.

169. În ceea ce privește, în al doilea rând, întinderea datelor din PNR enumerate în anexa I, aceste date, inclusiv cele enumerate la punctele 5, 6, 8, 12 și 18, astfel cum propunem să fie interpretate la punctele 134-164 din prezentele concluzii, nu sunt excesive, având în vedere, pe de o parte, importanța obiectivului de securitate publică urmărit de Directiva PNR și, pe de altă parte, caracterul adecvat al regimului instituit prin această directivă pentru a urmări un astfel de obiectiv.

170. În ceea ce privește mai ales datele API cu privire la care instanța de trimitere formulează întrebarea, subliniem că aceste date, care sunt de natură biografică și vizează traseul parcurs, nu permit, în general, decât obținerea unor informații limitate cu privire la viața privată a pasagerilor în cauză. Pe de altă parte, chiar dacă este adevărat că punctul 18 din anexa I se referă la informații care nu se numără printre cele menționate în mod expres la articolul 3 alineatul (2) din Directiva API, aceste informații, referitoare la identitatea pasagerului aerian (sex), la documentul de călătorie utilizat (țara emitentă, data expirării oricărui document de identitate) sau chiar la zborul efectuat (compania aeriană, numărul zborului, data și aeroportul de plecare și de sosire), se suprapun parțial sau pot fi extrase din datele din PNR prevăzute la alte puncte din anexa I, de exemplu punctele 3, 7 și 13. În plus, întrucât acestea privesc datele biografice sau documentele de călătorie utilizate, informațiile respective pot ajuta autoritățile de aplicare a legii să verifice identitatea unei persoane și să reducă astfel, după cum se menționează în considerentul (9) al Directivei PNR, riscul de a efectua verificări și cercetări nejustificate cu privire la persoane nevinovate. În sfârșit, trebuie subliniat că simplul fapt că punctul 18 din anexa I include date suplimentare față de cele prevăzute la articolul 3 alineatul (2) din Directiva API nu poate conduce în mod automat la constatarea caracterului excesiv al acestor date, întrucât această directivă și Directiva PNR urmăresc obiective diferite.

171. În ceea ce privește datele referitoare la minorii neînsoțiți, enumerate la punctul 12 din anexa I, acestea se referă la o categorie vulnerabilă de persoane care beneficiază de o protecție specială, inclusiv în ceea ce privește respectarea vieții private a acestora și protecția datelor lor cu caracter personal [164]. Nu este mai puțin adevărat că o limitare a acestor drepturi se poate dovedi necesară, în special pentru a proteja copiii de forme grave de criminalitate cărora le pot fi victime, precum traficul și exploatarea sexuală a copiilor sau răpirea copiilor. Prin urmare, nu se poate considera *a priori* că punctul 12 din anexa I depășește ceea ce este strict necesar prin faptul că impune transferul unui număr mai mare de date cu caracter personal în ceea ce privește minorii neînsoțiți.

[163] A se vedea punctele 133-153 din prezentele concluzii.

[164] Dreptul copilului la respectarea vieții sale private este consacrat în articolul 16 din Convenția de la New York privind drepturile copilului, adoptată la 20 noiembrie 1989 și intrată în vigoare la 2 septembrie 1990.

172. Chiar dacă datele cu caracter personal pe care transportatorii aerieni sunt obligați să le transmită către UIP în conformitate cu Directiva PNR îndeplinesc, în opinia noastră, cerințele de adecvare și de relevanță și întinderea lor nu depășește ceea ce este strict necesar pentru funcționarea regimului instituit prin această directivă, nu este mai puțin adevărat că o astfel de transmitere implică o cantitate importantă de date cu caracter personal de diferite tipuri pentru fiecare pasager în cauză, precum și un număr extrem de mare de astfel de date în termeni absoluți. În aceste împrejurări, este esențial ca un astfel de transfer să fie însoțit de garanții suficiente pentru a se asigura, pe de o parte, transferul doar al datelor vizate în mod expres și, pe de altă parte, garantarea securității și confidențialității datelor transferate.

173. În această privință, trebuie remarcat, pe de o parte, că legiuitorul Uniunii a prevăzut mai întâi o serie de garanții care permit limitarea categoriilor de date din PNR accesibile autorităților de aplicare a legii și asigurarea faptului că acest acces rămâne limitat la datele a căror prelucrare este considerată necesară pentru obiectivele urmărite de Directiva PNR. Astfel, în primul rând, această directivă enumeră, sub rezerva considerațiilor dezvoltate în cadrul răspunsului la a treia întrebare preliminară, în mod exhaustiv și exact datele care pot fi transferate către UIP. În al doilea rând, Directiva PNR prevede în mod explicit că numai datele conținute în această listă, care este rezultatul unui evaluări comparative între diferitele interese și cerințe menționate în considerentul (15) al acestei directive, pot fi transferate către UIP [articolul 6 alineatul (1) din Directiva PNR]. În al treilea rând, această directivă specifică faptul că, în cazul în care datele din PNR transferate includ alte date decât cele enumerate în anexa I, UIP le șterge „imediat și definitiv la primirea lor” [articolul 6 alineatul (1) din Directiva PNR]. În al patrulea rând, directiva respectivă prevede că datele din PNR menționate în anexa I pot fi transferate numai în măsura în care au fost deja colectate de transportatorii aerieni în cadrul activităților lor obișnuite [articolul 8 alineatul (1) și considerentul (8) al Directivei PNR], ceea ce implică faptul că nu toate datele prevăzute în anexa I sunt accesibile în mod sistematic pentru UIP, ci numai cele conținute în sistemul de rezervare al operatorului în cauză. În al cincilea rând, articolul 8 alineatul (1) din Directiva PNR prevede că transportatorii aerieni trebuie să utilizeze metoda „push” pentru a transmite datele din PNR către UIP. Această metodă, recomandată de Orientările OACI[165], presupune ca transportatorii aerieni să transfere ei înșiși datele din PNR în bazele de date ale UIP. În comparație cu metoda „pull”, care permite autorităților competente să acceadă la sistemele operatorilor și să extragă o copie a datelor solicitate din bazele de date ale acestora, metoda „push” oferă mai multe garanții, întrucât îi conferă transportatorului aerian în cauză rolul de custode și de controlor al datelor din PNR. În sfârșit, pentru a se conforma Orientărilor OACI și principiului „ghișeului unic”[166], Directiva PNR prevede că transferul datelor din PNR intervine prin intermediul unui singur organism, UIP, care acționează sub supravegherea responsabilului menționat la articolul 5 din directivă și în special sub cea a autorității naționale de supraveghere menționate la articolul 15 din directivă.

174. Pe de altă parte, Directiva PNR prevede o serie de garanții menite să asigure *securitatea* datelor din PNR. Facem referire în această privință la articolul 13 alineatul (2) din directiva respectivă, care permite aplicarea articolelor 28 și 29 din Directiva privind poliția în cazul tuturor prelucrărilor de date cu caracter personal efectuate în temeiul acesteia, în ceea ce privește confidențialitatea prelucrării și securitatea datelor, precum și la alineatul (3) al aceluiași articol care, în ceea ce privește prelucrarea datelor din PNR de către transportatorii aerieni, reamintește

165 A se vedea punctul 2.7.3 din Orientările OACI.

166 A se vedea punctul 2.7.4 din Orientările OACI.

obligațiile care le revin acestora din urmă în temeiul RGPD, în special în legătură cu măsurile tehnice și organizatorice adecvate care trebuie luate pentru a proteja securitatea și confidențialitatea acestor date [167].

175. În sfârșit, trebuie subliniat că Directiva PNR recunoaște, în considerentele (29) și (37), dreptul pasagerilor de a li se furniza „informații corecte, ușor accesibile și ușor de înțeles", printre altele, cu privire la colectarea datelor din PNR, solicitând statelor membre să se asigure că acest drept este respectat. Chiar dacă această recunoaștere nu se regăsește în textul Directivei PNR sub forma unei dispoziții obligatorii, reamintim că, astfel cum am arătat cu ocazia examinării primei întrebări preliminare, dispozițiile din RGPD se aplică transferului de date din PNR către UIP. În consecință, transportatorii aerieni sunt obligați, în contextul acestui transfer, să respecte, printre altele, articolele 13 și 14 din RGPD, care prevăd dreptul la informare al persoanelor vizate de prelucrarea datelor cu caracter personal. Chiar dacă ar fi oportun ca, în contextul transpunerii Directivei PNR, statele membre să prevadă în mod expres dreptul la informare al pasagerilor aerieni, astfel cum este recunoscut de considerentele (29) și (37) ale acestei directive, acestea nu pot în orice caz să limiteze domeniul de aplicare al articolelor 13 și 14 din RGPD în conformitate cu articolul 23 alineatul (1) din RGPD, întrucât acest lucru ar fi contrar spiritului directivei. Or, pentru a fi eficient, un astfel de drept trebuie să acopere și categoriile de date din PNR care fac obiectul transferului.

176. Având în vedere toate considerațiile menționate anterior, considerăm că datele din PNR a căror prelucrare este prevăzută de Directiva PNR, sub rezerva limitărilor sugerate și a precizărilor făcute în contextul celei de a treia întrebări preliminare, sunt relevante, adecvate și neexcesive în raport cu obiectivele urmărite de această directivă și că întinderea lor de aplicare nu depășește ceea ce este strict necesar pentru atingerea acestor obiective.

– *Cu privire la datele sensibile*

177. Directiva PNR interzice, într-un mod general, orice prelucrare a „datelor sensibile" [168].

178. Chiar dacă această directivă nu conține o definiție a noțiunii de „date sensibile", rezultă din articolul 13 alineatul (4) din aceasta că directiva include cel puțin „datele din PNR care dezvăluie rasa sau originea etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală a unei persoane" [169]. La punctul 165 din Avizul 1/15, Curtea a precizat că orice măsură întemeiată pe postulatul că una sau mai multe dintre aceste caracteristici „ar putea, prin ele însele și independent de comportamentul individual al călătorului vizat, să fie relevante din perspectiva finalității prelucrării datelor PNR […] ar încălca drepturile garantate la articolele 7 și 8 din cartă coroborate cu articolul 21 din aceasta". Prin interzicerea oricărei prelucrări a datelor menționate la articolul 13 alineatul (4), Directiva PNR respectă deci limitele impuse de Curte utilizării acestor categorii de date în cadrul unui sistem de prelucrare a datelor din PNR, indiferent că acesta este reglementat de dreptul intern, de dreptul Uniunii sau de un acord internațional încheiat de Uniune.

[167] Cerința de a asigura securitatea și fiabilitatea transferului de date către UIP este menționată de altfel la articolul 16 alineatul (1) din Directiva PNR în legătură cu mijloacele electronice utilizate pentru acest transfer și a fost unul dintre criteriile pe care Comisia le-a respectat pentru adoptarea, în conformitate cu alineatul (3) al acestui articol, a protocoalelor comune și a formatelor de date care trebuie utilizate de transportatorii aerieni cu ocazia transferului menționat; a se vedea Decizia de punere în aplicare (UE) 2017/759 a Comisiei din 28 aprilie 2017 privind protocoalele comune și formatele de date care trebuie să fie utilizate de transportatorii aerieni la transferul datelor PNR către unitățile de informații despre pasageri (JO 2017, L 113, p. 48).

[168] A se vedea considerentul (37) al Directivei PNR.

[169] Categoriile de date cu caracter personal enumerate la articolul 13 alineatul (4) din Directiva PNR sunt toate incluse în noțiunea de „categorii speciale de date cu caracter personal" menționate la articolul 9 alineatul (1) din RGPD.

179. Interdicția generală de prelucrare a datelor sensibile stabilită de Directiva PNR include și *colectarea* acestora. Astfel, după cum se menționează în mod expres în considerentul (15) al acestei directive, cele 19 rubrici prevăzute în anexa I nu se bazează pe datele din PNR menționate la articolul 13 alineatul (4) din directivă.

180. Chiar dacă niciuna dintre aceste rubrici nu vizează în mod explicit astfel de date, acestea ar putea totuși să intre sub incidența rubricii „Mențiuni cu caracter general” prevăzute la punctul 12 din anexa I, care constituie un „domeniu deschis” care ar putea, astfel cum am avut deja ocazia să observăm în cadrul analizei celei de a treia întrebări preliminare, să acopere un număr nedeterminat de informații de diferite tipuri. Într-adevăr, există un risc real, astfel cum a subliniat Curtea la punctul 164 din Avizul 1/15, ca informații prevăzute în această rubrică, referitoare, de exemplu, la preferințele dietetice, la solicitările de asistență, la pachetele tarifare pentru anumite categorii de persoane sau asociații să dezvăluie în mod direct date sensibile în sensul articolului 13 alineatul (4) din Directiva PNR, în legătură în special cu convingerile religioase ale pasagerilor în cauză, cu starea lor de sănătate sau cu apartenența lor la un sindicat sau la un partid politic.

181. Or, întrucât prelucrarea acestor date este în orice caz exclusă de Directiva PNR, transferul lor de către transportatorii aerieni nu numai că depășește în mod vădit ceea ce este strict necesar, dar se dovedește de asemenea lipsit de orice utilitate. În această privință, este important de subliniat că oricum obligația UIP, în conformitate cu articolul 13 alineatul (4) a doua teză din Directiva PNR, de a șterge imediat datele din PNR care dezvăluie oricare dintre informațiile enumerate în prima teză a acestui alineat nu permite autorizarea sau justificarea unui transfer al acestor date [170], întrucât interdicția de prelucrare a acestora prevăzută de directiva menționată trebuie să se aplice încă din prima etapă de prelucrare a datelor din PNR. Prin urmare, obligația de a șterge datele sensibile constituie numai o garanție suplimentară pe care directiva o prevede în cazul în care, în mod excepțional, astfel de date sunt transferate din greșeală către UIP.

182. Constatăm, în plus, astfel cum a subliniat domnul avocat general Mengozzi la punctul 222 din concluziile prezentate în Avizul 1/15 [171], că, întrucât informațiile prevăzute la rubricile de tip „text liber”, precum rubrica „Mențiuni cu caracter general”, menționată la punctul 12 din anexa I, care pot conține date sensibile în temeiul articolului 13 alineatul (4) din Directiva PNR, sunt comunicate de pasageri numai în mod facultativ, este puțin probabil ca persoanele implicate în infracțiuni de terorism sau infracțiuni grave să facă o astfel de comunicare spontană, astfel încât transferul sistematic al acestor date nu este probabil de natură să vizeze, în cea mai mare parte, decât persoane care au solicitat să beneficieze de un serviciu suplimentar care, în realitate, nu prezintă niciun interes pentru autoritățile de aplicare a legii [172].

183. În cadrul analizei celei de a treia întrebări preliminare, am ajuns la concluzia că punctul 12 din anexa I, în măsura în care se referă la rubrica „Mențiuni cu caracter general”, nu îndeplinește cerințele de claritate și precizie impuse de articolul 52 alineatul (1) prima teză din cartă. Pentru motivele pe care tocmai le-am prezentat, considerăm că nici includerea acestei rubrici în

[170] În această privință, considerăm irelevante afirmațiile făcute de o serie de state membre care au prezentat observații cu privire la a doua întrebare preliminară, întemeiate pe existența unor mijloace tehnice care permit ștergerea cu ușurință a datelor sensibile transmise de transportatorii aerieni.

[171] Concluziile avocatului general Mengozzi prezentate în Avizul 1/15 (Acordul PNR Canada-UE), EU:C:2016:656.

[172] Observăm că inclusiv Orientările OACI, chiar dacă nu exclud posibilitatea ca datele sensibile care pot fi extrase de la rubricile de tip „text liber” să fie utile la evaluarea riscului pe care îl poate prezenta un pasager, recomandă totuși ca statele contractante să se asigure că acestea sunt luate în considerare numai dacă există indicii concrete care să impună utilizarea lor în scopurile urmărite de regimurile lor privind PNR.

categoriile de date care fac obiectul unui transfer sistematic către UIP, fără nicio precizare a informațiilor pe care le poate viza, nu îndeplinește criteriul de necesitate prevăzut la articolul 52 alineatul (1) a doua teză din cartă, astfel cum a fost interpretat de Curte [173].

184. În aceste condiții, excluderea rubricilor denumite „text liber” din lista datelor din PNR care urmează să fie transferate autorităților statului în cadrul unui sistem de prelucrare a datelor din PNR nu este suficientă pentru a elimina riscul ca datele sensibile să fie totuși puse la dispoziția autorităților respective. Într-adevăr, astfel de date pot fi nu numai deduse în mod direct din informațiile din astfel de rubrici, ci pot fi dezvăluite sau prezumate și în mod indirect prin informații cuprinse în rubricile „codificate”. De exemplu, numele pasagerului aerian poate să furnizeze indicații sau cel puțin să permită formularea de ipoteze cu privire la originea etnică sau la apartenența religioasă a pasagerului în cauză. Același lucru este valabil și pentru naționalitate. În principiu, aceste date nu pot fi excluse din lista datelor din PNR care urmează să fie transferate și nici nu pot fi șterse de autoritățile abilitate să le primească. În consecință, pentru a evita riscul de stigmatizare, pe baza caracteristicilor protejate, a unui număr mare de persoane care nu sunt totuși suspectate de nicio infracțiune, este important ca un sistem de prelucrare a datelor din PNR să prevadă garanții suficiente pentru a exclude, în fiecare etapă a prelucrării datelor colectate, posibilitatea ca această prelucrare să ia în considerare, în mod direct sau indirect, astfel de caracteristici, de exemplu, prin aplicarea, cu ocazia analizei automatizate, a unor elemente de selecție care au la bază aceste caracteristici. Vom reveni asupra acestui aspect în continuarea analizei noastre.

185. Pe baza tuturor considerațiilor menționate anterior, apreciem, sub rezerva concluziei la care am ajuns la punctul 183 de mai sus, că Directiva PNR prevede, în etapa de transfer al datelor din PNR către UIP, garanții suficiente pentru protejarea datelor sensibile.

iii) Cu privire la noțiunea de „pasager” (a patra întrebare preliminară)

186. Prin intermediul celei de a patra întrebări preliminare, instanța de trimitere solicită în esență Curții să stabilească dacă sistemul instituit prin Directiva PNR, dat fiind că permite transferul și prelucrarea generalizate ale datelor din PNR ale oricărei persoane care corespunde noțiunii de „pasager”, în sensul articolului 3 punctul 4 din această directivă, independent de orice element obiectiv care permite să se considere că această persoană poate prezenta un risc pentru securitatea publică, este compatibil cu articolele 7, 8 și 52 alineatul (1) din cartă. În special, aceasta ridică întrebări cu privire la posibilitatea de a transpune jurisprudența Curții în materie de stocare a datelor și de acces la datele din sectorul comunicațiilor electronice în cazul sistemului de prelucrare a datelor cu caracter personal instituit prin Directiva PNR.

187. În cadrul acestei jurisprudențe, legat de ceea ce prezintă interes în prezenta procedură, Curtea a concluzionat că o reglementare care prevede, în vederea combaterii infracționalității grave, *stocarea* generalizată și nediferențiată a datelor de transfer aferente comunicațiilor electronice și a datelor de localizare [174], pentru a oferi acces autorităților de aplicare a legii, fără nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit, nu poate fi considerată, în

[173] Reamintim că o astfel de excludere a fost deja sugerată de CEPD în Avizul său din 25 martie 2011, punctul 47.

[174] Acestea sunt date care pot furniza informații privind comunicațiile efectuate de un utilizator printr-un mijloc electronic de comunicare sau privind localizarea echipamentelor terminale utilizate de acesta.

principiu, justificată într-o societate democratică [175]. Curtea a susținut același lucru în ceea ce privește o reglementare națională care, în vederea combaterii terorismului, prevedea *analiza automatizată a tuturor datelor menționate* prin intermediul unei filtrări efectuate de furnizorii de servicii de comunicații electronice la cererea autorităților naționale competente și cu aplicarea unor parametri stabiliți de acestea [176]. Potrivit Curții, astfel de măsuri pot fi justificate numai în situațiile în care un stat membru se confruntă cu o amenințare gravă la adresa securității naționale, care se dovedește reală și actuală sau previzibilă și în condițiile în care decizia care prevede punerea lor în aplicare face obiectul unui control efectiv fie din partea unei instanțe, fie a unei entități administrative independente [177]. În plus, potrivit Curții, recurgerea la aceste măsuri în astfel de situații trebuie să fie limitată în timp la strictul necesar și nu poate avea, în orice caz, un caracter sistematic [178].

188. În plus, subliniem că, deși în această jurisprudență Curtea nu a mers până într-acolo încât să afirme în mod expres, precum în Hotărârea Schrems I, că există o încălcare a substanței dreptului la respectarea vieții private, aceasta a considerat totuși că măsurile în cauză au atins un nivel de gravitate a ingerinței de așa natură încât, cu excepția cazului limitat al unor amenințări specifice la adresa securității naționale a unui stat membru, acestea pur și simplu nu pot fi considerate ca fiind limitate la strictul necesar și, prin urmare, conforme cu carta [179], indiferent de garanțiile prevăzute împotriva riscurilor de abuz și de acces ilegal la datele în cauză [180].

189. Am avut deja ocazia să subliniem că o reglementare precum cea prevăzută de Directiva PNR are în comun cu măsurile de tipul celor examinate de Curte în jurisprudența menționată la punctele precedente din prezentele concluzii o serie de elemente comune care îi conferă un caracter deosebit de intruziv. Astfel, directiva instituie un sistem generalizat și nediferențiat de stocare și de analiză automatizată a datelor cu caracter personal ale unei părți semnificative a populației, care se aplică în mod global tuturor persoanelor care se încadrează în noțiunea de „pasager” de la articolul 3 alineatul (4) din directivă și, în consecință, chiar și celor față de care nu există niciun indiciu care să sugereze că comportamentele acestor persoane ar putea avea o legătură, chiar indirectă sau îndepărtată, cu activități teroriste sau cu infracțiuni grave. În aceste condiții, instanța de trimitere ridică întrebarea dacă această jurisprudență poate fi transpusă în cazul unui sistem de prelucrare a datelor din PNR precum cel instituit de Directiva PNR.

190. În această privință, observăm că atunci când Curtea a examinat, la punctele 186-189 din Avizul 1/15, domeniul de aplicare *ratione personae* al proiectului de Acord PNR Canada-UE, aceasta a evitat orice paralelism între, pe de o parte, măsurile care vizează stocarea și accesul generalizat și nediferențiat la conținutul comunicațiilor electronice, la datele de transfer și la datele de localizare și, pe de altă parte, transferul de date din PNR și prelucrarea lor automatizată

175 A se vedea în acest sens Hotărârea La Quadrature du Net, punctele 141-145, și Hotărârea Tele2 Sverige, punctele 105 și 106, pronunțate în contextul interpretării articolului 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, precum și Hotărârea Digital Rights, punctele 57 și 58, în care Curtea a anulat Directiva 2006/24.

176 A se vedea Hotărârea La Quadrature du Net, punctul 177.

177 A se vedea Hotărârea La Quadrature du Net, punctele 134-139 și 177. Potrivit Curții, responsabilitatea care revine statelor membre în domeniul securității naționale „corespunde interesului primordial de a proteja funcțiile esențiale ale statului și interesele fundamentale ale societății și include prevenirea și sancționarea activităților de natură 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 ca atare, cum ar fi printre altele activitățile de terorism”; a se vedea Hotărârea La Quadrature du Net, punctul 135, și Hotărârea Privacy International, punctul 74.

178 A se vedea Hotărârea La Quadrature du Net, punctele 138 și 178.

179 A se vedea în special Hotărârea Quadrature du Net, punctele 141-145.

180 A se vedea Hotărârea La Quadrature du Net, punctele 115 și 116; a se vedea de asemenea Concluziile avocatului general Campos Sanchéz-Bordona prezentate în cauzele conexate SpaceNet și Telekom Deutschland (C-793/19 și C-794/19, EU:C:2021:939, punctele 74 și 75).

în contextul evaluării prealabile a pasagerilor menționate în acordul respectiv. Exista însă deja, la momentul pronunțării avizului, o jurisprudență consacrată – confirmată, cu numai câteva luni înainte de pronunțarea avizului, prin Hotărârea Tele2 Sverige la care face referire instanța de trimitere – în care măsurile menționate erau considerate incompatibile cu carta [181], cu excepția unor situații specifice și punctuale [182]. Cele mai recente hotărâri ale Curții în acest domeniu și în special Hotărârea La Quadrature du Net se înscriu pe linia acestei jurisprudențe, clarificând-o și, în anumite privințe, nuanțând-o.

191. La punctele menționate din Avizul 1/15, Curtea a considerat în mod explicit că nu rezulta că Acordul PNR Canada-UE depășea limitele strictului necesar, întrucât permitea *transferul* și *prelucrarea automatizată* ale datelor din PNR ale tuturor pasagerilor aerieni cu destinația Canada în scopul evaluării prealabile a acestora, în pofida faptului că un astfel de transfer și o astfel de prelucrare erau menite să aibă loc „independent de orice element obiectiv care permite să se considere că pasagerii pot să prezinte un risc pentru securitatea publică în Canada” [183]. La punctul 187 din acest aviz, Curtea a mers până într-acolo încât a afirmat că „excluderea anumitor categorii de persoane sau a anumitor zone de origine ar fi de natură să împiedice realizarea obiectivului prelucrării automate a datelor PNR, și anume identificarea, prin intermediul verificării acestor date, a persoanelor care pot prezenta un risc pentru securitatea publică din rândul tuturor pasagerilor aerieni, și să permită ca această verificare să fie evitată” [184].

192. Astfel, cel puțin în ceea ce privește transferul generalizat și nediferențiat al datelor din PNR, Curtea s-a delimitat de abordarea mai riguroasă adoptată în materie de stocare și de acces la metadate.

193. Deși este de netăgăduit că, în motivarea sa, Curtea a luat în considerare, astfel cum reiese în special din cuprinsul punctelor 152 și 188 din Avizul 1/15, pe de o parte, constatarea că prelucrarea automatizată a datelor din PNR facilitează controalele de securitate, în special la frontiere, și, pe de altă parte, faptul că, în conformitate cu Convenția de la Chicago, pasagerii aerieni care doresc să intre pe teritoriul unui stat care este parte la această convenție sunt obligați să se supună controalelor și să respecte condițiile de intrare și de ieșire stabilite de statul respectiv, inclusiv verificarea datelor lor din PNR, considerăm că există și alte motive care justifică o astfel de diversitate de abordare și, printre acestea, în primul rând, natura datelor prelucrate.

194. Curtea a subliniat în repetate rânduri că nu numai conținutul comunicațiilor electronice, ci și metadatele pot dezvălui informații despre „un număr important de aspecte ale vieții private a persoanelor în cauză, inclusiv informații sensibile precum orientarea sexuală, opiniile politice, convingerile religioase, filozofice, sociale sau de altă natură, precum și starea de sănătate”, că aceste date, în ansamblul lor, „pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost stocate, precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele” și că datele respective furnizează în special mijloacele de a stabili „profilul persoanelor în cauză, informație la fel de sensibilă, din perspectiva dreptului la respectarea vieții private, ca și conținutul însuși al

181 A se vedea în acest sens Hotărârea Tele2 Sverige, punctele 103-107 și 119, precum și jurisprudența citată.

182 A se vedea Hotărârea Tele2 Sverige, punctul 119.

183 A se vedea Avizul 1/15, punctele 186 și 187.

184 În Hotărârile Digital Rights (punctul 59) și Tele2 Sverige (punctul 111), precum și în jurisprudența ulterioară (a se vedea în special Hotărârea La Quadrature du Net, punctele 143-150), tocmai faptul că reglementarea în cauză nu se baza pe „elemente obiective” de tipul celor menționate de Curte la punctul 187 din Avizul 1/15, care să permită să fie vizat un public ale cărui date puteau dezvălui cel puțin indirect o legătură cu infracțiuni grave, a făcut ca această reglementare să nu fie proporțională.

comunicațiilor”[185]. În plus, reamintim că reglementările examinate până în prezent de Curte, inclusiv cea cuprinsă în Directiva 2006/24, nu prevedeau nicio excepție și se aplicau de asemenea comunicărilor către sau de la servicii cu caracter social ori religios sau de la profesioniști supuși obligației de păstrare a secretului profesional. Astfel, chiar dacă nu a stabilit o încălcare a substanței dreptului la respectarea vieții private, Curtea a afirmat totuși că, „ținând seama de caracterul sensibil al informațiilor pe care le pot furniza datele de transfer și datele de localizare, confidențialitatea acestora din urmă este esențială pentru dreptul la respectarea vieții private”[186].

195. În schimb, deși este adevărat că, astfel cum am reamintit la punctele 77 și 98 din prezentele concluzii, Curtea a recunoscut în Avizul 1/15 că datele din PNR pot eventual să dezvăluie informații foarte prețioase cu privire la viața privată a unei persoane[187], aceasta a precizat totuși că natura informațiilor respective este limitată la anumite aspecte ale acestei vieți private[188], ceea ce face ca accesul la astfel de date să fie mai puțin intruziv decât accesul la conținutul comunicațiilor electronice, precum și la datele de transfer și de localizare.

196. În al doilea rând, nu numai natura datelor din PNR diferă de cea a datelor de transfer și a datelor de localizare, ci și numărul și varietatea informațiilor care pot fi dezvăluite prin aceste diferite categorii de date, informațiile conținute în datele PNR fiind mai limitate atât din punct de vedere cantitativ, cât și calitativ. Acest lucru depinde nu numai de faptul că sistemul de prelucrare generalizată și nediferențiată a datelor privind comunicațiile electronice poate privi aproape întreaga populație vizată, în timp ce sistemele de prelucrare a datelor din PNR se aplică unui cerc mai restrâns de persoane, deși semnificativ din punct de vedere numeric, dar și de frecvența utilizării mijloacelor de comunicații electronice și de multiplicitatea acestora. În plus, Directiva PNR prevede stocarea și prelucrarea unui număr limitat și definit în mod exhaustiv de date din PNR, cu excepția datelor care se încadrează în categoriile enumerate la articolul 13 alineatul (4) din această directivă, astfel încât, dacă nu cantitatea, cel puțin sensibilitatea informațiilor privind viața privată a persoanelor vizate care pot fi obținute din acestea este susceptibilă de a fi, în parte, evaluată în prealabil[189]. Or, o astfel de limitare a tipologiei datelor în cauză, care ar permite excluderea unei mari părți a celor care pot conține informații sensibile, este numai parțial posibilă în cazul datelor de transfer și al datelor de localizare, ținând cont de numărul de utilizatori și de mijloacele de comunicare în cauză[190].

197. În al treilea rând, orice prelucrare a metadatelor comunicațiilor electronice este susceptibilă nu numai să afecteze sfera intimă a vieții aproape întregii populații, ci și să impieteze asupra exercitării altor libertăți prin intermediul cărora se realizează participarea fiecărui individ la viața socială și democratică a unei țări[191] și riscă mai ales să aibă un efect disuasiv asupra libertății de exprimare a utilizatorilor mijloacelor de comunicații electronice[192], care constituie „unul dintre

185 A se vedea Hotărârea La Quadrature du Net (punctul 117 și jurisprudența citată); a se vedea de asemenea Hotărârea Prokuratuur (punctul 36).

186 Hotărârea La Quadrature du Net, punctul 142.

187 A se vedea Avizul 1/15, punctele 128 și 150.

188 A se vedea Avizul 1/15, punctul 150.

189 Cu privire la dificultatea unei astfel de evaluări în ceea ce privește metadatele, a se vedea Hotărârea Prokuratuur, punctul 40.

190 Un efort în acest sens a fost făcut de legiuitorul german în reglementarea care face obiectul cauzelor conexate C-793/19 și C-794/19, SpaceNet și Telekom Deutschland, în care avocatul general Campos Sánchez-Bordona a prezentat concluzii (EU:C:2021:939, punctele 60 și 61).

191 În această privință, facem referire la punctul 93 din prezentele concluzii.

192 A se vedea Hotărârea La Quadrature du Net, punctul 118 și jurisprudența citată.

fundamentele esențiale al unei societăți democratice și pluraliste" care face parte dintre valorile pe care se întemeiază Uniunea [193]. Acest aspect este inerent măsurilor referitoare la aceste categorii de date cu caracter personal și nu privește, în principiu, sistemele de prelucrare a datelor din PNR.

198. În al patrulea rând, în principal din cauza numărului și a varietății informațiilor cu caracter sensibil care pot fi extrase din conținutul comunicațiilor electronice, precum și din datele de transfer și de localizare, există un risc semnificativ mai mare de prelucrare arbitrară a acestor date decât în ceea ce privește sistemele de prelucrare a datelor din PNR.

199. Pentru toate motivele pe care tocmai le-am menționat, considerăm că abordarea mai strictă adoptată de Curte în domeniul comunicațiilor electronice nu poate fi transpusă ca atare în cazul sistemelor de prelucrare a datelor din PNR. Curtea s-a exprimat deja, cel puțin implicit, în acest sens în Avizul 1/15, în contextul unui acord internațional care instituie un astfel de sistem în scopul protejării securității unei țări terțe. Aceeași poziție este, în opinia noastră, cu atât mai justificată în cazul Directivei PNR, al cărei obiectiv este protecția securității interne a Uniunii.

200. Acestea fiind spuse, trebuie remarcat, astfel cum a procedat domnul avocat general Mengozzi la punctul 216 din concluziile prezentate în Avizul 1/15 [194], că însuși interesul sistemelor de prelucrare a datelor din PNR, fie că sunt adoptate în mod unilateral, fie că fac obiectul unui acord internațional, este tocmai acela de a garanta transmiterea masivă de date care permit autorităților competente să identifice, cu ajutorul unor instrumente de prelucrare automată și al unor scenarii sau criterii de evaluare prestabilite, persoane care nu sunt cunoscute de serviciile de aplicare a legii, dar care par să prezinte un „interes" sau un risc pentru siguranța publică și care sunt, în consecință, susceptibile să fie supuse ulterior unor controale individuale mai exigente. În consecință, cerința existenței unei „suspiciuni rezonabile" pe care o regăsim evocată în jurisprudența Curții EDO referitoare la interceptările direcționate efectuate în contextul unei anchete penale [195] și în jurisprudența Curții privind stocarea metadatelor [196] este mai puțin relevantă în contextul unei astfel de transmiteri și prelucrări [197]. De asemenea, obiectivul îndeosebi de prevenție urmărit de astfel de sisteme nu poate fi atins prin limitarea aplicării lor la o categorie determinată de persoane, astfel cum a afirmat de altfel Curtea la punctele din Avizul 1/15 menționate la punctul 191 din prezentele concluzii, astfel încât rezultă că domeniul de aplicare al Directivei PNR garantează realizarea efectivă a acestui obiectiv [198].

201. Trebuie de asemenea subliniat că importanța strategică a prelucrării datelor din PNR ca instrument esențial al răspunsului comun al Uniunii în fața terorismului și a infracțiunilor grave și ca o componentă majoră a Uniunii privind securitatea a fost evidențiată de mai multe ori de Comisie [199]. În cadrul unei „abordări globale" în combaterea terorismului, rolul jucat de sistemele de prelucrare a datelor din PNR a fost recunoscut și de Consiliul de Securitate al Organizației Națiunilor Unite care, în Rezoluția 2396 (2017) [200], a solicitat statelor membre ale Organizației Națiunilor Unite să „își consolideze capacitatea de a colecta, prelucra și analiza, în cadrul

193 A se vedea Hotărârea Tele2 Sverige, punctul 93.

194 Concluziile avocatului general Mengozzi prezentate în Avizul 1/15 [(Acordul PNR Canada-UE), EU:C:2016:656].

195 A se vedea în special Curtea EDO, 4 decembrie 2015, Roman Zakharov împotriva Rusiei (CE:ECHR:2015:1204JUD004714306, punctul 260).

196 A se vedea Hotărârile La Quadrature du Net (punctele 146-151) și Tele2 Sverige (punctul 119).

197 În acest sens, în ceea ce privește măsurile de interceptare în masă, a se vedea Hotărârea Big Brother Watch, punctul 348.

198 A se vedea prin analogie Hotărârea din 3 octombrie 2019, A și alții (C-70/18, EU:C:2019:823, punctul 61).

199 A se vedea recent Comunicarea Comisiei referitoare la Strategia UE privind uniunea securității [COM(2020) 605 final, p. 28], precum și Comunicarea Comisiei: Agenda UE privind combaterea terorismului: anticipare, prevenire, protejare și răspuns [COM(2020) 795 final, p. 15 și urm.].

200 Rezoluția din 21 decembrie 2017 [denumită în continuare „Rezoluția 2396 (2017)"], https://undocs.org/fr/S/RES/2396(2017).

standardelor și al practicilor recomandate de OACI, datele din [PNR] și să se asigure că aceste date sunt comunicate tuturor autorităților naționale competente și utilizate de către acestea cu respectarea deplină a drepturilor omului și a libertăților fundamentale, în scopul prevenirii, depistării și investigării infracțiunilor de terorism și al deplasărilor efectuate de teroriști”[201]. Această obligație este reafirmată în Rezoluția 2482/2019, în domeniul terorismului și al infracțiunilor transnaționale grave[202].

202. În acest context, adoptarea unui sistem armonizat de prelucrare a datelor din PNR la nivelul Uniunii, în ceea ce privește atât zborurile extra-UE, cât și, în cazul statelor care au aplicat articolul 2 din Directiva PNR, zborurile intra-UE, permite garantarea faptului că prelucrarea acestor date se face în conformitate cu nivelul ridicat de protecție a drepturilor consacrate la articolele 7 și 8 din cartă, prevăzut de această directivă, și oferă un sistem juridic de referință pentru negocierea acordurilor internaționale privind prelucrarea și transferul datelor din PNR[203].

203. În plus, chiar dacă este adevărat că sistemul instituit prin Directiva PNR vizează în mod nediferențiat toți pasagerii aerieni, astfel cum a subliniat în mod corect în special Parlamentul în observațiile sale scrise și cum a evidențiat de asemenea Consiliul de Securitate al Organizației Națiunilor Unite în Rezoluția 2396 (2017), care face referire la riscul concret de utilizare a aviației civile în scopuri teroriste atât ca mijloc de transport, cât și ca țintă[204], există o legătură obiectivă între transportul aerian și amenințările la adresa securității publice, referitoare în special la terorism și cel puțin la anumite forme de infracțiuni grave, cum ar fi în special traficul de droguri sau de ființe umane care au în fond au o puternică componentă transfrontalieră.

204. În sfârșit, este important de subliniat, astfel cum au susținut Parlamentul, Consiliul și mai multe state membre care au prezentat observații scrise, că pasagerii aerieni trebuie să fie supuși unor controale de securitate la intrarea sau la ieșirea din Uniune[205]. Transferul și prelucrarea datelor din PNR înainte de sosirea sau de plecarea lor facilitează și accelerează aceste controale, astfel cum a remarcat de asemenea Curtea în Avizul 1/15, permițând autorităților de aplicare a legii să se concentreze asupra pasagerilor în privința cărora dispun de elemente factuale care indică un risc real pentru securitate[206].

205. În sfârșit, în ceea ce privește în special extinderea sistemului Directivei PNR la zborurile intra-UE, chiar dacă nu se poate exclude *a priori* orice impact asupra libertății de circulație a cetățenilor Uniunii, consacrate în special de articolul 45 din cartă, ingerința în viața privată pe care o aduce Directiva PNR, deși gravă, nu este, în opinia noastră, de natură să producă în sine un

201 A se vedea Rezoluția 2396(2017), punctul 12; la același punct 12, Consiliul de Securitate al Organizației Națiunilor Unite „îndeamnă OACI să colaboreze cu statele sale membre pentru a stabili un standard pentru colectarea, utilizarea, prelucrarea și protecția datelor din PNR”. În urma unei astfel de invitații, la 23 iunie 2020, OACI a adoptat amendamentul nr. 28 la anexa 9 la Convenția de la Chicago care, astfel cum s-a menționat deja, stabilește standarde internaționale în materie de facilitare, și al cărei capitol 9 secțiunea D face referire în mod specific la PNR. La 12 ianuarie 2021, Comisia a adoptat o propunere de Decizie a Consiliului privind poziția care urmează să fie adoptată în numele Uniunii Europene în cadrul [OACI] cu privire la această modificare [COM(2021) 16 final].

202 Rezoluția din 19 iulie 2019, punctul 15 litera c), https://undocs.org/fr/S/RES/2482(2019).

203 În prezent, există două acorduri internaționale încheiate de Uniune cu Australia [Acord între Uniunea Europeană și Australia privind prelucrarea și transferul datelor din [PNR] de către transportatorii aerieni către Serviciul vamal și de protecție a frontierelor din Australia (JO 2012, L 186, p. 4)] și, respectiv, cu Statele Unite ale Americii [Acord între Statele Unite ale Americii și Uniunea Europeană privind utilizarea și transferul de date din [PNR] către Departamentul pentru Securitate Internă al Statelor Unite (JO 2012, L 215, p. 5)]. Este în curs de desfășurare o evaluare comună a acestor două acorduri în vederea încheierii unor noi acorduri. În plus, la 18 februarie 2020, Consiliul a autorizat Comisia să deschidă negocieri cu Japonia.

204 A se vedea Rezoluția 2396 (2017), p. 4.

205 Inclusiv persoanele care beneficiază de dreptul la liberă circulație în temeiul dreptului Uniunii; a se vedea Regulamentul (UE) 2017/458 al Parlamentului European și al Consiliului din 15 martie 2017 de modificare a Regulamentului (UE) 2016/399 în ceea ce privește consolidarea verificărilor prin consultarea bazelor de date relevante la frontierele externe (JO 2017, L 74, p. 7).

206 În acest sens, a se vedea de asemenea Avizul 1/15, punctul 187. A se vedea de asemenea Comunicarea Comisiei privind o abordare globală referitoare la transferul de date din [PNR] către țări terțe [COM(2010) 492 final, p. 6, punctul 2.2].

efect disuasiv asupra exercitării acestei libertăți, iar prelucrarea datelor din PNR poate fi chiar percepută de public ca o măsură necesară pentru a asigura siguranța călătoriilor aeriene [207]. Rămâne ca eventualitatea unui astfel de efect disuasiv să facă obiectul unei evaluări și al unei monitorizări continue.

206. Cu toate acestea, pentru a se conforma jurisprudenței menționate la punctele 107 și 108 din prezentele concluzii, Directiva PNR nu se poate limita la a impune ca accesul și prelucrarea automatizată a datelor din PNR ale tuturor pasagerilor aerieni să servească scopului urmărit, ci trebuie de asemenea să stabilească în mod clar și precis condițiile materiale și procedurale care reglementează accesul și prelucrarea respective, precum și utilizarea ulterioară a acestor date [208] și să prevadă garanții adecvate în fiecare etapă a acestui proces. Am menționat deja garanțiile aferente transferului de date din PNR către UIP atunci când am examinat a doua întrebare preliminară. Vom trece în revistă, în contextul examinării celei de a șasea întrebări preliminare, garanțiile care însoțesc în mod specific prelucrarea automatizată a acestor date și, în contextul examinării celei de a opta întrebări preliminare, cele referitoare la stocarea acestor date.

207. Înainte de a continua această analiză, dorim să subliniem importanța fundamentală pe care o are, în cadrul sistemului de garanții stabilit de Directiva PNR, supravegherea exercitată de autoritatea independentă menționată la articolul 15 din această directivă. În conformitate cu acest articol, orice prelucrare de date în temeiul directivei menționate este supusă supravegherii unei autorități de supraveghere independente, care are competența de a verifica legalitatea acestei prelucrări, de a desfășura investigații, inspecții și audituri și de a trata plângerile depuse de orice persoană vizată. O astfel de supraveghere, exercitată de un subiect extern însărcinat cu apărarea unor interese potențial în conflict cu cele urmărite de autorii prelucrărilor de date din PNR și învestit cu rolul de a asigura respectarea tuturor limitărilor și garanțiilor care însoțesc prelucrările menționate, constituie o garanție esențială, prevăzută în mod explicit la articolul 8 alineatul (3) din cartă, a cărei eficacitate, în ceea ce privește protecția drepturilor fundamentale în cauză, este chiar mai mare decât sistemul de căi de atac puse la dispoziția particularilor. Prin urmare, este esențial, în opinia noastră, ca Curtea să interpreteze în sens larg întinderea competențelor de supraveghere prevăzute la articolul 15 din Directiva PNR și ca statele membre să recunoască propriei autorități naționale de supraveghere, atunci când transpun această directivă în dreptul intern, întreaga întindere a acestor competențe, punând la dispoziția acesteia resursele materiale și personale necesare pentru îndeplinirea sarcinii sale.

208. Pe baza tuturor considerațiilor care precedă, apreciem că Directiva PNR nu depășește limitele strictului necesar prin faptul că permite transferul și prelucrarea automatizată a datelor oricărei persoane care se încadrează în noțiunea de „pasager” în sensul articolului 3 punctul 4 din această directivă.

iv) Cu privire la caracterul suficient de clar, precis și limitat la strictul necesar al evaluării prealabile a pasagerilor (a șasea întrebare preliminară)

209. Prin intermediul celei de a șasea întrebări preliminare, instanța de trimitere solicită în esență Curții să stabilească dacă evaluarea prealabilă menționată la articolul 6 din Directiva PNR este compatibilă cu articolele 7, 8 și 52 alineatul (1) din cartă. Chiar dacă formularea acestei întrebări se concentrează asupra caracterului sistematic și generalizat al prelucrării automatizate a datelor din PNR ale tuturor pasagerilor aerieni pe care îl are această evaluare prealabilă, rezultă din

[207] Este, într-un fel, ceea ce sugerează Comisia în propunerea sa de Directivă PNR, p. 3.

[208] A se vedea în acest sens Hotărârea Prokuratuur, punctul 49 și jurisprudența citată.

motivarea deciziei de trimitere că Cour constitutionnelle (Curtea Constituțională) solicită Curții să efectueze o apreciere mai cuprinzătoare a respectării cerințelor de legalitate și proporționalitate în cadrul unei astfel de prelucrări. Vom efectua această apreciere în continuare, făcând trimitere la analiza efectuată cu ocazia examinării celei de a patra întrebări preliminare în ceea ce privește caracterul nedirecționat al prelucrării automatizate menționate.

210. Articolul 6 alineatul (2) litera (a) din Directiva PNR prevede că UIP efectuează o evaluare prealabilă a pasagerilor aerieni, înainte de sosirea sau de plecarea programată a acestora din statul membru. Scopul acestei evaluări este identificarea persoanelor care necesită o examinare suplimentară de către autoritățile competente, „având în vedere faptul că respectivele persoane pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă”. În conformitate cu articolul 6 alineatul (6) din Directiva PNR, UIP a unui stat membru transmite datele din PNR ale persoanelor identificate în cadrul acestei evaluări sau rezultatul prelucrării acestor date, în vederea unei „examinări suplimentare”, autorităților competente ale aceluiași stat membru menționate la articolul 7 din aceeași directivă.

211. În conformitate cu articolul 6 alineatul (3) din Directiva PNR, evaluarea prealabilă întemeiată pe articolul 6 alineatul (2) litera (a) se realizează prin compararea datelor din PNR cu bazele de date „relevante” [articolul 6 alineatul (3) litera (a)] sau prin prelucrarea acestora în conformitate cu anumite criterii stabilite [articolul 6 alineatul (3) litera (b)].

212. Înainte de a trece la examinarea fiecăruia dintre aceste două tipuri de prelucrare a datelor, observăm că nu rezultă în mod clar din textul articolului 6 alineatul (3) menționat mai sus dacă statele membre sunt obligate să prevadă ca evaluarea prealabilă a pasagerilor să fie efectuată prin utilizarea sistematică și în toate cazurile a ambelor tipuri de analiză automatizată sau dacă, astfel cum pare să confirme utilizarea verbului „poate” și a conjuncției disjunctive „sau”, acestea au dreptul de a-și concepe sistemele astfel încât să limiteze, de exemplu, examinarea prevăzută la articolul 6 alineatul (3) litera (b) la anumite cazuri. În această privință, precizăm că propunerea de Directivă PNR prevedea ca această examinare să fie efectuată numai în contextul combaterii infracțiunilor transfrontaliere grave [209].

213. Considerăm, în acord cu Comisia, că rezultă în special din economia Directivei PNR că statele membre sunt obligate să prevadă ambele tipuri de prelucrare automatizată, din motive care țin de asemenea de necesitatea de a asigura o aplicare cât mai uniformă posibil a sistemului de prelucrare a datelor din PNR al Uniunii. Totuși, acest lucru nu înseamnă că statele membre nu sunt autorizate – și chiar obligate, pentru a se asigura că prelucrarea datelor pe care o presupune evaluarea prealabilă efectuată în conformitate cu articolul 6 alineatul (2) litera (a) din Directiva PNR este limitată la strictul necesar – să limiteze analiza, în temeiul articolului 6 alineatul (3) litera (b) din Directiva PNR, în funcție de rezultatele sale în ceea ce privește eficiența pentru fiecare dintre infracțiunile vizate de această directivă și, dacă este cazul, să o limiteze numai la unele dintre aceste infracțiuni. Acest lucru este susținut de considerentul (7) al Directivei PNR, care prevede că, „pentru a asigura faptul că prelucrarea datelor din PNR rămâne limitată la ceea ce este necesar, definirea și aplicarea de criterii de evaluare ar trebui să fie limitate la infracțiuni de terorism și infracțiuni grave pentru care este relevantă utilizarea unor astfel de criterii”.

[209] A se vedea articolul 4 alineatul (2) litera (a) din propunerea de Directivă PNR.

– Cu privire la compararea cu bazele de date, în sensul articolului 6 alineatul (3) litera (a) din Directiva PNR

214. Prima componentă a evaluării prealabile efectuate de UIP în temeiul articolului 6 alineatul (2) litera (a) din Directiva PNR implică, în conformitate cu alineatul (3) litera (a) al acestui articol, compararea datelor din PNR („data matching") cu bazele de date pentru a căuta eventuale corespondențe pozitive („hits"). Aceste hits sunt menite a fi verificate de către UIP în conformitate cu articolul 6 alineatul (5) din Directiva PNR și, dacă este necesar, traduse în „match" înainte de a fi comunicate autorităților competente.

215. Astfel cum a recunoscut Curtea la punctul 172 din Avizul 1/15, întinderea ingerinței pe care o implică aceste tipuri de analize automatizate în exercitarea drepturilor consacrate la articolele 7 și 8 din cartă depinde esențialmente de bazele de date pe care se întemeiază acestea. În consecință, este determinant ca dispozițiile care prevăd o astfel de prelucrare a datelor să identifice într-un mod suficient de clar și de precis bazele de date cu care este autorizată confruntarea datelor care urmează să fie prelucrate.

216. În conformitate cu articolul 6 alineatul (3) litera (a) din Directiva PNR, UIP compară datele din PNR cu „bazele de date relevante"[210] prin prisma obiectivelor urmărite de această directivă. Această dispoziție menționează de asemenea o categorie specifică de baze de date, și anume cele privind „persoane sau obiecte căutate sau care fac obiectul unei alerte", pe care legiuitorul Uniunii a intenționat, așadar, să le califice în mod explicit drept „relevante" în sensul acestei dispoziții.

217. Pe lângă această precizare, noțiunea de „baze de date relevante" nu este clarificată ulterior. Nu se precizează în special dacă, pentru a fi considerate „relevante", bazele de date utilizate în scopul confruntării datelor din PNR trebuie să fie gestionate de autoritățile de aplicare a legii sau, mai general, de orice autoritate publică ori pur și simplu să le fie accesibile în mod direct sau indirect. Nu se specifică nici natura datelor pe care le pot conține astfel de baze de date și nici relația lor cu obiectivele urmărite de Directiva PNR[211]. În plus, din modul de redactare a articolului 6 alineatul (3) litera (a) din Directiva PNR rezultă că pot fi calificate drept „baze de date relevante" atât baze de date naționale și ale Uniunii, cât și cele internaționale, ceea ce extinde și mai mult lista bazelor de date potențial acoperite și sporește caracterul deschis al acestei noțiuni[212].

218. În aceste condiții, potrivit principiului general de interpretare amintit la punctul 151 din prezentele concluzii, revine Curții sarcina să interpreteze articolul 6 alineatul (3) litera (a) din Directiva PNR, în special noțiunea de „baze de date relevante", pe cât posibil în conformitate cu

[210] În timp ce versiunea în limba franceză a articolului 6 alineatul (3) litera (a) menționează „bases de données utiles", în majoritatea celorlalte versiuni lingvistice, această dispoziție se referă mai degrabă la „baze de date relevante": a se vedea în special versiunea în limbile spaniolă („pertinentes"), germană („massgeblich"), engleză („relevant"), italiană („pertinenti"), neerlandeză („relevant") și portugheză („relevantes").

[211] Astfel cum este redactat, articolul 6 alineatul (3) litera (a) din Directiva PNR pare să permită efectuarea de analize sub formă de cercetări de date prin confruntare cu date foarte variate, astfel încât cercetarea de date să fie realizată în vederea atingerii obiectivelor directivei. În ceea ce privește riscurile legate de „data mining" în materie de date din PNR, a se vedea raportul Korff, p. 77. CEPD a subliniat cu fermitate în Avizul său din 25 martie 2011, punctul 18, lipsa de precizie și de previzibilitate în identificarea bazelor de date cu care pot fi confruntate datele din PNR.

[212] Caracterul vag și deschis al modului de redactare a articolului 6 alineatul (3) litera (a) din Directiva PNR se reflectă într-o mare varietate de transpuneri în dreptul național, care merge de la o interpretare strictă a noțiunii de „bază de date relevantă", care limitează analiza prevăzută numai la confruntarea cu bazele de date menționate în mod explicit în această dispoziție (acesta este cazul Republicii Federale Germania, după cum reiese din observațiile prezentate de guvernul acesteia în fața Curții), la o interpretare mai largă care acoperă orice bază de date disponibilă sau accesibilă autorităților competente în cadrul misiunii lor [în acest sens este redactat în special articolul 24 alineatul (1) punctul 1 din Legea PNR].

cerințele de claritate și de precizie impuse de cartă. În plus, întrucât această dispoziție prevede o ingerință în exercitarea drepturilor fundamentale prevăzute la articolele 7 și 8 din cartă, aceasta trebuie interpretată în mod restrictiv și având în vedere cerința de a asigura un nivel ridicat de protecție a acestor drepturi fundamentale, astfel cum este enunțată în special în considerentul (15) al Directivei PNR. În plus, aceasta trebuie interpretată în lumina principiului limitării scopurilor în care pot fi prelucrate datele din PNR, prevăzut la articolul 1 alineatul (2) din Directiva PNR.

219. Având în vedere aceste criterii, noțiunea de „baze de date relevante” trebuie interpretată, în opinia noastră, în sensul că vizează numai bazele de date naționale gestionate de autoritățile competente în temeiul articolului 7 alineatul (1) din Directiva PNR, precum și bazele de date ale Uniunii și cele internaționale exploatate direct de aceste autorități în exercitarea atribuțiilor lor. În plus, bazele de date menționate trebuie să aibă o legătură directă și strânsă cu obiectivele combaterii terorismului și a infracțiunilor grave urmărite de Directiva PNR, ceea ce presupune ca acestea să fi fost create în aceste scopuri. Interpretată astfel, această noțiune vizează în esență, dacă nu exclusiv, bazele de date privind persoanele sau obiectele căutate ori care fac obiectul unei alerte, menționate în mod explicit la articolul 6 alineatul (3) litera (a) din Directiva PNR.

220. Sunt excluse într-un mod general din noțiunea de „baze de date relevante” bazele de date gestionate sau operate de serviciile de informații ale statelor membre, cu excepția cazului în care acestea îndeplinesc în mod strict condiția de a fi strâns legate de obiectivele urmărite de Directiva PNR, iar statul membru în cauză conferă serviciilor sale de informații competențe specifice în domeniul aplicării legii [213].

221. Interpretarea propusă mai sus este conformă cu recomandările formulate de Curte la punctul 172 din Avizul 1/15.

222. Cu toate acestea, chiar și astfel interpretat, articolul 6 alineatul (3) litera (a) din Directiva PNR nu permite o identificare suficient de exactă a bazelor de date care vor fi utilizate de statele membre în cadrul confruntării cu datele din PNR și nu se poate considera că îndeplinește cerințele care decurg din articolul 52 alineatul (1) din cartă, astfel cum a fost interpretat de Curte. În consecință, această dispoziție trebuie interpretată în sensul că obligă statele membre ca, la transpunerea Directivei PNR în dreptul intern, să publice o listă a acestor baze de date și să o actualizeze. În plus, ar fi de dorit ca la nivelul Uniunii să se întocmească o listă a bazelor de date „relevante”, în sensul articolului 6 alineatul (3) litera (a) din Directiva PNR, gestionate de Uniune în cooperare cu statele membre, precum și a bazelor de date internaționale, pentru a uniformiza practicile statelor membre în această privință.

– *Cu privire la prelucrarea datelor din PNR în funcție de criterii prestabilite*

223. A doua componentă a evaluării prealabile în temeiul articolului 6 alineatul (2) litera (a) din Directiva PNR constă într-o analiză automatizată în funcție de criterii prestabilite. În cadrul acestei analize, datele din PNR sunt prelucrate, în principal în scopuri predictive, prin aplicarea unor algoritmi despre care se consideră că permit „identificarea” pasagerilor ce ar putea fi implicați în infracțiuni de terorism sau în infracțiuni grave. În acest context, UIP desfășoară în

[213] În niciun caz, în opinia noastră, un stat membru nu va trebui să se considere obligat, în temeiul articolului 6 alineatul (3) litera (a) din Directiva PNR, să autorizeze propria UIP să confrunte în mod sistematic datele din PNR cu „bazele de date relevante” în sensul acestei dispoziții, gestionate de serviciile sale de informații.

esență o activitate de creare de profiluri [214]. Întrucât este posibil să aibă consecințe semnificative asupra persoanelor identificate prin algoritm [215], o astfel de prelucrare necesită un cadru exact în ceea ce privește atât modalitățile în care este efectuată, cât și garanțiile care trebuie să o însoțească. Într-adevăr, astfel cum a remarcat Curtea la punctul 172 din Avizul 1/15, întinderea ingerinței pe care o implică aceste tipuri de analize în exercitarea drepturilor consacrate la articolele 7 și 8 din cartă depinde în principal de modelele și de criteriile prestabilite aplicate.

224. În această privință, observăm, în primul rând, că articolul 6 alineatul (4) a doua teză din Directiva PNR precizează că criteriile prestabilite în funcție de care se efectuează evaluarea prealabilă prevăzută la articolul 6 alineatul (3) litera (b) din această directivă trebuie să fie „personalizate, proporționale și specifice”. Prima dintre aceste cerințe se referă la obiectivul evaluării prealabile prevăzut la alineatul (2) litera (a) al acestui articol, și anume identificarea persoanelor care necesită o examinare suplimentară de către autoritățile competente și răspunde astfel necesității, subliniate de Curte în Avizul 1/15, ca utilizarea criteriilor să ajungă să „personalizeze” indivizii cu privire la care ar putea exista o „bănuială rezonabilă” de participare la infracțiuni de terorism sau la infracțiuni grave [216]. O astfel de „personalizare” presupune aplicarea unor criterii de evaluare abstracte sau, pentru a folosi o expresie prevăzută în Recomandarea din anul 2021 privind crearea de profiluri, a unor „profiluri” [217] prin intermediul cărora să se „filtreze” datele din PNR pentru a identifica pasagerii care corespund acestor criterii și care, prin urmare, ar putea fi supuși unui control suplimentar. În schimb, Directiva PNR nu permite crearea de profiluri individuale pentru toți pasagerii aerieni ale căror date sunt analizate, de exemplu prin asocierea unei categorii de risc pe o scară predefinită pentru fiecare dintre aceștia, întrucât acest lucru ar încălca atât articolul 6 alineatul (4) din această directivă, cât și limitele impuse de Curte în Avizul 1/15 cu privire la prelucrarea automatizată a datelor din PNR.

225. În conformitate cu articolul 6 alineatul (4) a doua teză, criteriile prestabilite menționate la articolul 6 alineatul (3) litera (b) din Directiva PNR trebuie, în plus, să fie „specifice” [218], și anume adaptate scopului urmărit și relevante în raport cu acesta, dar și „proporționale” [219], altfel spus să nu depășească limitele acestui scop. Pentru a îndeplini aceste cerințe și în special „pentru a asigura faptul că prelucrarea datelor din PNR rămâne limitată la ceea ce este necesar”,

214 Articolul 3 alineatul (4) din Directiva privind poliția definește „crearea de profiluri” ca fiind „orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, localizarea sau deplasările respectivei persoane fizice”. Aceeași definiție se regăsește la articolul 4 punctul 4 din RGPD și la punctul 1 litera (c) din anexa la Recomandarea CM/Rec(2021)8 din 3 noiembrie 2021 a Comitetului de Miniștri al Consiliului Europei privind protecția persoanelor fizice în ceea ce privește prelucrarea automată a datelor cu caracter personal în contextul creării de profiluri, https://search.coe.int/cm/pages/result_details.aspx?ObjectId= 0900001680a46148, (denumită în continuare „Recomandarea din anul 2021 privind crearea de profiluri”).

215 Punctul 1 litera (j) punctul (i) din Recomandarea din anul 2021 privind crearea de profiluri definește drept „prelucrare în vederea creării de profiluri cu grad ridicat de risc” „crearea de profiluri a căror funcționare produce efecte juridice sau care au un impact semnificativ asupra persoanei vizate sau a grupului de persoane identificate prin prelucrarea în vederea creării de profiluri”.

216 A se vedea Avizul 1/15, punctul 272.

217 În conformitate cu punctul 1.1 litera (d) din anexa la Recomandarea din 2021 privind crearea de profiluri, termenul „profil” desemnează „un set de date care sunt atribuite unei persoane, care caracterizează o categorie de persoane sau care este menit a fi aplicat unei persoane”. Astfel cum se explică în Raportul privind evoluțiile ulterioare adoptării Recomandării (2010)13 privind crearea de profiluri (https://rm.coe.int/t-pd-2019-07fin-fr-rapport-profilage-2770-2878-8993-1-final-clean-2755/1680a0925b, p. 21), care a precedat adoptarea Recomandării din anul 2021 privind crearea de profiluri, noțiunea de „profil” își menține întreaga semnificație în sisteme care, precum Directiva PNR, fac distincție între operațiunile de creare de profiluri [a se vedea în special articolul 6 alineatul (2) litera (b) din această directivă], de cele care îl aplică și permit „transparența criteriilor care sunt aplicate într-o a doua etapă prin operațiunea de creare de profiluri”.

218 A se vedea articolul 6 alineatul (4) din Directiva PNR, precum și Avizul 1/15, punctul 172.

219 A se vedea articolul 6 alineatul (4) din Directiva PNR.

considerentul (7) al Directivei PNR precizează, astfel cum am subliniat deja, că „definirea și aplicarea de criterii de evaluare ar trebui să fie limitate la infracțiuni de terorism și infracțiuni grave pentru care este relevantă utilizarea unor astfel de criterii”.

226. În sfârșit, rezultă atât din preambulul și din dispozițiile Directivei PNR, cât și din cerințele stabilite de Curte în Avizul 1/15 că criteriile prestabilite menționate la articolul 6 alineatul (3) litera (b) din Directiva PNR trebuie să fie de asemenea „fiabile” [220], ceea ce înseamnă, pe de o parte, că acestea trebuie să fie concepute astfel încât să reducă la minimum riscul de erori [221] și, pe de altă parte, că acestea trebuie să fie „actuale” [222]. În această privință, articolul 6 alineatul (4) a treia teză din Directiva PNR impune statelor membre să se asigure că „UIP stabilesc aceste criterii și le revizuiesc periodic în cooperare cu autoritățile competente menționate la articolul 7” [223]. Pentru a asigura fiabilitatea acestor criterii și pentru a limita cât mai mult posibil rezultatele fals pozitive, mai este necesar, așa cum a recunoscut Comisia în răspunsul său la o întrebare scrisă adresată de Curte, ca acestea să fie concepute astfel încât să ia în considerare atât elementele incriminatorii, cât și pe cele dezincriminatorii.

227. În al doilea rând, Directiva PNR interzice în mod expres crearea de profiluri discriminatorii. Astfel, articolul 6 alineatul (4) prima teză din această directivă prevede că evaluarea prealabilă efectuată pe baza unor criterii prestabilite în temeiul alineatului (3) litera (b) din acest articol „se realizează în mod nediscriminatoriu”. În acest sens, trebuie precizat că, în timp ce a treia teză a articolului 6 alineatul (4) prevede că aceste criterii „nu se întemeiază în niciun caz pe rasa sau originea etnică a unei persoane, opiniile sale politice, religia sau convingerile sale filozofice, apartenența la un sindicat, starea sa de sănătate, viața sexuală sau orientarea sexuală”, interdicția generală privind crearea de profiluri discriminatorii trebuie interpretată în sensul că acoperă toate motivele de discriminare menționate la articolul 21 din cartă, chiar și pe cele care nu sunt menționate în mod expres [224].

228. În al treilea rând, rezultă atât din formularea articolului 6 alineatul (3) litera (b) din Directiva PNR, cât și din sistemul de garanții care însoțește prelucrarea automatizată a datelor din PNR prevăzută de Directiva PNR că funcționarea algoritmilor utilizați în cadrul analizei menționate în această dispoziție trebuie să fie transparentă, iar rezultatul aplicării lor să fie trasabil. Această cerință de transparență nu implică desigur că „profilurile” utilizate trebuie să fie făcute publice. În schimb, aceasta impune asigurarea caracterului identificabil al procesului decizional algoritmic. Într-adevăr, pe de o parte, cerința conform căreia criteriile în funcție de care este necesar să fie efectuată această analiză trebuie să fie „prestabilite” exclude posibilitatea ca aceste criterii să fie modificate fără intervenție umană și, prin urmare, se opune utilizării unor tehnologii de inteligență artificială denumite „machine learning” [225] care, deși pot avea un grad mai mare de precizie, sunt dificil de interpretat chiar și pentru operatorii care au efectuat prelucrarea automatizată [226]. Pe de altă parte, garanția prevăzută la articolul 6 alineatele (5) și (6) din Directiva

220 A se vedea Avizul 1/15, punctul 172.

221 A se vedea considerentul (7) al Directivei PNR.

222 A se vedea Avizul 1/15, punctul 174.

223 Aceeași cerință se regăsește la punctul 174 din Avizul 1/15.

224 Observăm că toate motivele de discriminare prevăzute la articolul 21 din cartă sunt reproduse în considerentul (20) al Directivei PNR. O aliniere la lista motivelor de discriminare interzise menționată la articolul 21 a fost propusă de FRA în Avizul său 1/2011, p. 8.

225 În conformitate cu punctul 1.1 litera (g) din anexa la Recomandarea din anul 2021 privind crearea de profiluri, expresia „machine learning” desemnează „prelucrarea care utilizează metode specifice de inteligență artificială, bazată pe abordări statistice pentru a conferi computerelor capacitatea de a «învăța» pornind de la date, și anume de a-și îmbunătăți performanța în rezolvarea sarcinilor fără a fi programate în mod explicit pentru fiecare sarcină”.

226 În ceea ce privește efectele opacității sistemelor algoritmice asupra posibilității unui control uman pentru a preveni efectele prejudiciabile ale acestor sisteme și impactul negativ al acestora asupra drepturilor omului, a se vedea Recomandarea CM/Rec(2020)1 a Comitetului de Miniștri al Consiliului Europei către statele membre privind impactul sistemelor algoritmice asupra drepturilor omului.

PNR, conform căreia orice rezultat pozitiv obținut printr-o prelucrare automatizată a datelor din PNR realizată în temeiul alineatului (2) litera (a) al acestui articol este reexaminat individual prin mijloace neautomatizate, pentru a fi efective, impune – în ceea ce privește analiza menționată la articolul 6 alineatul (3) litera (b) din Directiva PNR – să fie posibilă înțelegerea motivului pentru care programul a ajuns la un astfel de rezultat pozitiv, fapt care nu poate fi asigurat mai ales în cazul în care se utilizează sisteme de autoinstruire. Același lucru este valabil și pentru controlul legalității acestei analize, inclusiv în ceea ce privește caracterul nediscriminatoriu al rezultatelor obținute, care ține de competența responsabilului cu protecția datelor și a autorității naționale de supraveghere, în temeiul articolului 6 alineatul (7) și, respectiv, al articolului 15 alineatul (3) litera (b) din Directiva PNR. Transparența funcționării algoritmilor utilizați este tot o condiție necesară pentru a permite persoanelor în cauză să își exercite dreptul de a formula o plângere, precum și dreptul la o cale de atac judiciară eficace.

– *Cu privire la garanțiile care însoțesc prelucrarea automatizată a datelor din PNR*

229. Am avut deja ocazia să menționăm unele dintre garanțiile care însoțesc prelucrarea automatizată a datelor din PNR în contextul evaluării prealabile în temeiul articolului 6 alineatul (2) litera (a) din Directiva PNR și care respectă cerințele stabilite de Curte în Avizul 1/15, și anume, interzicerea prelucrării pe baza unor criterii prestabilite discriminatorii [articolul 6 alineatul (4) prima și a patra teză din Directiva PNR, Avizul 1/15, punctul 172], actualizarea la intervale regulate a criteriilor prestabilite în funcție de care trebuie efectuată evaluarea prealabilă menționată la articolul 6 alineatul (3) litera (b) din această directivă [articolul 6 alineatul (4) a treia teză din Directiva PNR, Avizul 1/15, punctul 174], revizuirea prin mijloace neautomatizate a oricăror rezultate pozitive obținute în urma prelucrării automatizate a datelor din PNR [articolul 6 alineatele (5) și (6) din Directiva PNR, Avizul 1/15, punctul 173] și controlul legalității acestei prelucrări de către responsabilul cu protecția datelor și autoritatea națională de supraveghere [articolul 6 alineatul (7) din Directiva PNR și articolul 15 alineatul (3) litera (b) din Directiva PNR]. În acest context, este esențial ca controlul efectuat de o autoritate independentă, precum autoritatea menționată la articolul 15 din Directiva PNR, pe de o parte, să poată viza orice aspect inerent prelucrării automatizate a datelor din PNR, inclusiv identificarea bazelor de date utilizate în scopul comparării în sensul articolului 6 alineatul (3) litera (a) din această directivă și elaborarea criteriilor prestabilite aplicate în scopul analizei prevăzute la articolul 6 alineatul (3) litera (b) din directiva menționată, și, pe de altă parte, să poată fi exercitată atât *ex ante*, cât și *ex post*.

230. Este important de subliniat faptul că garanțiile menționate mai sus trebuie considerate aplicabile în mod transversal ambelor tipuri de analiză menționate la articolul 6 alineatul (3) din Directiva PNR, în pofida termenilor în care sunt formulate. Astfel, chiar dacă articolul 6 alineatul (4) prima teză din această directivă face referire la cerința privind respectarea principiului nediscriminării numai în raport cu evaluarea prealabilă efectuată în funcție de criterii prestabilite, această cerință se aplică în fiecare etapă a procesului de prelucrare a datelor din PNR și, prin urmare, inclusiv atunci când aceste date sunt comparate cu bazele de date relevante în cadrul evaluării prealabile în sensul articolului 6 alineatul (3) litera (a) din această directivă. Același lucru este valabil și pentru cerința potrivit căreia criteriile prestabilite utilizate în analiza menționată la articolul 6 alineatul (3) litera (b) din Directiva PNR trebuie să fie fiabile și actualizate, care trebuie interpretată în sensul că se referă și la datele conținute în bazele de date utilizate în scopul efectuării comparației prevăzute la articolul 6 alineatul (3) litera (a) din această directivă. În această privință, observăm, în termeni mai generali, că toate garanțiile aplicabile prelucrării automatizate a datelor cu caracter personal prevăzute de Directiva privind poliția sunt

aplicabile și în contextul Directivei PNR, întrucât analizele automatizate efectuate în contextul acestei directive trebuie considerate ca intrând în domeniul de aplicare al Directivei privind poliția.

231. Pe lângă garanțiile enumerate la punctul 229 de mai sus se adaugă cea prevăzută la articolul 7 alineatul (6) din Directiva PNR, care completează, pe de o parte, interdicția ca orice proces decizional să se bazeze exclusiv pe rezultatele prelucrării automatizate a datelor PNR și, pe de altă parte, interzicerea discriminării în cadrul prelucrării și utilizării acestor date. Astfel, această dispoziție prevede că „[a]utoritățile competente nu iau doar pe baza prelucrării automatizate a datelor PNR nicio decizie care produce efecte juridice adverse asupra unei persoane sau care afectează în mod semnificativ o persoană” și că astfel de decizii „nu se iau pe baza rasei sau originii etnice a unei persoane, a opiniilor sale politice, a religiei sau a convingerilor sale filozofice, a apartenenței la un sindicat, a stării sale de sănătate, a vieții sexuale sau orientării sexuale”. Astfel cum am arătat la punctul 227 din prezentele concluzii cu privire la articolul 6 alineatul (4) a patra teză din Directiva PNR, această listă de motive de discriminare trebuie completată prin adăugarea celor prevăzute la articolul 21 din cartă și care nu sunt menționate în mod expres.

232. În ceea ce privește securitatea datelor din PNR, articolul 6 alineatul (8) din Directiva PNR prevede că stocarea, prelucrarea și analiza datelor din PNR de către UIP se realizează exclusiv într-un loc sigur sau în locuri sigure de pe teritoriul statelor membre.

– *Concluzie cu privire la a șasea întrebare preliminară*

233. Având în vedere toate considerațiile menționate anterior și sub rezerva interpretărilor propuse în special la punctele 213, 219, 220, 222, 227, 228, 230 și 231 din prezentele concluzii, considerăm că prelucrarea automatizată a datelor din PNR în contextul evaluării prealabile menționate la articolul 6 alineatul (2) litera (a) din Directiva PNR respectă cerințele de claritate și de precizie și se limitează la strictul necesar.

v) Cu privire la păstrarea datelor din PNR (a opta întrebare preliminară)

234. Prin intermediul celei de a opta întrebări preliminare, instanța de trimitere solicită Curții să stabilească dacă articolul 12 din Directiva PNR coroborat cu articolele 7, 8 și 52 alineatul (1) din cartă trebuie interpretat în sensul că se opune unei reglementări naționale care prevede un termen general de păstrare a datelor din PNR de cinci ani, fără a distinge dacă reiese, în cadrul evaluării prealabile, că pasagerii vizați pot sau nu să prezinte un risc pentru securitatea publică.

235. Articolul 12 alineatul (1) din Directiva PNR prevede că datele din PNR sunt păstrate într-o bază de date „pentru o perioadă de cinci ani după transferul lor către UIP a statului membru pe teritoriul căruia sosește sau de pe teritoriul căruia pleacă zborul”. În conformitate cu alineatul (2) al acestui articol, după o „perioadă inițială de păstrare”[227] de șase luni, datele din PNR se depersonalizează prin mascarea anumitor date care ar putea servi la identificarea directă a persoanei în cauză. În conformitate cu alineatul (3) al aceluiași articol, după expirarea acestei perioade de șase luni, dezvăluirea datelor complete din PNR, inclusiv a elementelor mascate, este permisă numai dacă se consideră „în mod rezonabil” că este necesară în scopul menționat la articolul 6 alineatul (2) litera (b) din Directiva PNR și când a fost aprobată de o autoritate judiciară sau de o altă autoritate națională competentă, în temeiul dreptului intern, să verifice

[227] Această definiție se regăsește în considerentul (25) al Directivei PNR.

dacă sunt îndeplinite condițiile pentru dezvăluire. În sfârșit, alineatul (4) al articolului menționat prevede că, după expirarea perioadei menționate la alineatul (1), datele din PNR sunt șterse în mod definitiv.

236. Rezultă din cele menționate anterior că Directiva PNR stabilește ea însăși regimul de păstrare a datelor din PNR, inclusiv durata acestei păstrări, prin stabilirea acesteia la cinci ani [228], astfel încât statele membre nu au, în principiu, nicio marjă de apreciere în această privință, fapt care a fost confirmat de altfel de Comisie. În aceste condiții, după cum am avut deja ocazia să observăm, a opta întrebare preliminară, chiar dacă este formulată ca o problemă de interpretare, solicită de fapt Curții să se pronunțe asupra compatibilității regimului menționat cu carta.

237. Constituie un principiu general al protecției datelor cu caracter personal faptul că astfel de date nu trebuie păstrate într-o formă care să permită identificarea directă sau indirectă a persoanelor vizate mai mult timp decât este necesar pentru îndeplinirea scopului în care sunt prelucrate [229]. În plus, conform jurisprudenței constante, o reglementare care prevede o stocare a datelor cu caracter personal trebuie să răspundă întotdeauna unor criterii obiective, stabilind un raport între datele cu caracter personal care trebuie stocate și obiectivul urmărit [230].

238. În Avizul 1/15, Curtea a considerat, în ceea ce privește datele colectate la intrarea în Canada, că raportul necesar între datele din PNR și scopul urmărit de Acordul PNR Canada-UE a fost stabilit pentru toți pasagerii aerieni atât timp cât aceștia se aflau pe teritoriul acestei țări terțe [231]. În schimb, în ceea ce privește pasagerii aerieni care au părăsit Canada și pentru care nu a fost identificat un risc în materie de terorism sau de infracțiuni transnaționale grave la sosirea lor în Canada și până la plecarea din această țară terță, Curtea a considerat că nu rezulta că exista, fie și indirect, un astfel de raport care să justifice stocarea datelor din PNR ale acestora [232]. Cu toate acestea, Curtea a considerat că o astfel de stocare ar putea fi admisibilă „[î]n măsura în care însă sunt identificate în cazuri particulare elemente obiective care permit să se considere că anumiți pasageri aerieni ar putea să prezinte, chiar și după plecarea lor din Canada, un risc în termeni de combatere a terorismului și a altor infracțiuni transnaționale grave” [233].

239. Transpuse în contextul Directivei PNR, principiile stabilite de Curte în Avizul 1/15 ar implica faptul că datele din PNR ale zborurilor extra-UE colectate la intrarea în Uniune, precum și datele din PNR ale zborurilor intra-UE colectate la intrarea în statul membru în cauză pot fi stocate, după analiza lor prealabilă în sensul articolului 6 alineatul (2) litera (a) din Directiva PNR, numai atât timp cât pasagerii în cauză rămân pe teritoriul Uniunii sau al statului membru respectiv. În ceea ce privește datele din PNR ale zborurilor extra-UE colectate la ieșirea din Uniune și datele din PNR ale zborurilor intra-UE colectate la ieșirea din statul membru în cauză,

228 Enunțul din considerentul (37) al Directivei PNR conform căruia „păstrarea datelor din PNR în UIP [este autorizată] pentru o perioadă *care nu depășește cinci ani*, după care datele ar trebui șterse” (sublinierea noastră) nu permite, în opinia noastră, repunerea în discuție a modului de redactare clar a articolului 12 alineatul (1) din această directivă.

229 A se vedea, în ceea ce privește prelucrarea datelor cu caracter personal în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor, Directiva privind poliția, articolul 4 litera (e) și considerentul (26). A se vedea, într-un mod mai general, articolul 5 alineatul (1) litera (e) din RGPD și articolul 5 alineatul (4) litera (e) din Convenția 108 modernizată.

230 A se vedea Hotărârea Schrems I (punctul 93), Hotărârea Tele2 Sverige (punctul 110), Avizul 1/15 (punctul 191), precum și Hotărârea La Quadrature du Net, (punctul 133).

231 A se vedea Avizul 1/15, punctul 197.

232 A se vedea Avizul 1/15, punctul 205.

233 A se vedea Avizul 1/15, punctul 207.

acestea ar putea, în principiu, să fie păstrate, după evaluarea prealabilă menționată, numai în cazul acelor pasageri pentru care elemente obiective ar dezvălui existența unui risc în termeni de combatere a terorismului și a altor infracțiuni transnaționale grave [234].

240. Guvernele și instituțiile care au prezentat observații Curții se opun, în general, transpunerii în prezenta cauză a principiilor stabilite în Avizul 1/15 privind păstrarea datelor din PNR. În această privință, nu este exclus, desigur, ca utilizarea de către Curte a unui criteriu legat de ședederea persoanei vizate pe teritoriul Canadei să fi fost influențată de faptul că aceasta s-a confruntat cu păstrarea datelor cu caracter personal pe teritoriul unei țări terțe. Este de asemenea posibil ca aplicarea unui astfel de criteriu în contextul Directivei PNR să aibă ca rezultat concret o ingerință potențial mai mare în exercitarea drepturilor la respectarea vieții private și la protecția datelor cu caracter personal potențial mai importante pentru anumite categorii de persoane, în special pentru cele care au reședința permanentă în Uniune și care călătoresc în interiorul acesteia sau care se întorc după o ședere în străinătate. În sfârșit, este adevărat că criteriul menționat s-ar putea dovedi dificil de aplicat în practică, cel puțin pentru zborurile intra-UE, astfel cum au subliniat unele state membre și Consiliul.

241. Nu este mai puțin adevărat că, chiar dacă s-ar dori înlăturarea criteriului utilizat de Curte în Avizul 1/15, păstrarea tuturor datelor din PNR ale tuturor pasagerilor aerieni, indiferent de rezultatul evaluării prealabile menționate la articolul 6 alineatul (2) litera (a) din Directiva PNR și fără a se face nicio distincție în funcție de riscul în termeni de combatere a terorismului și al infracțiunilor grave pe baza unor criterii obiective și verificabile contravine jurisprudenței constante a Curții amintite la punctul 237 din prezentele concluzii, pe care Curtea a intenționat să o pună în aplicare în avizul menționat. Or, considerațiile prezentate la punctele 201-203 din prezentele concluzii în cadrul examinării celei de a patra întrebări preliminare, chiar dacă justifică, în opinia noastră, transferul generalizat și nediferențiat al datelor din PNR, precum și prelucrarea automată a acestora în cadrul evaluării prealabile prevăzute la articolul 6 alineatul (2) litera (a) din Directiva PNR, nu justifică, în opinia noastră, prin ele însele, păstrarea generalizată și nediferențiată a acestor date, chiar și după o astfel de evaluare.

242. În plus, observăm că aceeași perioadă de păstrare de cinci ani se aplică combaterii atât a terorismului, cât și a infracțiunilor grave și, în contextul acestui din urmă obiectiv, a tuturor infracțiunilor enumerate în anexa II, fără excepție. Or, astfel cum reiese din considerentele prezentate la punctul 121 din prezentele concluzii, această listă este deosebit de extinsă și cuprinde infracțiuni de diferite tipuri și gravități. În această privință, este important de remarcat că justificarea invocată practic de aproape toate statele membre și instituțiile care au prezentat observații în prezenta procedură, referitoare la durata și complexitatea investigațiilor, este amintită în mod concret numai pentru infracțiunile de terorism și pentru anumite infracțiuni care au un caracter eminamente transnațional, precum traficul de ființe umane sau de droguri, și, în general, pentru anumite forme de criminalitate organizată. În plus, amintim că în Avizul 1/15 o justificare similară a fost acceptată de Curte doar în ceea ce privește păstrarea datelor din PNR ale pasagerilor aerieni pentru care există un risc obiectiv în ceea ce privește combaterea terorismului sau a infracțiunilor transnaționale grave, pentru care s-a considerat că o stocare a datelor timp de cinci ani nu depășește limitele a ceea ce este strict necesar [235]. În schimb, s-a considerat că această

[234] Aceasta ar fi o aplicare prin analogie a punctului 187 și urm. din Avizul 1/15, întrucât acesta din urmă făcea referire numai la ipoteza datelor din PNR colectate la intrarea pe teritoriul Canadei.

[235] A se vedea Avizul 1/15, punctul 209.

justificare nu poate permite „o stocare continuă a datelor din PNR ale tuturor pasagerilor aerieni […] în vederea unui eventual acces la aceste date, independent de vreo legătură cu combaterea terorismului și a altor infracțiuni transnaționale grave” [236].

243. Este adevărat, desigur, astfel cum subliniază Consiliul, Parlamentul și Comisia, precum și toate guvernele care au prezentat observații cu privire la a opta întrebare preliminară, că Directiva PNR prevede garanții specifice atât în ceea ce privește stocarea datelor din PNR, dintre care unele sunt mascate după o perioadă inițială de șase luni, cât și în ceea ce privește utilizarea lor în timpul perioadei de păstrare, care este supusă unor condiții stricte. Cu toate acestea, în primul rând, observăm, pe de o parte, că proiectul de Acord PNR Canada-UE prevedea și un sistem de depersonalizare a datelor din PNR prin mascare [237] și, pe de altă parte, că, deși o asemenea depersonalizare, astfel cum a subliniat în special Comitetul consultativ al Convenției 108 [238], poate reduce riscurile legate de stocarea prelungită a datelor, cum ar fi accesul abuziv, datele mascate mai permit totuși identificarea persoanelor și, ca atare, rămân date cu caracter personal a căror păstrare trebuie de asemenea limitată în timp pentru a preveni o supraveghere permanentă generalizată. În această privință, subliniem că un termen de păstrare de cinci ani are drept consecință faptul că un număr mare de pasageri, în special cei care călătoresc în interiorul Uniunii, vor putea să se regăsească înregistrați aproape permanent. În al doilea rând, în ceea ce privește restricțiile privind utilizarea datelor, observăm că păstrarea datelor cu caracter personal și accesul la astfel de date reprezintă ingerințe separate în exercitarea drepturilor fundamentale la respectarea vieții private și la protecția datelor, care trebuie justificate în mod autonom. Deși existența unor garanții stricte privind accesul la datele păstrate permite o evaluare globală a impactului unei măsuri de supraveghere asupra drepturilor fundamentale menționate, totuși acestea nu permit eliminarea ingerințelor legate de o păstrare generalizată prelungită.

244. În ceea ce privește argumentul Comisiei potrivit căruia este necesar să se păstreze datele din PNR ale tuturor pasagerilor aerieni pentru a permite UIP să îndeplinească sarcina, menționată la articolul 6 alineatul (2) litera (c) din Directiva PNR, de a actualiza sau de a defini noi criterii care să fie utilizate pentru evaluările efectuate în temeiul alineatului (3) litera (b) al acestui articol, observăm că, chiar admițând că acuratețea acestor criterii depinde în parte de compararea lor cu un comportament „normal”, astfel cum afirmă Comisia, nu este mai puțin adevărat că acestea trebuie să fie elaborate pe baza unui comportament „infracțional”. Un astfel de argument care, de altfel, este formulat numai de un număr limitat de state membre nu poate, în opinia noastră, să aibă importanța decisivă pe care Comisia pare să i-o atribuie și să justifice, în sine, stocarea generalizată a datelor din PNR ale tuturor pasagerilor aerieni într-o formă neanonimizată.

245. Având în vedere considerațiile menționate anterior, pentru a asigura o interpretare a articolului 12 alineatul (1) din Directiva PNR care să fie conformă cu articolele 7, 8 și 52 alineatul (1) din cartă, se impune, în opinia noastră, interpretarea acestei dispoziții în sensul că păstrarea datelor din PNR furnizate de transportatorii aerieni către UIP într-o bază de date pentru o perioadă de cinci ani după transferul lor către UIP din statul membru pe teritoriul căruia se află punctul de sosire sau de plecare al zborului este permisă, după efectuarea evaluării prealabile prevăzute la articolul 6 alineatul (2) litera (a) din directiva respectivă, numai în măsura în care se stabilește, pe baza unor criterii obiective, un raport între aceste date și combaterea terorismului sau a infracțiunilor grave. O stocare generalizată și nediferențiată a datelor din PNR

[236] A se vedea Avizul 1/15, punctul 205.

[237] Proiectul de Acord Canada-UE prevedea mascarea numelor tuturor pasagerilor la 30 de zile de la primirea acestora de către Canada și mascarea altor informații enumerate în mod expres la doi ani după această primire; a se vedea articolul 16 alineatul 3 din proiectul de Acord Canada-UE analizat de Curte și Avizul 1/15, punctul 30.

[238] A se vedea Avizul din 19 august 2016, p. 9.

într-o formă neanonimizată poate fi justificată, prin analogie cu ceea ce a afirmat Curtea în jurisprudența menționată, numai în fața unei amenințări grave la adresa securității statelor membre, care se dovedește reală și actuală sau previzibilă, legate, de exemplu, de activități teroriste și cu condiția ca durata acestei stocări să fie limitată la strictul necesar.

246. Delimitarea măsurii de stocare prevăzute la articolul 12 alineatul (1) din Directiva PNR se poate baza, de exemplu, pe o evaluare a riscurilor sau pe experiența dobândită de autoritățile naționale competente, care permite să fie vizate anumite rute aeriene, scheme de călătorie definite, agenții prin intermediul cărora se fac rezervările sau chiar categorii de persoane sau anumite zone geografice, identificate pe baza unor factori obiectivi și nediscriminatorii, astfel cum a statuat Curtea în jurisprudența sa privind păstrarea metadatelor comunicațiilor electronice [239]. În plus, prin analogie cu Avizul 1/15, legătura necesară între datele din PNR și obiectivul urmărit de Directiva PNR trebuie considerată ca fiind stabilită atât timp cât pasagerii aerieni se află în Uniune (sau în statul membru în cauză) sau pleacă din aceasta. Același lucru este valabil și pentru datele pasagerilor care au făcut obiectul unui rezultat pozitiv verificat.

247. Pentru a concluziona cu privire la a opta întrebare preliminară, dorim să consacrăm câteva considerații normelor care reglementează accesul și utilizarea datelor din PNR după efectuarea evaluării prealabile menționate la articolul 6 alineatul (2) litera (a) din Directiva PNR și înainte de depersonalizarea acestora la expirarea perioadei inițiale de păstrare de șase luni prevăzute la articolul 12 alineatul (2) din Directiva PNR.

248. Rezultă din interpretarea coroborată a articolului 6 alineatul (2) litera (b) și a articolului 12 alineatul (3) din Directiva PNR că, pe parcursul acestei perioade inițiale, datele din PNR care nu sunt depersonalizate sau rezultatul prelucrării acestora pot fi comunicate autorităților competente în conformitate cu prima dintre aceste dispoziții, fără respectarea condițiilor prevăzute la literele (a) și (b) din a doua dintre dispozițiile menționate [240]. Articolul 6 alineatul (2) litera (b) din Directiva PNR prevede numai că solicitările autorităților competente pentru o astfel de prelucrare și divulgare trebuie să fie „temeinic justificate” și „bazate pe motive suficiente”.

249. Potrivit unei jurisprudențe constante, amintită de Curte în Avizul 1/15, o reglementare a Uniunii nu se poate limita la a impune ca accesul unei autorități la date cu caracter personal păstrate în mod legal să servească uneia dintre finalitățile acestei reglementări, ci trebuie să prevadă și condițiile materiale și procedurale care guvernează această utilizare [241], printre altele, pentru a proteja aceste date de riscul de abuz [242]. În acest aviz, Curtea a statuat că utilizarea datelor din PNR după verificarea lor la sosirea pasagerilor aerieni în Canada și în timpul ședерii lor în această țară trebuie să se bazeze pe împrejurări noi care justifică această utilizare [243], precizând că „atunci când există elemente obiective care permit să se considere că datele din PNR ale unuia sau mai multor pasageri aerieni ar putea aduce o contribuție efectivă la obiectivul de combatere a infracțiunilor de terorism și a altor infracțiuni transnaționale grave, utilizarea acestor date nu depășește limitele strictului necesar” [244]. Referindu-se prin analogie la punctul 120 din Hotărârea Tele2 Sverige, Curtea a considerat că, pentru a garanta în practică deplina

239 A se vedea în special Hotărârea La Quadrature du Net, punctele 148 și 149.

240 Același lucru este valabil și pentru cererile de comunicare a datelor din PNR formulate de UIP din alte state membre în temeiul articolului 9 alineatul (2) din Directiva PNR.

241 A se vedea Avizul 1/15, punctul 192 și jurisprudența citată. Mai recent, a se vedea Hotărârile Privacy International, punctul 77, și, prin analogie, Prokuratuur, punctul 49 și jurisprudența citată.

242 A se vedea Avizul 1/15, punctul 200.

243 A se vedea Avizul 1/15, punctul 200.

244 A se vedea Avizul 1/15, punctul 201.

respectare a acestor condiții, „este esențial ca utilizarea în timpul ședерii pasagerilor aerieni în Canada a datelor lor din PNR păstrate să fie, în principiu, cu excepția unor situații de urgență justificate corespunzător, condiționată 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 competente, în special în cadrul unor proceduri de prevenire, de detectare sau de urmărire penală”[245]. În consecință, Curtea a supus posibilitatea de a utiliza datele din PNR păstrate după verificarea lor cu ocazia călătoriei aeriene unei duble condiții, una materială – și anume existența unor motive obiective care să justifice o astfel de utilizare – și una procedurală – și anume controlul exercitat de o instanță sau de o autoritate administrativă independentă. Interpretarea adoptată de Curte, departe de a fi „contextuală”, constituie aplicarea în domeniul datelor din PNR a jurisprudenței care rezultă în special din Hotărârea Digital Rights și Hotărârea Tele2 Sverige.

250. Or, cerințele stabilite de Curte în Avizul 1/15 nu sunt respectate de regimul instituit de Directiva PNR în cursul primelor șase luni de păstrare a datelor din PNR, care permite, după evaluarea prealabilă menționată la articolul 6 alineatul (2) litera (a) din această directivă, comunicarea și prelucrarea potențial repetate ale datelor din PNR, în lipsa unor garanții procedurale adecvate și a unor norme materiale suficient de clare și de precise care să definească obiectul și modalitățile acestor diferite ingerințe. Acesta nu pare să îndeplinească nici cerința ca utilizarea datelor din PNR să fie limitată la strictul necesar.

251. În consecință, propunem Curții să interpreteze articolul 6 alineatul (2) litera (b) din Directiva PNR astfel încât prelucrarea datelor în temeiul acestei dispoziții efectuată în cursul perioadei inițiale de șase luni prevăzute la articolul 12 alineatul (2) din această directivă să respecte cerințele stabilite de Curte în Avizul 1/15.

252. În ceea ce privește prima condiție, de natură materială, față de care Curtea a subordonat utilizarea ulterioară a datelor din PNR, considerăm că noțiunile „în mod rezonabil”, în sensul articolului 12 alineatul (3) litera (a) din Directiva PNR, și „motive suficiente”, în conformitate cu articolul 6 alineatul (2) litera (b) din această directivă, pot fi ușor interpretate în sensul că solicitările autorităților competente, avute în vedere în aceste dispoziții, trebuie să indice „elemente obiective care permit să se considere că datele din PNR ale unuia sau mai multor pasageri aerieni ar putea aduce o contribuție efectivă la obiectivul de combatere a infracțiunilor de terorism și a altor infracțiuni […] grave”[246].

253. În ceea ce privește a doua condiție, de natură procedurală, considerăm că articolul 6 alineatul (2) litera (b) din Directiva PNR trebuie interpretat în mod coroborat cu articolul 12 alineatul (3) din aceasta și în lumina articolelor 7, 8 și 52 alineatul (1) din cartă, în sensul că cerința privind aprobarea prealabilă de către o autoritate judiciară sau o autoritate administrativă independentă prevăzută la articolul 12 alineatul (3) litera (b) din această directivă se aplică oricărei prelucrări de date din PNR efectuate în conformitate cu respectivul articol 6 alineatul (2) litera (b).

4. Concluzii cu privire la a doua, a treia, a patra, a șasea și a opta întrebare preliminară

254. Pe baza tuturor considerațiilor care precedă, propunem Curții să anuleze punctul 12 din anexa I în măsura în care acesta include „mențiunile cu caracter general” printre categoriile de date din PNR pe care transportatorii aerieni trebuie să le transmită către UIP, în conformitate cu

[245] A se vedea Avizul 1/15, punctul 202.

[246] A se vedea în acest sens Avizul 1/15, punctul 201.

articolul 8 din Directiva PNR, și să declare că examinarea celei de a doua, a treia, a patra, a șasea și a opta întrebări preliminare nu a evidențiat alte elemente de natură să afecteze validitatea acestei directive, sub rezerva interpretărilor dispozițiilor acesteia propuse la punctele 153, 160, 161-164, 219, 228, 239 și 251 din prezentele concluzii.

255. În lumina răspunsului propus a fi dat la întrebările preliminare referitoare la validitatea Directivei PNR, nu se poate admite, făcând abstracție de orice altă considerație, cererea formulată în special de Consiliu prin care se solicită menținerea efectelor Directivei PNR în cazul în care Curtea decide să anuleze în totalitate sau în parte Directiva PNR.

C. Cu privire la a cincea întrebare preliminară

256. Prin intermediul celei de a cincea întrebări preliminare, instanța de trimitere solicită în esență Curții să stabilească dacă articolul 6 din Directiva PNR coroborat cu articolele 7, 8 și 52 alineatul (1) din cartă trebuie interpretat în sensul că se opune unei reglementări naționale care permite ca scopul prelucrării datelor din PNR să fie monitorizarea activităților vizate de serviciile de informații și de securitate. Rezultă din decizia de trimitere că aceste activități sunt cele desfășurate de serviciul de securitate al statului și de serviciul general de informații și de securitate în cadrul misiunii lor de protejare a securității naționale.

257. Astfel cum am arătat la punctele 113 și 114 din prezentele concluzii, limitarea scopurilor prelucrării datelor cu caracter personal este o garanție esențială care trebuie respectată pentru ca ingerința în exercitarea drepturilor fundamentale consacrate la articolele 7 și 8 din cartă să nu depășească ceea ce este necesar și proporțional în sensul jurisprudenței Curții. Am precizat deja și că, în ceea ce privește ingerințele în exercitarea acestor drepturi fundamentale prevăzute de Directiva PNR, revine legiuitorului Uniunii sarcina de a stabili, pentru a respecta principiile legalității și proporționalității consacrate în special la articolul 52 alineatul (1) din cartă, norme clare și precise care să reglementeze conținutul și aplicarea măsurilor care implică astfel de ingerințe.

258. Or, articolul 1 alineatul (2) din Directiva PNR specifică faptul că datele din PNR colectate în conformitate cu aceasta „pot fi prelucrate doar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, astfel cum este prevăzut la articolul 6 alineatul (2) literele (a), (b) și (c)” din această directivă. În conformitate cu această dispoziție, UIP prelucrează datele din PNR numai în scopul efectuării unei evaluări prealabile a pasagerilor aerieni [articolul 6 alineatul (2) litera (a)], pentru a răspunde la cererile punctuale din partea autorităților competente [articolul 6 alineatul (2) litera (b)] și pentru a actualiza sau a defini noi criterii care urmează să fie utilizate pentru evaluările efectuate în temeiul articolului 6 alineatul (3) litera (b) [articolul 6 alineatul (2) litera (a)]. În toate cele trei cazuri, obiectivele stabilite la articolul 1 alineatul (2) din Directiva PNR în ceea ce privește combaterea terorismului și a infracțiunilor grave sunt menționate în mod explicit.

259. În plus, articolul 7 alineatul (4) din această directivă precizează că nu numai prelucrarea datelor din PNR prevăzută la articolul 6 din directivă, ci și prelucrarea ulterioară a acestor date și a rezultatului acestei prelucrări de către autoritățile competente ale statelor membre trebuie să fie limitate „doar în scopul specific al prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave”.

260. Caracterul exhaustiv al determinării obiectivelor urmărite de Directiva PNR rezultă în mod clar din modul de redactare a articolului 1 alineatul (2) din aceasta și se coroborează, pe lângă articolul 6 alineatul (2) și articolul 7 alineatul (4) deja menționate, cu mai multe articole și considerente ale acestei directive care conectează în mod sistematic fiecare etapă a procesului de accesare, prelucrare, stocare și partajare a datelor din PNR numai de aceste obiective specifice [247].

261. Rezultă atât din textul articolului 1 alineatul (2) din Directiva PNR, cât și din interpretarea acestuia în lumina principiilor legalității și proporționalității, care impun o limitare exhaustivă a scopurilor măsurilor care implică o ingerință în exercitarea drepturilor fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, că orice extindere a scopurilor prelucrării datelor din PNR dincolo de obiectivele de securitate menționate în mod expres de această dispoziție este contrară Directivei PNR.

262. Această interdicție privind extinderea obiectivelor urmărite de directivă se aplică, în opinia noastră, în mod deosebit în ceea ce privește activitățile serviciilor de securitate și de informații ale statelor membre, inclusiv din cauza lipsei de transparență care caracterizează modul lor de operare. În această privință, opiniile noastre corespund cu cele ale Comisiei, și anume că aceste servicii nu ar trebui, ca regulă generală, să aibă acces direct la datele din PNR. În acest context, considerăm deja ca fiind în sine criticabil faptul că UIP naționale, cum este cazul UIP belgiene, pot avea printre membrii lor funcționari detașați de la serviciile de securitate [248].

263. Pe baza considerațiilor menționate anterior, este necesar, în opinia noastră, să se răspundă la a cincea întrebare preliminară în sensul că Directiva PNR, și în special articolul 1 alineatul (2) și articolul 6, trebuie interpretată în sensul că se opune unei reglementări naționale care permite ca scopul prelucrării datelor din PNR să fie desfășurarea anumitor activități ale serviciilor de informații și de securitate, întrucât, în contextul unui astfel de scop, UIP națională ar fi determinată să prelucreze datele menționate și/sau să le transmită sau să transmită rezultatul prelucrării acestora către serviciile respective în alte scopuri decât cele exhaustiv indicate la articolul 1 alineatul (2) din această directivă, aspect care trebuie verificat de instanța națională.

D. Cu privire la a șaptea întrebare preliminară

264. Prin intermediul celei de a șaptea întrebări, instanța de trimitere solicită în esență Curții să stabilească dacă articolul 12 alineatul (3) litera (b) din Directiva PNR trebuie interpretat în sensul că UIP constituie o „autoritate națională competentă” în sensul acestei dispoziții, care poate autoriza dezvăluirea datelor complete din PNR după expirarea perioadei inițiale de șase luni de la transferul acestor date.

265. Reamintim că articolul 12 alineatul (2) din Directiva PNR prevede că, la expirarea unei perioade de șase luni, datele din PNR se depersonalizează prin mascarea anumitor date care ar putea servi la identificarea directă a pasagerului la care acestea se referă. După această perioadă, dezvăluirea datelor complete din PNR este permisă numai în condițiile prevăzute la articolul 12

[247] A se vedea în special articolul 4, articolul 7 alineatele (1) și (2), articolul 9 alineatul (2), articolul 10 alineatul (2), articolul 12 alineatul (4) din Directiva PNR; a se vedea în special considerentele (6), (9), (10), (11), (15), (23), (25), (35) și (38) ale acestei directive. Dorim să subliniem de altfel că propunerea de Directivă PNR enunța în considerentul (28) că „[p]rezenta directivă nu aduce atingere posibilității ca statele membre să prevadă, în conformitate cu dreptul lor intern, un sistem de colectare și prelucrare a datelor din PNR în alte scopuri decât cele menționate în prezenta directivă (...)”. Or, această precizare nu a fost inclusă în textul final al Directivei PNR.

[248] Această posibilitate este totuși permisă de articolul 4 alineatul (3) din Directiva PNR, conform căruia „[m]embrii personalului UIP pot fi detașați de la autoritățile competente”, cel puțin în măsura în care serviciile de informații și de securitate ale statului membru în cauză pot fi calificate drept „autorități competente” în sensul articolului 7 alineatul (2) din această directivă.

alineatul (3) și în special în cazul în care o astfel de dezvăluire a fost aprobată în prealabil de o „autoritate judiciară” [articolul 12 alineatul (3) litera (b) punctul (i)] sau de „o altă autoritate națională competentă, în temeiul dreptului intern, să verifice dacă sunt îndeplinite condițiile pentru dezvăluire, sub rezerva informării responsabilului cu protecția datelor din cadrul UIP și a revizuirii ulterioare de către acesta” [articolul 12 alineatul (3) litera (b) punctul (ii)].

266. Majoritatea guvernelor care au prezentat observații scrise în prezenta procedură nu s-au pronunțat cu privire la a șaptea întrebare preliminară. Guvernul ceh consideră, precum Comisia, că articolul 12 alineatul (3) din Directiva PNR nu poate fi interpretat în sensul că UIP poate constitui o „autoritate națională competentă”. În schimb, guvernele belgian [249], irlandez, spaniol, francez și cipriot se opun unei astfel de interpretări. Acestea consideră în esență că nicio dispoziție din Directiva PNR sau din dreptul Uniunii nu se opune desemnării UIP drept una dintre autoritățile naționale competente, în sensul articolului 12 alineatul (2) litera (b) punctul (ii) din directiva menționată, și că UIP ar fi, prin natura sa, o autoritate suficient de independentă pentru a putea autoriza prelucrarea datelor din PNR.

267. În ceea ce ne privește, observăm, în primul rând, că din textul articolului 12 alineatul (3) litera (b) din Directiva PNR și în special din utilizarea conjuncției „sau” care face legătura între cele două ipoteze de la punctele (i) și (ii) din această dispoziție reiese că legiuitorul Uniunii a intenționat să pună pe același plan controlul exercitat de autoritatea națională menționată la punctul (ii) și cel efectuat de autoritatea judiciară menționată la punctul (i). Rezultă că autoritatea națională menționată trebuie să aibă un nivel de independență și de imparțialitate suficient, astfel încât controlul pe care îl exercită să poată fi considerat o alternativă comparabilă la controlul care poate fi efectuat de o autoritate judiciară [250].

268. În al doilea rând, din lucrările pregătitoare privind Directiva PNR rezultă că legiuitorul Uniunii, pe de o parte, nu a acceptat propunerea Comisiei de a încredința responsabilului din cadrul UIP sarcina de a autoriza dezvăluirea datelor complete din PNR [251] și, pe de altă parte, a extins la șase luni perioada inițială de păstrare a acestor date propusă de Comisie care era de 30 de zile. În acest context, caracterizat de căutarea unui echilibru între durata perioadei de păstrare înainte de depersonalizarea datelor din PNR și condițiile în care este înlăturată mascarea acestora, la sfârșitul perioadei menționate, se înscrie decizia legiuitorului Uniunii de a supune accesul deplin la datele din PNR unor condiții procedurale mai stricte decât cele prevăzute inițial de Comisie și de a încredința unei autorități independente sarcina de a verifica dacă sunt îndeplinite condițiile de dezvăluire.

269. În al treilea rând, astfel cum a observat în mod corect Comisia, rezultă din economia Directivei PNR că rațiunea introducerii procedurii de aprobare prevăzute la articolul 12 alineatul (3) din Directiva PNR este de a atribui unei entități terțe imparțiale sarcina de a evalua comparativ, în fiecare caz în parte, drepturile persoanelor vizate și scopul aplicării legii urmărit de această directivă.

[249] În ceea ce privește îndoielile exprimate de guvernul belgian cu privire la competența Curții de a răspunde la a șaptea întrebare preliminară, este necesar să se constate că, în conformitate cu formularea acestei întrebări, instanța de trimitere adresează Curții o întrebare cu privire la interpretarea articolului 12 alineatul (3) din Directiva PNR, iar nu cu privire la compatibilitatea dreptului intern cu această dispoziție. În orice caz, potrivit unei jurisprudențe constante, Curtea poate oferi indicații instanțelor naționale care să le permită să aprecieze această compatibilitate (a se vedea în special Hotărârea din 7 septembrie 2016, ANODE, C-121/15, EU:C:2016:637, punctul 54 și jurisprudența citată).

[250] A se vedea în acest sens Hotărârea din 5 noiembrie 2019, Comisia/Polonia (Independența instanțelor de drept comun) (C-192/18, EU:C:2019:924, punctele 108-110).

[251] Articolul 9 alineatul (2) teza a patra din propunerea de Directivă PNR prevedea că „[a]ccesul la datele complete din PNR este autorizat numai de către șeful unității de informații despre pasageri […]”.

270. În al patrulea rând, rezultă din jurisprudența Curții că o entitate însărcinată cu efectuarea controlului prealabil necesar pentru a autoriza accesul autorităților naționale competente la datele cu caracter personal păstrate în mod legal trebuie să dispună de toate atribuțiile și să prezinte toate garanțiile necesare în vederea asigurării unei concilieri a diferitelor interese și drepturi în cauză. Curtea a precizat de asemenea că această entitate trebuie să beneficieze de un statut care să îi permită să acționeze în mod obiectiv și imparțial în exercitarea misiunilor sale și trebuie să fie, în acest scop, protejată de orice influență externă [252]. În special, având în vedere cerința de independență impusă, mai ales în domeniul penal, autoritatea responsabilă cu controlul prealabil trebuie să aibă calitatea de terț în raport cu cea care solicită accesul la date, astfel încât să nu fie implicată în desfășurarea investigației penale în cauză și să aibă o poziție de neutralitate față de părțile din procedura penală [253].

271. Or, trebuie remarcat că UIP nu oferă toate garanțiile de independență și de imparțialitate pe care trebuie să le îndeplinească autoritatea responsabilă cu efectuarea controlului prealabil prevăzut la articolul 12 alineatul (3) din Directiva PNR. Într-adevăr, UIP sunt direct legate de autoritățile competente în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor de terorism sau a infracțiunilor grave. În conformitate cu articolul 4 alineatul (1) din Directiva PNR, UIP este ea însăși o astfel de autoritate sau o filială a acesteia. În plus, articolul 4 alineatul (3) din Directiva PNR prevede că membrii personalului UIP pot fi detașați de la autoritățile competente. Acesta este în special cazul UIP belgiene care, în conformitate cu articolul 14 din Legea PNR, este compusă, printre altele, din membri detașați din cadrul poliției, al securității statului, al serviciului general de informații și securitate și al administrației generale a vămilor și accizelor.

272. Desigur, în general, membrii UIP trebuie să ofere toate garanțiile de integritate, competență, transparență și independență, iar statelor membre le revine sarcina de a se asigura eventual că, având în vedere legăturile dintre aceștia și structurile de care aparțin, aceste garanții pot fi respectate în practică, în special pentru a evita ca autoritățile competente din structura cărora acești membri sunt inserați inițial să nu aibă acces direct la baza de date din PNR, ci numai la rezultatele operațiunilor efectuate de UIP. Nu este mai puțin adevărat că membrii UIP care sunt detașați de la autoritățile competente, în sensul articolului 7 alineatul (2) din Directiva PNR, păstrează în mod inevitabil o legătură cu serviciile lor de origine pe perioada detașării, păstrându-și statutul chiar dacă sunt plasați sub autoritatea funcțională și ierarhică a funcționarului care administrează UIP.

273. Concluzia potrivit căreia UIP nu este o autoritate națională în sensul articolului 12 alineatul (3) litera (b) punctul (ii) din Directiva PNR este de altfel susținută și de faptul că, în conformitate cu această dispoziție, responsabilul cu protecția datelor din cadrul UIP în cauză trebuie să fie „informat” cu privire la cererea de divulgare și efectuează o „revizuire ulterioară”. Într-adevăr, în cazul în care UIP ar fi împuternicită, în calitate de „altă autoritate națională”, să aprobe o cerere de dezvăluire, în temeiul articolului 12 alineatul (3) din Directiva PNR, responsabilul cu protecția datelor care este însărcinat, printre altele, potrivit articolului 5 alineatul (1) din această directivă, cu punerea în aplicare a garanțiilor relevante care însoțesc prelucrarea datelor din PNR, ar fi informat cu privire la cererea de acces la momentul depunerii acesteia, iar controlul său ar interveni în mod necesar *ex ante* [254].

252 Hotărârea Prokuratuur, punctele 52 și 53.

253 Hotărârea Prokuratuur, punctele 53 și 54. În același sens, a se vedea Hotărârea Big Brother Watch, punctele 349-352.

254 Articolul 9 alineatul (2) teza a patra din propunerea de Directivă PNR prevedea că „[a]ccesul la datele complete din PNR este autorizat numai de către șeful unității de informații despre pasageri”.

274. Având în vedere considerentele precedente, propunem Curții să răspundă la a șaptea întrebare preliminară că articolul 12 alineatul (3) litera (b) din Directiva PNR trebuie interpretat în sensul că UIP nu constituie o „altă autoritate națională competentă” în sensul acestei dispoziții.

E. Cu privire la a noua întrebare preliminară

275. Prin intermediul celei de a noua întrebări preliminare, instanța de trimitere solicită în esență Curții, pe de o parte, să stabilească dacă Directiva API este compatibilă cu articolul 3 alineatul (2) TUE și cu articolul 45 din cartă, în măsura în care se aplică zborurilor în interiorul Uniunii, și, pe de altă parte, dacă această directivă coroborată cu articolul 3 alineatul (2) TUE și cu articolul 45 din cartă trebuie interpretată în sensul că se opune unei reglementări naționale care, în vederea combaterii imigrației ilegale și al îmbunătățirii controalelor la frontiere, autorizează un sistem de colectare și de prelucrare a datelor pasagerilor care ar putea implica în mod indirect restabilirea controalelor la frontierele interne.

276. Rezultă din decizia de trimitere că această întrebare preliminară se înscrie în cadrul analizei celui de al doilea motiv al acțiunii, invocat de LDH cu titlu subsidiar. Acest motiv, întemeiat pe încălcarea articolului 22 din Constituția belgiană coroborat cu articolul 3 alineatul (2) TUE și cu articolul 45 din cartă, este îndreptat împotriva articolului 3 alineatul (1), articolului 8 alineatul (2) și capitolului 11, în special articolelor 28-31, din Legea PNR. Deși primul dintre aceste articole enunță, în termeni generali, scopul acestei legi, precizând că aceasta „stabilește obligațiile transportatorilor și ale operatorilor de turism referitoare la transmiterea datelor pasagerilor care călătoresc spre, pleacă de pe sau tranzitează teritoriul național”, articolul 8 alineatul (2) din legea menționată prevede că, „[î]n condițiile prevăzute în capitolul 11 [din aceasta], datele pasagerilor sunt prelucrate de asemenea în scopul îmbunătățirii controlului persoanelor la frontierele externe și al combaterii imigrației ilegale”. În cadrul acestui scop, în conformitate cu articolul 29 alineatul (1) din Legea PNR, numai „datele pasagerilor” menționate la articolul 9 alineatul (1) punctul 18 din legea menționată (și anume, datele API de la punctul 18 din Directiva PNR), referitoare la trei categorii de pasageri, sunt transmise serviciilor de poliție responsabile cu controlul la frontieră și Oficiului pentru străini (Belgia). Este vorba despre „pasagerii care intenționează să intre sau au intrat pe teritoriu pe la frontierele externe ale Belgiei”, „pasagerii care intenționează să părăsească sau au părăsit teritoriul pe la frontierele externe ale Belgiei” și „pasagerii care intenționează să treacă prin, se află în sau au trecut printr-o zonă internațională de tranzit situată în Belgia” [255]. Rezultă din articolul 29 alineatul (3) din Legea PNR că aceste date sunt transmise serviciilor de poliție responsabile cu controlul la frontieră și Oficiului pentru străini de către UIP „imediat după înregistrarea lor în banca de date privind pasagerii” și că sunt distruse la 24 de ore după transmitere. Potrivit dispoziției amintite, după această perioadă, Oficiul pentru străini poate de asemenea să trimită o cerere motivată la UIP pentru a obține accesul la aceleași date, atunci când acest lucru este necesar în cadrul misiunii sale legale. În consecință, cadrul juridic în care se înscrie a noua întrebare preliminară se situează în afara celui al Directivei PNR, dat fiind obiectivul prelucrării datelor menționat la articolele 28 și 29 din Legea PNR, și se înscrie în cel al Directivei API. În plus, reiese în special din dosarul depus la grefa Curții că al doilea motiv invocat de LDH se întemeiază pe o interpretare a dispozițiilor capitolului 11 din Legea PNR potrivit căreia aceste dispoziții se aplică și în cazul trecerii frontierelor interne ale Belgiei.

[255] Legea PNR, articolul 29, alineatele (1) și (2).

277. Prima parte a celei de a noua întrebări se bazează pe o presupunere eronată și, în opinia noastră, nu necesită un răspuns din partea Curții. Astfel, din articolul 3 alineatul (1) din Directiva API coroborat cu articolul 2 literele (b) și (d) din aceasta rezultă în mod neechivoc că această directivă prevede obligația transportatorilor aerieni de a transmite datele API autorităților responsabile de controlul persoanelor la frontierele externe numai în ceea ce privește zborurile care transportă pasageri către un punct de trecere autorizat pentru trecerea frontierelor externe ale statelor membre cu țări terțe. De asemenea, articolul 6 alineatul (1) din această directivă prevede numai prelucrarea datelor API referitoare la astfel de zboruri. În plus, chiar dacă este adevărat că Directiva PNR prevede posibilitatea ca statele membre să extindă obligația de a transfera datele API colectate și la transportatorii aerieni care operează zboruri intra-UE, această extindere trebuie interpretată fără a aduce atingere Directivei API [256]. În contextul Directivei PNR, datele API transferate vor fi prelucrate numai în limitele obiectivelor de aplicare a legii prevăzute de această directivă. În schimb, considerentul (34) al Directivei PNR prevede că aceasta nu aduce atingere normelor actuale ale Uniunii privind modalitățile în care se realizează controalele la frontieră și nici normelor Uniunii care reglementează intrarea pe și ieșirea de pe teritoriul Uniunii, iar articolul 6 alineatul (9) a doua teză din Directiva PNR prevede că, atunci când evaluările efectuate în temeiul alineatului (2) al articolului respectiv se efectuează în cazul unor zboruri intra-UE între state membre cărora li se aplică Codul Frontierelor Schengen [257], consecințele acestor evaluări respectă regulamentul menționat.

278. Reformularea acestei părți a celei de a noua întrebări preliminare, astfel cum sugerează în subsidiar Comisia, în sensul că aceasta privește compatibilitatea Directivei PNR, în special a articolului 2 din aceasta, iar nu a Directivei API cu dispozițiile tratatului și ale cartei, ar însemna nu numai să se modifice actul cu privire la care instanța de trimitere a solicitat aprecierea validității, ci ar însemna de asemenea ieșirea din cadrul juridic în care se înscrie această întrebare preliminară. Într-adevăr, astfel cum am explicat, dispozițiile capitolului 11 din Legea PNR, împotriva cărora este îndreptat al doilea motiv al acțiunii, transpun Directiva API, iar nu Directiva PNR.

279. În ipoteza în care Curtea ar face o astfel de reformulare, ne limităm la următoarele reflecții, în special în ceea ce privește întrebarea dacă evaluarea prealabilă pe care statele membre sunt autorizate să o efectueze cu privire la datele din PNR ale pasagerilor zborurilor intra-UE, în conformitate cu competența de care dispun în sensul articolului 2 din Directiva PNR, poate fi considerată echivalentă cu exercitarea „verificărilor la frontiere” în sensul articolului 23 litera (a) din Codul Frontierelor Schengen [258]. În primul rând, în cazul în care evaluarea prealabilă a datelor din PNR nu are loc „la punctul de trecere a frontierei” sau în „momentul trecerii frontierei”, ci înainte de acest moment, aceasta este totuși efectuată „din cauza” trecerii iminente a frontierei. În al doilea rând, în conformitate cu articolul 2 din Directiva PNR, statele membre sunt autorizate să extindă evaluarea prealabilă a datelor din PNR, prevăzută la articolul 6 alineatul (2) litera (a) din Directiva PNR, la pasagerii tuturor zborurilor intra-UE, indiferent de comportamentul persoanelor în cauză și de împrejurările care stabilesc un risc la adresa siguranței publice. Această evaluare prealabilă are în plus un caracter sistematic. Or, niciunul dintre aceste

256 A se vedea considerentul (10) al Directivei PNR.

257 Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO 2016, L 77, p. 1, denumit în continuare „Codul Frontierelor Schengen”).

258 Articolul 23 litera (a) din Codul Frontierelor Schengen prevede că exercitarea competențelor polițienești nu poate fi considerată echivalentă cu exercitarea verificărilor la frontiere în cazul în care măsurile poliției: „(i) nu au ca obiectiv controlul la frontiere; (ii) se bazează pe informații generale și pe experiența serviciilor de poliție privind eventualele amenințări la adresa securității publice și vizează în special combaterea criminalității transfrontaliere; (iii) sunt concepute și executate într-o manieră net diferită de verificările sistematice asupra persoanelor efectuate la frontierele externe; (iv) sunt realizate pe baza verificărilor inopinate”.

elemente nu pare să îndeplinească cerințele prevăzute la articolul 23 litera (a) a doua teză punctele (ii), (iii) și (iv) din Codul Frontierelor Schengen [259]. În al treilea rând, în ceea ce privește cerințele menționate la articolul 23 litera (a) teza a doua punctele (i) și (iii) din Codul Frontierelor Schengen, ne punem întrebarea dacă evaluarea prealabilă în temeiul articolului 6 alineatul (2) litera (a) din Directiva PNR nu se suprapune, cel puțin parțial, cu scopul verificărilor la frontieră efectuate în conformitate cu articolul 8 alineatul (2) litera (b) și alineatul (3) litera (a) punctul (vi) și litera (g) punctul (iii) din Codul Frontierelor Schengen, astfel cum a fost modificat prin Regulamentul 2017/458, și în special dacă aceasta se distinge în mod clar, din punctul de vedere al modalităților sale, de aceste verificări sistematice [260]. În această privință, observăm că articolul 8 alineatul (2e) și alineatul (3) litera (i) punctul (ia) din cod specifică faptul că astfel de verificări „pot fi efectuate în prealabil, pe baza datelor privind pasagerii primite în conformitate cu Directiva [API] sau în conformitate cu alte dispoziții legale naționale sau ale Uniunii”. Cu toate acestea, este adevărat că scopul Directivei PNR nu este „să garanteze că persoanele *pot fi autorizate* să intre pe teritoriul statului membru sau să îl părăsească” sau „să împiedice persoanele să se sustragă de la verificări”, pe care Curtea le-a recunoscut ca fiind obiective ale „controlului la frontiere” în temeiul Codului Frontierelor Schengen [261], întrucât această directivă are un scop exclusiv de aplicare a legii. În plus, articolul 23 litera (a) a doua teză punctul (ii) din codul menționat prevede în mod explicit că exercitarea competențelor polițienești nu poate fi considerată echivalentă cu exercitarea verificărilor la frontiere în cazul în care controalele vizează în special combaterea criminalității transfrontaliere [262]. În sfârșit, Curtea ar trebui să ia în considerare la aprecierea sa și împrejurarea, subliniată îndeosebi de Comisie, că articolul 2 din Directiva PNR autorizează statele membre doar să impună transportatorilor aerieni să transfere datele din PNR pe care le-au colectat în cursul normal al activităților lor și, în consecință, nu prevede o obligație similară cu cea prevăzută de Directiva API pentru trecerea frontierelor externe.

280. În ceea ce privește a doua parte a celei de a noua întrebări preliminare, considerăm, precum Comisia, că aceasta trebuie interpretată în sensul că se raportează la trecerea frontierelor interne și că vizează obținerea unor clarificări din partea Curții care să permită instanței de trimitere să evalueze compatibilitatea dispozițiilor capitolului 11 din Legea PNR cu eliminarea controalelor la frontierele interne ale statelor membre din spațiul Schengen.

281. În această privință, având în vedere puținele elemente de care dispune Curtea, ne limităm să observăm că dispozițiile capitolului 11 din Legea PNR pot fi compatibile cu dreptul Uniunii și în special cu articolul 67 alineatul (2) TFUE numai în cazul în care sunt interpretate în sensul că se referă doar la transferul și prelucrarea datelor API ale pasagerilor care trec frontierele externe ale Belgiei cu țări terțe.

282. În măsura în care Curtea ar decide să reformuleze a doua parte a celei de a noua întrebări preliminare în sensul că vizează interpretarea Directivei PNR în raport cu dispozițiile capitolului 11 din Legea PNR, ne limităm să arătăm că prelucrarea datelor API prevăzută la articolele 28 și 29 din această lege se grefează pe sistemul instituit de legiuitorul belgian în vederea transpunerii Directivei PNR. Astfel, în primul rând, datele API care fac obiectul prelucrării sunt

[259] A se vedea prin analogie Hotărârea din 13 decembrie 2018, Touring Tours und Travel și Sociedad de transportes (C-412/17 și C-474/17, EU:C:2018:1005, punctul 61 și jurisprudența citată), precum și Ordonanța din 4 iunie 2020, FU (C-554/19, nepublicată, EU:C:2020:439, punctele 49-56).

[260] În această privință, observăm că, la punctul 188 din Avizul 1/15, Curtea a afirmat că „identificarea, prin intermediul datelor din PNR, a pasagerilor care pot prezenta un risc pentru securitatea publică face parte din controalele la frontieră”.

[261] A se vedea Hotărârea din 13 decembrie 2018, Touring Tours und Travel și Sociedad de transportes (C-412/17 și C-474/17, EU:C:2018:1005, punctul 55 și jurisprudența citată).

[262] A se vedea în acest sens în special Ordonanța din 4 iunie 2020, FU (C-554/19, nepublicată, EU:C:2020:439, punctul 46).

cele enumerate la punctul 12 din anexa I la această directivă, iar nu doar cele conținute în lista care figurează la articolul 3 alineatul (2) din Directiva API. În al doilea rând, în conformitate cu articolul 29 alineatul (1) din Legea PNR, aceste date sunt transmise serviciilor de poliție responsabile cu controlul la frontieră și Oficiului pentru străini de către UIP – care are responsabilitatea de a colecta și de a prelucra datele din PNR exclusiv în scopurile urmărite de Directiva PNR –, iar nu, astfel cum prevede Directiva API, direct de către transportatorii aerieni. În plus, această transmitere se referă și la datele pasagerilor care intenționează să părăsească sau care au părăsit teritoriul belgian și nu se adresează numai autorităților responsabile de controlul la frontieră, ci și Oficiului pentru străini care este responsabil de gestionarea populației imigrante și de combaterea imigrației clandestine. În al treilea rând, în temeiul articolului 29 alineatul (4) al doilea paragraf din Legea PNR, Oficiul pentru străini pare să aibă competența de a adresa UIP cereri de acces la datele API chiar și după prelucrarea acestor date cu ocazia trecerii frontierelor de către pasagerii în cauză. În acest sens, oficiul menționat este *de facto* asimilat unei autorități competente în temeiul articolului 7 din Directiva PNR, chiar dacă nu este de aceeași natură și nu figurează pe lista acestor autorități care a fost comunicată Comisiei de către Belgia. Or, un astfel de amalgam între sistemele prevăzute de Directiva API și de Directiva PNR nu poate fi acceptat, în opinia noastră, pentru faptul că încalcă principiul limitării obiectivelor stabilit la articolul 1 alineatul (2) din Directiva PNR [263].

283. Având în vedere toate considerațiile sus-menționate, propunem Curții să răspundă la a noua întrebare preliminară în sensul că articolul 3 alineatul (1) din Directiva API, în temeiul căruia statele membre iau toate măsurile necesare pentru a obliga operatorii de transport să transmită, la cererea autorităților însărcinate cu controlul persoanelor la frontierele externe, înainte de sfârșitul înregistrării, informațiile privind pasagerii menționate la alineatul (2) al articolului amintit coroborat cu articolul 2 literele (b) și (d) din directiva respectivă vizează numai pasagerii transportați spre un punct de trecere autorizat pentru trecerea frontierelor externe ale statelor membre cu țări terțe. O reglementare națională care, doar în scopul de a îmbunătăți controalele la frontieră și de a combate imigrația ilegală, ar extinde această obligație la datele persoanelor care trec frontierele interne ale statului membru în cauză cu avionul sau cu alte mijloace de transport ar fi contrară articolului 67 alineatul (2) TFUE și articolului 22 din Codul frontierelor Schengen.

F. Cu privire la a zecea întrebare preliminară

284. Prin intermediul celei de a zecea întrebări preliminare, instanța de trimitere solicită în esență Curții să stabilească dacă, în cazul în care va concluziona că Legea PNR încalcă articolele 7, 8 și 52 alineatul (1) din cartă, ar putea menține provizoriu efectele acestei legi pentru a evita insecuritatea juridică și pentru a permite ca datele colectate și păstrate anterior să fie utilizate în continuare în scopurile vizate de Legea PNR.

285. Curtea a răspuns la o întrebare similară în Hotărârea La Quadrature du Net privind stocarea metadatelor comunicațiilor electronice, pronunțată după introducerea prezentei cereri de decizie preliminară. În acea hotărâre, Curtea a reamintit mai întâi jurisprudența sa potrivit căreia s-ar aduce atingere supremației și aplicării uniforme ale dreptului Uniunii dacă instanțele naționale ar avea puterea de a conferi dispozițiilor naționale supremația în raport cu dreptul Uniunii față de care aceste dispoziții sunt contrare, chiar și numai cu titlu provizoriu. În continuare, aceasta a reamintit că, în Hotărârea din 29 iulie 2019, Inter-Environnement Wallonie et Bond Beter

[263] În documentul său de lucru din anul 2020 privind Directiva API (p. 20), Comisia subliniază de asemenea caracterul problematic al unei suprapuneri a sistemelor de prelucrare a datelor din PNR și API la nivel național.

Leefmilieu Vlaanderen [264], în care era în discuție legalitatea unor măsuri adoptate cu încălcarea obligației prevăzute de dreptul Uniunii de a efectua o evaluare prealabilă a efectelor unui proiect asupra mediului și asupra unui sit protejat, a admis că o instanță națională poate, dacă dreptul intern o permite, să mențină în mod excepțional efectele unor astfel de măsuri atunci când această menținere este justificată de considerații imperative legate de necesitatea de a înlătura o amenințare reală și gravă de întrerupere a aprovizionării cu energie electrică a statului membru în cauză în perioada strict necesară pentru a remedia nelegalitatea respectivă. Cu toate acestea, Curtea a concluzionat că, spre deosebire de omisiunea unei obligații procedurale precum evaluarea prealabilă a efectelor unui proiect în domeniul specific al protecției mediului, o încălcare a drepturilor fundamentale garantate de articolele 7 și 8 din cartă nu poate face obiectul unei regularizări pe calea unei proceduri comparabile cu cea prevăzută în hotărârea sus-menționată [265]. Considerăm că același răspuns trebuie furnizat și celei de a zecea întrebări preliminare din cadrul prezentei proceduri.

286. În măsura în care atât instanța de trimitere și guvernul belgian, cât și Comisia și Consiliul ridică problema dacă dreptul Uniunii se opune utilizării, în cadrul unei proceduri penale, a informațiilor sau a probelor obținute prin utilizarea datelor din PNR colectate, prelucrate și/sau păstrate într-un mod incompatibil cu dreptul Uniunii, reamintim că, la punctul 222 din Hotărârea La Quadrature du Net, Curtea a precizat că, în stadiul actual al dreptului Uniunii, revine, în principiu, numai dreptului național sarcina de a stabili normele referitoare la admisibilitatea și la aprecierea, în cadrul unei proceduri penale inițiate împotriva unor persoane suspectate de săvârșirea unor infracțiuni grave, a informațiilor și a elementelor de probă obținute printr-o păstrare a datelor contrară dreptului Uniunii, sub rezerva respectării principiilor echivalenței și efectivității. În ceea ce privește acest din urmă principiu, Curtea a considerat că acesta impune instanței penale naționale să înlăture informațiile și elementele de probă care au fost obținute prin intermediul unei stocări generalizate și nediferențiate a datelor de transfer și a datelor de localizare, incompatibilă cu dreptul Uniunii, într-o procedură penală inițiată împotriva unor persoane suspectate de săvârșirea unor infracțiuni, în cazul în care persoanele respective nu sunt în măsură să prezinte în mod eficient observații cu privire la aceste informații și elemente de probă care provin dintr-un domeniu care excedă cunoștințelor instanței și care pot influența în mod preponderent aprecierea faptelor. Aceste principii pot fi transpuse *mutatis mutandis* și împrejurărilor din litigiul principal.

IV. Concluzie

287. Pe baza tuturor considerațiilor menționate anterior, propunem Curții să răspundă la întrebările preliminare adresate de Cour constitutionnelle (Curtea Constituțională, Belgia), după cum urmează:

1) Articolul 23 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 (Regulamentul general privind protecția datelor) coroborat cu articolul 2 alineatul (2) litera (d) din acest regulament trebuie interpretat în sensul că:

   – se aplică unei reglementări naționale care transpune Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din

[264] C-411/17, EU:C:2019:622, punctele 175, 176, 179 și 181.

[265] A se vedea Hotărârea La Quadrature du Net, punctele 217-219.

registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, în măsura în care aceasta reglementează prelucrarea datelor din PNR efectuată de transportatorii aerieni și de alți operatori economici, inclusiv transferul datelor din PNR către unitățile de informații despre pasageri (UIP) prevăzute la articolul 4 din directiva menționată, în conformitate cu articolul 8 din aceasta;

– nu se aplică unei reglementări naționale care transpune Directiva 2016/681, în măsura în care aceasta reglementează prelucrarea datelor efectuată în scopurile prevăzute la articolul 1 alineatul (2) din această directivă de către autoritățile naționale competente, inclusiv de către UIP și, după caz, de către serviciile de securitate și de informații ale statului membru în cauză;

– se aplică unei reglementări naționale care transpune Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii și Directiva 2010/65/UE a Parlamentului European și a Consiliului din 20 octombrie 2010 privind formalitățile de raportare aplicabile navelor la sosirea în și/sau la plecarea din porturile statelor membre și de abrogare a Directivei 2002/6/CE, în vederea îmbunătățirii controalelor persoanelor la frontierele externe și a combaterii imigrației ilegale.

2) Punctul 12 din anexa I la Directiva 2016/681 este nevalid, în măsura în care include „mențiunile cu caracter general” printre categoriile de date pe care transportatorii aerieni trebuie să le transmită către UIP, în conformitate cu articolul 8 din această directivă.

3) Examinarea celei de a doua, de a treia, de a patra, de a șasea și de a opta întrebări nu a evidențiat niciun alt element de natură să afecteze validitatea Directivei 2016/681.

4) Punctul 12 din anexa I la Directiva 2016/681, în ceea ce privește partea care nu este declarată nevalidă, trebuie interpretat în sensul că vizează numai informațiile referitoare la minori menționate în mod expres și care sunt direct legate de zbor.

5) Punctul 18 din anexa I la Directiva 2016/681 trebuie interpretat în sensul că se referă numai la informațiile prealabile privind pasagerii care sunt enumerate în mod expres la acest punct, precum și la articolul 3 alineatul (2) din Directiva 2004/82 și care au fost colectate de transportatorii aerieni în cadrul desfășurării activităților lor obișnuite.

6) Noțiunea de „baze de date relevante” menționată la articolul 6 alineatul (3) litera (a) din Directiva 2016/681 trebuie interpretată în sensul că se referă numai la bazele de date naționale gestionate de autoritățile competente în temeiul articolului 7 alineatul (1) din această directivă, precum și la bazele de date ale Uniunii și internaționale exploatate în mod direct de aceste autorități în cadrul atribuțiilor lor. Aceste baze de date trebuie să aibă o legătură directă și strânsă cu obiectivele de combatere a terorismului și a infracțiunilor grave urmărite de directiva amintită, ceea ce presupune ca ele să fi fost dezvoltate în aceste scopuri. La transpunerea Directivei 2016/681 în dreptul intern, statele membre au obligația de a publica o listă a acestor baze de date și de a o actualiza.

7) Articolul 6 alineatul (3) litera (b) din Directiva 2016/681 trebuie interpretat în sensul că se opune utilizării, în cadrul prelucrării automatizate prevăzute de această dispoziție, a unor sisteme algoritmice care pot conduce la o modificare, fără intervenție umană, a criteriilor prestabilite pe baza cărora a fost efectuată această prelucrare și care nu permit identificarea în mod clar și transparent a motivelor care au condus la un rezultat pozitiv ca urmare a prelucrării menționate.

8) Articolul 12 alineatul (1) din Directiva 2016/681 coroborat cu articolele 7, 8 și 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretat în sensul că este permisă păstrarea într-o bază de date a datelor din PNR furnizate de transportatorii aerieni către UIP pentru o perioadă de cinci ani după transferul acestora către UIP din statul membru pe teritoriul căruia se află punctul de sosire sau de plecare al zborului, după efectuarea evaluării prealabile în temeiul articolului 6 alineatul (2) litera (a) din această directivă, numai în măsura în care se stabilește, pe baza unor criterii obiective, o legătură între aceste date și combaterea terorismului sau a infracțiunilor grave. Păstrarea generalizată și nediferențiată a acestor date din PNR într-o formă neanonimizată poate fi justificată numai în fața unei amenințări grave la adresa securității statelor membre, care se dovedește reală și actuală sau previzibilă, legată, de exemplu, de activități de terorism, și cu condiția ca durata acestei păstrări să fie limitată la strictul necesar.

9) Articolul 6 alineatul (2) litera (b) din Directiva 2016/681 trebuie interpretat în sensul că comunicarea datelor din PNR sau a rezultatului prelucrării acestor date în temeiul acestei dispoziții, care are loc în cursul perioadei inițiale de șase luni prevăzute la articolul 12 alineatul (2) din această directivă, trebuie să respecte condițiile prevăzute la articolul 12 alineatul (3) litera (b) din directiva menționată.

10) Directiva 2016/681, și în special articolul 1 alineatul (2) și articolul 6 din aceasta, trebuie interpretată în sensul că se opune unei reglementări naționale care acceptă ca obiectiv al prelucrării datelor din PNR desfășurarea anumitor activități ale serviciilor de informații și de securitate, în măsura în care, în cadrul unui astfel de obiectiv, UIP națională ar fi determinată să prelucreze aceste date și/sau să le transmită sau să transmită rezultatul prelucrării lor serviciilor respective în alte scopuri decât cele indicate în mod exhaustiv la articolul 1 alineatul (2) din directiva menționată, aspect a cărui verificare este de competența instanței naționale.

11) Articolul 12 alineatul (3) litera (b) din Directiva 2016/681 trebuie interpretat în sensul că UIP nu constituie o „altă autoritate națională competentă” în sensul acestei dispoziții.

12) Articolul 3 alineatul (1) din Directiva 2004/82, potrivit căruia statele membre iau toate măsurile necesare pentru a stabili obligația transportatorilor aerieni de a transmite, la cererea autorităților însărcinate cu controlul persoanelor la frontierele externe, înainte de sfârșitul înregistrării, informațiile privind pasagerii menționate la alineatul (2) al acestui articol coroborat cu articolul 2 literele (b) și (d) din directiva amintită vizează numai pasagerii transportați către un punct de trecere autorizat pentru trecerea frontierelor externe ale statelor membre cu țări terțe. O reglementare națională care, numai în scopul de a îmbunătăți controalele la frontieră și de a combate imigrația ilegală, ar extinde această obligație la datele persoanelor care trec frontierele interne ale statului membru în cauză cu avionul sau cu un alte mijloace de transport ar fi contrară articolului 67 alineatul (2) TFUE și

articolului 22 din Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul frontierelor Schengen).

13) O instanță națională nu poate aplica o dispoziție din dreptul său intern care îi permite să limiteze în timp efectele unei declarații de nelegalitate care îi revine în temeiul acestui drept în ceea ce privește o reglementare națională care impune transportatorilor aerieni, terestri și maritimi, precum și operatorilor de turism, în vederea combaterii terorismului și a infracțiunilor grave, să transfere datele din PNR ale pasagerilor și care prevede o prelucrare și o păstrare generalizate și nediferențiate ale acestor date, incompatibile cu articolele 7, 8 și 52 alineatul (1) din Carta drepturilor fundamentale. În conformitate cu principiul efectivității, instanța penală națională este obligată să înlăture informațiile și elementele de probă obținute în temeiul unei astfel de reglementări incompatibile cu dreptul Uniunii, într-o procedură penală inițiată împotriva persoanelor suspectate de săvârșirea unor acte de terorism sau a unor infracțiuni grave, în cazul în care aceste persoane nu sunt în măsură să formuleze observații în mod efectiv cu privire la aceste informații și probe, informații și elementele de probă care provin dintr-un domeniu care excedă cunoștințelor instanței și care pot influența în mod determinant aprecierea faptelor.