

**Cauza C-817/19****Rezumatul cererii de decizie preliminară întocmit în temeiul articolului 98 alineatul (1) din Regulamentul de procedură al Curții de Justiție****Data depunerii:**

31 octombrie 2019

**Instanța de trimitere:**

Cour constitutionnelle (Belgia)

**Data deciziei de trimitere:**

17 octombrie 2019

**Reclamantă:**

ASBL „Ligue des droits humains”

---

**I. Obiectul acțiunii și poziția părților**

- 1 Legiuitorul belgian a adoptat Legea din 25 decembrie 2016 privind prelucrarea datelor pasagerilor (*Moniteur belge* din 25 ianuarie 2017, denumită de asemenea în continuare „Legea PNR”) pentru a transpune în principal:
  - Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (denumită de asemenea în continuare „Directiva PNR”).
  - Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii (denumită de asemenea în continuare „Directiva API”).
- 2 Legea PNR impune diverselor sectoare ale transportului de persoane cu caracter internațional (aerian, feroviar, rutier internațional și maritim) și operatorilor de turism să transmită datele pasagerilor lor unei bănci de date administrate de SPF Intérieur [Serviciul Public Federal de Afaceri Interne].
- 3 În acest scop, legea creează în cadrul SPF de Afaceri Interne o „Unitate de informații despre pasageri” (articolele 12-14), formată printre alții din membri

detașați ai serviciilor de poliție, de siguranță a statului, de informații și de securitate și vamale, responsabilă în special de colectarea, păstrarea și prelucrarea datelor pasagerilor transmise de transportatori și de operatorii de turism.

- 4 „Banca de date privind pasagerii” cuprinde, pe de o parte, datele de rezervare și, pe de altă parte, datele de înregistrare și de îmbarcare [date denumite „API” (Advance Passenger Information) și date denumite „PNR” (Passenger Name Record)] (articolul 9).
- 5 Aceste date sunt prelucrate în special în scopul cercetării, al urmăririi penale și al executării pedepselor aferente unor infracțiuni prevăzute de lege, precum și al prevenirii tulburărilor grave ale siguranței publice în cadrul radicalizării violente, al monitorizării activităților serviciilor de informații și de securitate și în vederea îmbunătățirii controlului persoanelor la frontierele externe și a combaterii imigrației ilegale (articolul 8).
- 6 Prelucrarea datelor poate interveni în cadrul evaluării prealabile a pasagerilor (înainte de plecarea sau de sosirea lor) (articolele 24-26) sau în cadrul unor cercetări care vizează informații specifice (articolul 27).
- 7 Legea prevede că datele pasagerilor sunt păstrate în banca de date privind pasagerii pentru o perioadă maximă de cinci ani începând de la înregistrarea lor (articolele 18-23).
- 8 ASBL „Ligue des droits humains” critică legea sub următoarele șapte aspecte:
  - modalitățile de punere în aplicare a Legii din 25 decembrie 2016 (articolul 3 alineatul 2 și articolul 7 alineatul 3);
  - noțiunile de „documente de identitate” și de „documente de călătorie” (articolul 7 alineatele 1 și 2);
  - datele vizate (articolul 4 punctul 9 și articolul 9);
  - noțiunea de „pasager” (articolul 4 punctul 10);
  - scopurile prelucrării datelor „PNR” (articolul 8);
  - administrarea băncii de date privind pasagerii și prelucrarea datelor în cadrul evaluării prealabile a pasagerilor și al cercetărilor care vizează informații specifice (articolele 12-16, 24-27, 50 și 51);
  - perioada de păstrare a datelor PNR (articolul 18).
- 9 Aceasta denunță neregularități și a sesizat Cour constitutionnelle [Curtea Constituțională] cu o acțiune în anulare întemeiată pe două motive.

- 10 Primul motiv se întemeiază în esență pe articolul 23 din Regulamentul (UE) 2016/679<sup>1</sup>, pe articolul 7, pe articolul 8 și pe articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) și pe articolul 8 din Convenția europeană a drepturilor omului (denumită în continuare „CEDO”).
- 11 Aceasta susține, în esență, că ingerința în dreptul la respectarea vieții private și în dreptul la protecția datelor cu caracter personal este ilicită întrucât nu răspunde criteriilor de legalitate, de necesitate și de proporționalitate.
- 12 În primul rând, Legea PNR conferă o marjă de apreciere importantă puterii executive, pe care o însărcinează să definească, prin decret regal, anumite elemente esențiale cu încălcarea principiului legalității, care impune ca ingerința să fie prevăzută de lege sau, în cazul delegării către Rege, ca elementele esențiale să fie prevăzute de lege în mod suficient de precis și detaliat.  
  
Pe de altă parte, legea atacată nu urmărește un scop legitim. Aceasta prevede, astfel, o evaluare prealabilă denumită „pre-screening”, care constă în evaluarea riscului pe care îl prezintă pasagerii înainte de sosirea, de tranzitul sau de plecarea de pe teritoriul național.
- 13 Reclamanta contestă apoi necesitatea măsurilor atacate pentru îndeplinirea scopului urmărit.  
  
Aceasta susține că o corelare a datelor, în mod clar mai puțin intruzivă în viața privată decât crearea unei bănci de date, ar permite de asemenea atingerea obiectivului urmărit.
- 14 În sfârșit, aceasta susține că legea atacată nu respectă principiul proporționalității, în măsura în care datele sunt colectate în mod nediferențiat și generalizat de către operatori și transmise autorităților competente pentru a fi păstrate timp de cinci ani, fără distincție, diferențiere, limitare sau excepție în funcție de obiectivul urmărit.
- 15 Mai precis, legea încalcă principiul proporționalității, având în vedere (a) domeniul său de aplicare și categoriile de date prevăzute, (b) prelucrarea de date pe care o instituie, (c) scopurile sale și (d) perioada de păstrare a datelor.
- 16 În primul rând, legea atacată definește în mod foarte larg datele colectate, care depășesc în mod vădit ceea ce este strict necesar.

<sup>1</sup> 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), JO 2016, L 119, p. 1 (denumit de asemenea în continuare „RGPD”).

- 17 Reclamanta constată că se pare – însă legea nu este clară - că pre-screeningul ar trebui efectuat în banca de date centralizată la UIP, cu ajutorul unor criterii prestabilite care să servească drept indicatori cu privire la amenințare. Or, Legea PNR nu definește nici natura precisă a băncilor de date utilizate pentru corelare, nici modalitățile acestora din urmă. Legea PNR nu prevede nici că această corelare este limitată la bazele de date exploatate în legătură cu combaterea terorismului și a infracțiunilor grave.
- 18 Reclamanta critică de asemenea cercetările care vizează informații specifice pe care legea le prevede, fără a preciza datele efectiv accesibile.
- 19 Reclamanta denunță de asemenea scopurile prelucrării datelor, care sunt în mod clar mai largi decât cele care sunt prevăzute de Directiva PNR, precum combaterea imigrației ilegale, a activităților care pot constitui o amenințare pentru interesele fundamentale ale statului sau combaterea „radicalizării violente”, definită numai printr-o circulară.
- 20 În sfârșit, reclamanta critică perioada de păstrare a datelor de cinci ani. Legiuitorul nu a justificat în nici un mod alegerea perioadei maxime autorizate de Directiva PNR, care arată caracterul disproporționat al măsurii.
- 21 Conseil des ministres [Consiliul de Miniștri] (care susține legea) invocă, cu titlu principal, inadmisibilitatea primului motiv, în măsura în care acesta este întemeiat pe încălcarea articolului 23 din RGPD, întrucât reiese în mod clar atât din considerentul (19) al RGPD, cât și din articolul 1 din Directiva PNR că prelucrarea datelor „PNR” nu intră sub incidența RGPD, ci sub incidența cooperării judiciare și polițienești dintre statele membre și a Directivei (UE) 2016/680<sup>2</sup>.
- 22 Pe de altă parte, acesta susține că principiul legalității nu este încălcat, întrucât legea cuprinde elementele esențiale ale măsurilor pe care le prevede, iar abilitarea regelui este suficient de precisă. În rest, cerința legalității este înțeleasă în sens material potrivit Curții Europene a Drepturilor Omului, astfel încât normele administrative intră sub incidența noțiunii de „lege” în sensul Convenției europene a drepturilor omului.

Legea PNR urmărește să asigure siguranța publică, permițând nu numai urmărirea penală a infracțiunilor de terorism sau a anumitor infracțiuni grave, ci și, printr-o analiză prealabilă a datelor colectate, prevenirea acestor infracțiuni. Curtea de Justiție a recunoscut că aceste obiective sunt legitime în sensul articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, atât în

<sup>2</sup> 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 (JO 2016, L 119, p. 89) (denumită în continuare „Directiva 2016/680”).

Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții (C-293/12 și C-594/12, EU:C:2014:238), cât și în Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592.

- 23 Consiliul de Miniștri apreciază că măsurile atacate sunt proporționale.
- 24 În ceea ce privește crearea unei „bănci de date privind pasagerii”, Consiliul de Miniștri arată că reclamanta se limitează la a afirma, fără a demonstra, că o corelare a datelor ar fi permis realizarea obiectivului urmărit și ar fi fost mai puțin intruzivă în ceea ce privește dreptul la respectarea vieții private. Acesta adaugă că o simplă corelare nu ar fi suficientă pentru realizarea evaluărilor prealabile în vederea identificării riscurilor pentru siguranță. Crearea unei baze de date ar permite, de altfel, respectarea considerentului (25) al Directivei PNR, care invită la păstrarea datelor pe perioada necesară ținând seama de obiectivele urmărite.
- 25 În ceea ce privește corelarea între diferitele baze de date, Consiliul de Miniștri amintește că articolele 24 și 25 din Legea PNR transpun articolul 6 din Directiva PNR. Din lucrările pregătitoare reiese, pe de altă parte, că legiuitorul nu intenționează să efectueze o corelare între „banca de date privind pasagerii” și ansamblul băncilor de date la care au acces autoritățile competente, ci numai între „banca de date privind pasagerii” și cele care corespund scopurilor urmărite de legea atacată. Aceste măsuri sunt conforme cu concluziile deduse din Avizul 1/15 al Curții de Justiție, întrucât nici articolul 6 alineatul (3) din Directiva PNR nu precizează nici acesta ce bănci de date pot fi corelate. O putere de apreciere nu este incompatibilă nici cu principiul legalității, astfel cum este interpretat de Curtea Europeană a Drepturilor Omului.
- Obiectivul legii nu ar putea fi atins, pe de altă parte, dacă călătorii ar cunoaște dinainte criteriile care vor conduce la o corespondență pozitivă, întrucât aceștia și-ar putea adapta comportamentul în consecință. Articolul 16 din legea atacată indică, în plus, în mod clar că pre-screeningul trebuie efectuat în cadrul „bazei de date privind pasagerii”, ceea ce este, așadar, în conformitate cu principiul legalității.
- 26 În ceea ce privește perioada de păstrare a datelor, Consiliul de Miniștri apreciază că nu este nerezonabil să se prevadă o perioadă de păstrare de cinci ani, care corespunde, de altfel, perioadei minime de prescripție a acțiunii publice în ceea ce privește infracțiunile de competența instanțelor corecționale.
- Perioada de păstrare a acestor date, care este conformă cu durata prevăzută de Directiva PNR, nu este, așadar, nicidecum disproporționată.
- 27 Al doilea motiv, invocat cu titlu subsidiar, se întemeiază, în esență, pe nerespectarea dispozițiilor articolului 3 alineatul (2) TFUE coroborat cu articolul 45 din cartă.
- 28 Reclamanta susține că articolul 3 alineatul 1, articolul 8 alineatul 2 și capitolul 11, care cuprinde articolele 28-31, din Legea PNR sunt contrare liberei circulații a

persoanelor, întrucât privesc nu numai transporturile extra-UE, ci și transporturile intra-UE (inclusiv escalele). Reclamanta apreciază, cu alte cuvinte, că, prin extinderea sistemului „PNR” la zborurile intra-UE, dispozițiile atacate restabilesc indirect controalele la frontiere, care ar fi contrare liberei circulații a persoanelor.

- 29 Consiliul de Miniștri apreciază că legea atacată nu reinstituie niciun control la frontiere și că nu contravine în nici un mod liberei circulații a persoanelor. Directiva PNR nu se aplică imigrației ilegale, iar legea atacată nu transpune numai Directiva PNR, ci și Directiva API.

Motivul, astfel cum este formulat, privește numai articolul 3 alineatul 1, articolul 8 alineatul 2, precum și capitolul 11 din legea atacată. Or, din definiția noțiunii de „frontiere externe” reiese că Legea PNR privește numai controalele extra-UE. În plus, Legea PNR transpune Directiva 2004/82/CE, astfel încât aceasta nu poate fi interpretată în sensul că reinstituie un control la frontierele spațiului Schengen.

Cu titlu infinit subsidiar, considerentul (10) al Directivei PNR enunță în mod expres posibilitatea de a extinde utilizarea datelor „PNR” la zborurile intra-UE, ceea ce demonstrează că această măsură nu este în sine contrară liberei circulații și nici Regulamentului (CE) nr. 562/2006.

## **II. Cadrul juridic**

### ***Convenția europeană a drepturilor omului***

- 30 Articolul 8 prevede:

„1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale.

2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei ori protejarea drepturilor și libertăților altora.”

### ***Dreptul Uniunii***

#### ***Carta drepturilor fundamentale a Uniunii Europene;***

- 31 Articolul 7 din cartă („Respectarea vieții private și de familie”) prevede:

„Orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor.”



32 Articolul 8 din cartă („Protecția datelor cu caracter personal”) prevede:

„(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”.

33 Articolul 52 alineatul (1) din cartă prevede:

„Orice 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.”

*Regulamentul general privind protecția datelor (RGPD)*

34 Articolul 2 alineatul (2) litera (d) prevede:

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

[...]

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

35 Articolul 23 prevede:

„(1) 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:

(a) securitatea națională;

(b) apărarea;

- (c) securitatea publică;
  - (d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
  - (e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;
  - (f) protejarea independenței judiciare și a procedurilor judiciare;
  - (g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
  - (h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(e) și (g);
  - (i) protecția persoanei vizate sau a drepturilor și libertăților altora;
  - (j) punerea în aplicare a pretențiilor de drept civil.
- (2) În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:
- (a) scopurile prelucrării sau ale categoriilor de prelucrare;
  - (b) categoriile de date cu caracter personal;
  - (c) domeniul de aplicare al restricțiilor introduse;
  - (d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal;
  - (e) menționarea operatorului sau a categoriilor de operatori;
  - (f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;
  - (g) riscurile pentru drepturile și libertăților persoanelor vizate și
  - (h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției”.

#### *Directiva PNR*

36 Articolul 3 are următorul cuprins:



„În sensul prezentei directive, se aplică următoarele definiții:

[...]

4. «pasager» înseamnă orice persoană, inclusiv persoanele aflate în transfer sau în tranzit și excluzând membrii echipajului, transportată sau care urmează să fie transportată într-o aeronavă cu consimțământul transportatorului aerian, acest consimțământ fiind exprimat prin înregistrarea persoanei respective pe lista pasagerilor”.

37 Articolul 4 prevede:

„Unitatea de informații despre pasageri

(1) Fiecare 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).

(2) UIP este responsabilă de:

(a) colectarea datelor din PNR de la transportatorii aerieni, stocarea și prelucrarea acestor date și transferul datelor respective sau al rezultatului prelucrării acestora autorităților competente menționate la articolul 7;

(b) schimbul de date din PNR, precum și de schimbul de rezultate ale prelucrării acestora cu UIP din alte state membre și cu Europol, în conformitate cu articolele 9 și 10.

[...]”.

38 Articolul 6 prevede:

„(1) Datele din PNR transferate de către transportatorii aerieni sunt colectate de către UIP a statului membru relevant, astfel cum este prevăzut la articolul 8. În 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.

(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;

(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.

[...]”.

39 Articolul 12 prevede:

„(1) Statele membre se asigură că datele din PNR furnizate de transportatorii aerieni UIP 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 sosește sau de pe teritoriul căruia pleacă zborul.

(2) La expirarea unei perioade de șase luni de la transferul datelor din PNR, menționat la alineatul (1), toate datele din PNR se depersonalizează prin mascarea următoarelor elemente de date care ar putea servi la identificarea directă a pasagerului la care se referă datele din PNR:

(a) numele, inclusiv numele altor pasageri din PNR precum și numărul călătorilor din PNR care călătoresc împreună;

(b) adresa și informațiile de contact;

(c) toate informațiile privind plata, inclusiv adresa de facturare, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a pasagerului la care se referă PNR sau a oricăror altor persoane;

(d) informațiile din profilul «client fidel» («frequent flyer»);

(e) mențiuni cu caracter general, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a pasagerului la care se referă PNR, și

(f) orice date API care au fost colectate.

(3) După expirarea perioadei de șase luni menționată la alineatul (2), dezvăluirea datelor complete din PNR este permisă numai dacă:

(a) se consideră în mod rezonabil că este necesară în scopul menționat la articolul 6 alineatul (2) litera (b) și

(b) este aprobată de către:

(i) o autoritate judiciară sau

(ii) 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.

(4) Statele membre asigură ștergerea definitivă a datelor din PNR după expirarea perioadei menționate la alineatul (1). Această obligație nu aduce atingere cazurilor în care date specifice din PNR au fost transferate unei autorități competente și sunt utilizate în contextul unor cazuri specifice în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave, când păstrarea acestor date de către autoritatea competentă este reglementată de dreptul intern.

(5) Rezultatul prelucrării menționate la articolul 6 alineatul (2) litera (a) este păstrat de UIP numai pentru perioada necesară pentru informarea autorităților competente și, în conformitate cu articolul 9 alineatul (1), informarea UIP ale altor state membre cu privire la un rezultat pozitiv. În cazul în care rezultatul unei prelucrări automatizate s-a dovedit negativ, după o reexaminare individuală prin mijloace neautomatizate astfel cum se menționează la articolul 6 alineatul (5), acesta poate fi, totuși, stocat pentru a se evita viitoare răspunsuri pozitive «false» pe durata în care datele de bază nu sunt șterse în temeiul alineatului (4) din prezentul articol.”

- 40 Anexa I la Directiva PNR, intitulată „Datele din registrul cu numele pasagerilor în măsura în care au fost colectate de transportatorii aerieni”, menționează printre altele:

„[...]”

12. 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)

[...]”

18. 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)

[...]”.

## *Directiva API*

### 41 Articolul 1 prevede:

„Prezenta directivă urmărește să amelioreze controalele la frontiere și să combată imigrația ilegală, prin transmiterea în prealabil, autorităților naționale competente, de către operatorii de transport, a datelor privind pasagerii.”

## ***Dreptul belgian***

### 42 Dispozițiile relevante ale **Legii PNR** (astfel cum a fost modificată prin Legile din 15 și din 30 iulie 2018 și prin Legea din 2 mai 2019) sunt următoarele:

#### „CAPITOLUL 2. Domeniul de aplicare

Articolul 3. § 1. Prezenta lege stabilește obligațiile transportatorilor și ale operatorilor de turism referitoare la transmiterea datelor pasagerilor care călătoresc spre, pleacă de pe sau tranzitează teritoriul național.

§ 2. Regele stabilește prin decret adoptat în Consiliul de Miniștri, pe sectoare de transport și pentru operatorii de transport, datele pasagerilor care trebuie transmise și modalitățile de transmitere a acestora, după obținerea unui aviz din partea autorității competente de control al prelucrării datelor cu caracter personal. [...]

#### CAPITOLUL 3. Definiții

Articolul 4. În scopul aplicării prezentei legi și a decretelor sale de punere în aplicare:

[...]

9° «PNR» înseamnă registrul cerințelor de călătorie ale fiecărui pasager, care conține informațiile prevăzute la articolul 9, necesare pentru a permite prelucrarea și controlul rezervărilor de către transportatorii și operatorii de turism care efectuează rezervările, 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, utilizate pentru verificarea pasagerilor la îmbarcarea în avion, sau în sisteme echivalente care oferă aceleași funcționalități;

10° «pasager» înseamnă orice persoană, inclusiv persoanele aflate în transfer sau în tranzit și excluzând membrii echipajului, transportată sau care urmează să fie transportată de către transportator cu consimțământul acestuia, acest consimțământ fiind exprimat prin înregistrarea persoanei respective pe lista pasagerilor;

[...]

#### CAPITOLUL 5. Scopurile în care sunt prelucrate datele

Articolul 8. § 1. Datele pasagerilor sunt prelucrate în scopul:

1° cercetării și urmăririi penale, inclusiv executarea pedepselor sau a măsurilor limitative de libertate, referitoare la infracțiunile prevăzute [în] Codul de procedură penală;

2° cercetării și urmăririi penale, inclusiv executarea pedepselor sau a măsurilor limitative de libertate, referitoare la infracțiunile prevăzute [în] Codul penal;

3° prevenirii tulburărilor grave ale siguranței publice în cadrul radicalizării violente prin monitorizarea fenomenelor și a grupărilor 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;

5° cercetării și urmăririi penale a infracțiunilor prevăzute [în diferite legi].

§ 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.

## CAPITOLUL 6. – Datele pasagerilor

Articolul 9. § 1. În ceea ce privește datele de rezervare, datele pasagerilor cuprind cel mult:

1° codul de reper al PNR;

2° data rezervării și a emiterii biletului;

3° datele prevăzute ale călătoriei;

4° numele, prenumele și data nașterii;

5° adresa și informațiile de contact (numărul de telefon, adresa de e-mail);

6° informațiile privind forma de plată, inclusiv adresa de facturare;

7° itinerarul complet de călătorie pentru pasagerul respectiv;

8° informațiile referitoare la «pasagerii înregistrați», și anume pasagerii cu profilul «client fidel»;

9° agenția sau agentul de turism;

10° situația 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;

11° informațiile scindate/divizate din PNR;

12° mențiunile 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;

13° informațiile despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu, câmpurile aferente prețului biletelor furnizate automat;

14° numărul locului și alte informații privind locul;

15° informațiile cu privire la codurile partajate;

16° toate informațiile cu privire la bagaje;

17° numărul și numele celorlalți pasageri care figurează în PNR;

18° toate datele prealabile privind pasagerii (date API) care au fost colectate, enumerate la alineatul 2;

19° istoricul tuturor modificărilor datelor enumerate la punctele 1-18;

§ 2. În ceea ce privește datele de înregistrare și de îmbarcare, datele prealabile prevăzute la alineatul 1 punctul 18 sunt:

1 ° tipul documentului de călătorie;

2° numărul documentului;

3° cetățenia;

4° țara de emisie a documentului;

5° data de expirare a documentului;

6° numele de familie, prenumele, sexul, data nașterii;

7° transportatorul/operatorul de transport;

8° numărul transportului;

9° data plecării și data sosirii;

10° locul de plecare și locul de sosire;

11° ora plecării și ora sosirii;

12° numărul total de persoane transportate;

13° numărul locului;

14° codul de reper al PNR;

15° numărul, greutatea și datele de identificare a bagajelor;

16° punctul de trecere a frontierei utilizat pentru a intra pe teritoriul național.

[...]

## CAPITOLUL 7. Unitatea de informații despre pasageri

Articolul 12. Este instituită, în cadrul Serviciului Public Federal de Afaceri Interne, o Unitate de informații despre pasageri.

Articolul 13. § 1. UIP este responsabilă de:

1° colectarea, stocarea și prelucrarea datelor pasagerilor transmise de transportatori și de operatorii de turism, precum și de administrarea băncii de date privind pasagerii;

2° schimbul de date privind pasagerii, precum și de schimbul de rezultate ale prelucrării acestora cu UIP din alte state membre ale Uniunii Europene, cu Europol și cu țările terțe, în conformitate cu capitolul 12.

§ 2. Fără a aduce atingere altor dispoziții legale, UIP nu poate utiliza datele stocate în temeiul capitolului 9 în alte scopuri decât cele prevăzute la articolul 8.

Articolul 14. § 1. UIP este formată din:

1° un funcționar [...] responsabil de:

- a) organizarea și funcționarea UIP;
- b) controlul respectării de către transportatori și operatorii de turism a obligațiilor lor prevăzute în capitolul 4;
- c) administrarea și exploatarea băncii de date privind pasagerii;
- d) prelucrarea datelor privind pasagerii;
- e) respectarea legalității și a regularității prelucrărilor prevăzute în capitolul 10;

[...].



2° membri detașați din serviciile [...] următoare:

- a) serviciile de poliție [...];
- b) Serviciul de siguranță a statului [...];
- c) Serviciul general de informații și de securitate [...];
- d) Administrația [...] vămilor și a accizelor [...]

[...].

## CAPITOLUL 8. Banca de date privind pasagerii

Articolul 15. § 1. Este instituită o bancă de date privind pasagerii administrată de Serviciul Public Federal de Afaceri Interne, în care sunt înregistrate datele pasagerilor.

[...].

§ 4. Prelucrarea datelor pasagerilor efectuată în temeiul prezentei legi este supusă Legii privind protecția datelor. Autoritatea competentă de control al prelucrării datelor cu caracter personal exercită competențele prevăzute de loi sur la protection de la vie privée [Legea privind protecția vieții private]. [...]

[...]

## CAPITOLUL 9. Perioadele de păstrare

Articolul 18. 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.

[...]

## CAPITOLUL 10. Prelucrarea datelor

Secțiunea I. Prelucrarea datelor pasagerilor în cadrul evaluării prealabile a pasagerilor

Articolul 24. § 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 ce persoane trebuie supuse unei examinări mai aprofundate.

[metode de evaluare prealabilă]

Articolul 25. [...]

§ 2. Evaluarea pasagerilor înainte de sosirea, tranzitul sau plecarea lor pe baza unor criterii prestabilite se realizează în mod nediscriminatoriu. Aceste criterii nu pot viza identificarea unei persoane și trebuie să fie personalizate, proporționale și specifice.

§ 3. Aceste criterii nu se întemeiază pe date care dezvăluie rasa sau originea etnică a unei persoane, convingerile sale religioase sau filozofice, opiniile sale politice, apartenența la o organizație sindicală, starea sa de sănătate, viața sexuală sau orientarea sexuală.

[...]

Secțiunea 2. – Prelucrarea datelor în cadrul cercetărilor care vizează informații specifice

Articolul 27. Datele pasagerilor sunt exploatate pentru efectuarea de cercetări care vizează informații specifice în scopurile prevăzute la articolul 8 alineatul 1 punctele 1, 2, 4 și 5 și în condițiile prevăzute la articolul 46 septies din Codul de procedură penală sau la articolul 16/3 din Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate sau la articolul 281 alineatul 4 din Legea generală privind vămile și accizele, consolidată la 18 iulie 1977.

CAPITOLUL 11. Prelucrarea datelor pasagerilor în vederea îmbunătățirii controlului la frontiere și a combaterii imigrației ilegale

Articolul 28. § 1. Prezentul capitol se aplică prelucrării datelor pasagerilor de către serviciile de poliție responsabile de controlul la frontiere și de Oficiul pentru Străini în vederea îmbunătățirii controlului persoanelor la frontierele externe și a combaterii imigrației ilegale.

[...]

Articolul 29. § 1. [...]

§ 2. Sunt transmise numai datele [API] referitoare la următoarele categorii de pasageri:

1° pasagerii care intenționează să intre sau au intrat pe teritoriu pe la frontierele externe ale Belgiei;

2° pasagerii care intenționează să părăsească sau au părăsit teritoriul pe la frontierele externe ale Belgiei;

3° pasagerii care intenționează să treacă prin, se află în sau au trecut printr-o zonă internațională de tranzit situată în Belgia.

§ 3. Datele pasagerilor prevăzute la alineatul 2 sunt transmise serviciilor de poliție prevăzute la articolul 14 alineatul 1 punctul 2 litera a) imediat după înregistrarea

lor în banca de date privind pasagerii. Acestea păstrează datele menționate într-un fișier temporar și le distrug în 24 de ore de la transmitere.

§ 4. [...] datele pasagerilor prevăzute la alineatul 2 sunt transmise Oficiului pentru Străini imediat după înregistrarea lor în banca de date privind pasagerii. Acesta păstrează datele menționate într-un fișier temporar și le distruge în 24 de ore de la transmitere.

[...].

Articolul 31. În 24 de ore de la finalizarea transportului prevăzut la articolul 4 punctele 3-6, transportatorii și operatorii de turism distrug toate datele pasagerilor prevăzute la articolul 9 alineatul 1 punctul 18 [...].

[...]

## CAPITOLUL 15. Dispoziții de modificare

### Secțiunea I. Modificarea Codului de procedură penală

Articolul 50. În Codul de procedură penală se inserează articolul 46septies, care are următorul cuprins:

«Articolul 46septies. În cadrul cercetării infracțiunilor prevăzute la articolul 8 alineatul 1 punctele 1, 2 și 5 din Legea din 25 decembrie 2016 privind prelucrarea datelor pasagerilor, procurorul regelui, printr-o decizie scrisă și motivată, poate însărcina ofițerul de poliție judiciară să solicite UIP să comunice datele pasagerilor în conformitate cu articolul 27 din Legea din 25 decembrie 2016 privind prelucrarea datelor pasagerilor.»

[...]

### Secțiunea 2. Modificarea Legii organice din 30 noiembrie 1998 privind serviciile de informații și de securitate

Articolul 51. În capitolul III secțiunea I subsecțiunea 2 din Legea organică din 30 noiembrie 1998 privind serviciile de informații și de securitate se inserează articolul 16/3, care are următorul cuprins:

«Articolul 16/3. § 1. Serviciile de informații și de securitate pot decide, motivând corespunzător, să acceseze, în interesul exercitării misiunilor lor, datele pasagerilor prevăzute la articolul 27 din Legea din 25 decembrie 2016 privind prelucrarea datelor pasagerilor [...].»

### III. Aprecierea Cour constitutionnelle [Curtea Constituțională]

- 43 Cour constitutionnelle [Curtea Constituțională] precizează de la început că va examina acțiunea ținând seama de modificările Legii din 25 decembrie 2016 aduse prin Legile din 15 și din 30 iulie 2018 și prin Legea din 2 mai 2019.
- 44 Cour constitutionnelle [Curtea Constituțională] reduce, pe de altă parte, întinderea acțiunii în anulare stabilind că primul motiv vizează numai articolul 3 alineatul 2, articolul 4 punctele 9 și 10, articolele 7-9, articolele 12-16, articolul 18, articolele 24-27 și articolele 50 și 51 din lege și că al doilea motiv vizează articolul 3 alineatul 1, articolul 8 alineatul 2 și articolele 28-31 din lege.

#### 1. Cu privire la admisibilitatea primului motiv: articolul 23 din RGPD este aplicabil Legii PNR?

- 45 Instanța de trimitere amintește că protecția conferită de RGPD se întemeiază pe articolul 16 alineatul (2) TFUE și că, în principiu, prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor nu intră în domeniul de aplicare al RGPD, ci al Directivei 2016/680. Această directivă stabilește norme specifice 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, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, cu respectarea naturii speciale a activităților în cauză.
- 46 Legea PNR organizează colectarea și transferul datelor PNR, crearea unei bănci de date privind pasagerii, administrată de UIP, scopurile prelucrării de către banca de date menționată și accesul la aceasta din urmă. Ea transpune în esență Directiva PNR, însă conținutul său depășește transpunerea acestei directive.
- 47 Referindu-se la Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (EU:C:2017:592), instanța de trimitere constată că dispozițiile care organizează colectarea, transferul și prelucrarea datelor „PNR” pot intra atât sub incidența protecției datelor (articolul 16 TFUE), cât și a cooperării polițienești (articolul 87 TFUE).

Aceasta arată de asemenea că considerentul (5) al Directivei PNR precizează că obiectivele acestei directive sunt „*printre altele, asigurarea securității, protejarea vieții și siguranței persoanelor și crearea unui cadru juridic pentru protecția datelor din PNR în ceea ce privește prelucrarea acestora de către autoritățile competente*”. Considerentul (38) al aceleiași directive precizează totuși că obiectivele directivei sunt „*transferul datelor din PNR de către transportatorii aerieni și prelucrarea acestor date în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave*”, ceea ce ar

putea conferi acestor obiective un caracter preponderent față de cel al protecției datelor.

Aceasta constată, pe de altă parte, că dreptul național nu exclude întreaga Lege PNR din domeniul de aplicare al articolului 23 din RGPD.

- 48 Cour constitutionnelle [Curtea Constituțională] concluzionează, prin urmare, că, pentru a stabili dacă cerințele prevăzute la articolul 23 din RGPD se aplică Legii PNR, care transpune, printre altele și în principal, Directiva PNR, trebuie adresată Curții o primă întrebare preliminară.

## **2. *Cu privire la fondul primului motiv***

Cour constitutionnelle [Curtea Constituțională] examinează, în continuare, fondul motivului sub cele șapte aspecte menționate la punctul 8 din prezentul rezumat. Aceasta consideră că primele două obiecții emise împotriva „modalităților de punere în aplicare” și împotriva noțiunilor de „documente de identitate” și „document de călătorie” sunt neîntemeiate. Instanța de trimitere examinează în continuare celelalte cinci obiecții și are îndoieli cu privire la interpretarea care trebuie dată anumitor dispoziții ale Directivei PNR și cu privire la validitatea lor din perspectiva cartei.

### *Cu privire la datele vizate (articolul 4 punctul 9 și articolul 9 din Legea PNR)*

- 49 Reclamanta apreciază că domeniul de aplicare foarte larg referitor la datele pasagerilor prevăzute la articolul 4 punctul 9 și la articolul 9 din Legea PNR este vădit disproporționat în raport cu obiectivul urmărit. În opinia sa, datele vizate ar putea face parte dintre datele sensibile, precum apartenența la o organizație sindicală, afinitățile personale și relațiile personale sau profesionale.
- 50 Instanța de trimitere amintește că o ingerință a puterilor publice în exercitarea dreptului la respectarea vieții private trebuie nu numai să se întemeieze pe o dispoziție legislativă suficient de precisă, ci și să răspundă unei nevoi sociale imperative într-o societate democratică și să fie proporțională cu scopul legitim urmărit. Legiuitorul dispune în acest domeniu de o marjă de apreciere care nu este totuși nelimitată: pentru ca o normă să fie compatibilă cu dreptul la respectarea vieții private, legiuitorul trebuie să fi stabilit un just echilibru între toate drepturile și interesele în cauză.

În Avizul său 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (EU:C:2017:592), Curtea a amintit că o ingerință în dreptul la protecția datelor cu caracter personal trebuie să fie limitată la „strictul necesar” (a se vedea punctele 140 și 141).

- 51 Cour constitutionnelle [Curtea Constituțională] arată că Legea PNR are ca obiectiv să asigure securitatea publică, instituind transferul datelor pasagerilor și utilizarea acestora în cadrul combaterii infracțiunilor de terorism și a infracțiunilor

transnaționale grave. Aceste obiective constituie obiective de interes general care pot justifica ingerințe în dreptul la respectarea vieții private și în dreptul la protecția datelor cu caracter personal (Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctul 42). Curtea de Justiție a confirmat, de altfel, că aceste obiective de interes general pot justifica transferul și prelucrarea datelor din registrul cu numele pasagerilor [Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctele 148 și 149].

- 52 Instanța de trimitere examinează în continuare dacă aceste ingerințe sunt suficient de precise, proporționale și limitate la „strictul necesar”, ținând seama de amploarea datelor prevăzute de Legea PNR.

Colectarea datelor pasagerilor prevăzute de Legea PNR este însoțită de garanții în ceea ce privește conținutul acestor date. Aceste date sunt astfel stabilite în mod exhaustiv la articolul 9 din Legea PNR. Este vorba despre informații legate în mod direct de călătoria care ocazional transportul care intră în domeniul de aplicare al Legii PNR, de care transportatorii și operatorii de turism dispun deja, în principiu. Pe de altă parte, aceste date corespund anexei I la Orientările Organizației Aviației Civile Internaționale (OACI). Acestea sunt, așadar, pertinente în raport cu obiectivele urmărite de Legea PNR.

Pe de altă parte, articolele 10 și 11, neatacate, din Legea PNR prevăd că datele privind pasagerii nu pot privi rasa sau originea etnică a unei persoane, convingerile sale religioase sau filozofice, opiniile sale politice, apartenența la o organizație sindicală, starea sa de sănătate, viața sexuală sau orientarea sexuală. Atunci când datele pasagerilor transferate de transportatori și de operatorii de turism cuprind alte date decât cele enumerate la articolul 9 sau date enumerate la articolul 10, UIP șterge definitiv datele suplimentare de la primirea lor. Aceste dispoziții garantează că datele sensibile nu pot, în principiu, să fie colectate sau păstrate ca „date privind pasagerii”.

- 53 În Avizul 1/15, citat anterior, din 26 iulie 2017, Curtea de Justiție a considerat de asemenea, în ceea ce privește datele sensibile, că *„articolele 7, 8 și 21, precum și articolul 52 alineatul (1) din cartă se opun atât transferului de date sensibile către Canada, cât și stabilirii condițiilor, negociată de Uniune cu această țară terță, privind utilizarea și păstrarea unor astfel de date de către autoritățile acestei țări terțe”* (punctul 167).

Această observație poate fi transpusă în speță. Deși există garanții care însoțesc datele pasagerilor prevăzute de Legea PNR, trebuie totuși ridicată problema dacă aceste garanții sunt suficiente, având în vedere amploarea datelor vizate. Datele prevăzute la articolul 9 alineatul 1 din Legea PNR, care reia datele prevăzute în anexa I la Directiva PNR, includ astfel date foarte largi, pe lângă datele de înregistrare și de îmbarcare, printre altele: itinerariul complet al pasagerului, agenția de turism, numărul locului, toate informațiile referitoare la bagaje, informațiile referitoare la forma de plată, inclusiv adresa de facturare, mențiunile



generale, „inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani”.

În Avizul 1/15 din 26 iulie 2017, citat anterior, Curtea a observat de altfel că, *„chiar dacă anumite date 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, precum cele definite la articolul 2 litera (e) din acordul preconizat”* (punctul 128).

În Avizul din 19 august 2016 privind implicațiile în ceea ce privește protecția datelor din registrul cu numele pasagerilor (denumit în continuare „Avizul din 19 august 2016”), Comitetul consultativ al Convenției nr. 108 a Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumit în continuare „Comitetul consultativ al Convenției nr. 108”) a observat de asemenea că *„PNR conțin informații care urmăresc să faciliteze călătoria unui pasager și pot cuprinde un o serie de date sensibile (date care pot servi la indicarea rasei, a opiniilor politice, a convingerilor religioase și altele, a stării de sănătate sau a orientării sexuale a unei persoane), nu numai sub anumite date «codate», ci și în câmpul deschis care conține observații generale (precum cererile referitoare la regimul alimentar și medicale sau faptul că o asociație politică sau religioasă a beneficiat de bilete la preț redus pentru călătoria membrilor săi), ceea ce ar putea conduce la o discriminare directă”* (Consiliul Europei, Avizul din 19 august 2016, T-PD(2016)18rev, p. 7).

Agencia pentru Drepturi Fundamentale a Uniunii Europene a remarcat de asemenea că datele PNR *„pot cuprinde date sensibile sau speciale sub titlul «mențiuni cu caracter general»”* (Avizul 1/2011 al Agenției pentru Drepturi Fundamentale a Uniunii Europene referitor la Propunerea de directivă privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (COM(2011) 32 final), 14 iunie 2011, p. 8; a se vedea de asemenea *ibid.*, p. 13).

- 54 Având în vedere domeniul lor foarte larg de aplicare, datele prevăzute la articolul 9 din Legea PNR, deși nu pot conține în mod direct date sensibile, ar putea totuși să dezvăluie în mod indirect elemente sensibile care țin de protecția datelor cu caracter personal și de respectarea vieții private. Având în vedere Avizul 1/15 al Curții de Justiție, Cour constitutionnelle [Curtea Constituțională] ridică problema dacă aceste date, care includ datele prevăzute în anexa I la Directiva PNR, nu depășesc „strictul necesar” pentru atingerea obiectivelor urmărite de aceeași directivă. Aceasta decide, prin urmare, să adreseze Curții o a doua întrebare preliminară.



- 55 În Avizul 1/15, citat anterior, din 26 iulie 2017, Curtea a exprimat, de altfel, următoarele observații în ceea ce privește cerința unei definiții clare și precise a datelor prevăzute de Proiectul de acord dintre Canada și Uniunea Europeană privind transferul și prelucrarea datelor din registrul cu numele pasagerilor:

„156. În această privință, deși cele 19 rubrici privind datele PNR care figurează în anexa la acordul preconizat corespund, potrivit observațiilor Comisiei, cu anexa I din Orientările Organizației Aviației Civile Internaționale (OACI) privind datele PNR, trebuie subliniat însă, astfel cum a arătat avocatul general la punctul 217 din concluzii, că rubrica 5, referitoare la «informații disponibile privind programele de fidelitate și avantajele oferite (de exemplu, bilete gratuite, transferul la o clasă superioară etc.)», și rubrica 7, care acoperă «toate informațiile disponibile privind datele de contact (inclusiv cele referitoare la sursa informației)», nu definesc suficient de clar și de precis datele PNR care trebuie transferate.

157. Astfel, în ceea ce privește rubrica 5, folosirea termenului «etc.» nu stabilește în mod suficient întinderea datelor care trebuie transferate. În plus, formularea acestei rubrici nu permite să se cunoască dacă ea vizează informații care privesc numai statutul pasagerilor aerieni în programele de fidelitate sau dacă, dimpotrivă, vizează toate informațiile privind călătorii aerieni și tranzacțiile efectuate în cadrul unor astfel de programe.

158. Similar, rubrica 7, folosind expresia «toate informațiile disponibile privind datele de contact», nu stabilește în mod suficient întinderea datelor care trebuie transferate. În special, ea nu precizează care este tipul de date de contact pe care le vizează și nici dacă aceste date de contact acoperă de asemenea, astfel cum se poate deduce din răspunsul scris al Comisiei la întrebările adresate de Curte, datele de contact ale terților care au efectuat rezervarea zborului pentru pasagerul aerian, ale terților prin intermediul cărora pasagerul aerian poate fi contactat sau ale terților care trebuie informați în caz de urgență.

159. În ceea ce privește rubrica 8, aceasta privește «toate informațiile disponibile privind plata/facturarea biletului (fără a include alte detalii ale tranzacției, referitoare la cartea de credit sau la contul bancar, care nu au legătură cu tranzacția efectuată în vederea călătoriei)». Desigur, această rubrică ar putea părea deosebit de largă întrucât folosește expresia «toate informațiile disponibile». Cu toate acestea, după cum rezultă din răspunsul Comisiei la întrebările adresate de Curte, trebuie să se considere că respectiva rubrică 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. Dacă este interpretată în acest sens, se poate considera, așadar, că aceeași rubrică îndeplinește cerințele de claritate și de precizie.

160. În ceea ce privește rubrica 17, aceasta vizează «observații generale, inclusiv alte informații suplimentare (Other Supplementary Information – OSI), informații privind serviciile speciale (Special Service Information – SSI) și informații privind

cereri ale serviciilor speciale (Special Service Request – SSR)». Potrivit explicațiilor date în special de Comisie, această rubrică constituie o rubrică denumită «text liber» (free text), care poate include «toate informațiile suplimentare», în plus față de cele enumerate de altfel în anexa la acordul preconizat. Astfel, o asemenea rubrică 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 PNR. În plus, din moment ce informațiile vizate în respectiva rubrică nu sunt furnizate decât cu titlu exemplificativ, 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. În aceste condiții, nu se poate considera că rubrica 17 este delimitată cu suficientă claritate și precizie.

161. În ceea ce privește, în sfârșit, rubrica 18, aceasta privește «orice informații prelabile referitoare la pasageri (Advance Passenger Information – API) colectate în scopul rezervării». Potrivit precizărilor făcute de Consiliu și de Comisie, aceste informații corespund informațiilor vizate la articolul 3 alineatul (2) din Directiva 2004/82, și anume 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, precum și punctul inițial de îmbarcare. Se poate considera că această rubrică, în măsura în care este interpretată în sensul că acoperă doar informațiile expres vizate la această din urmă dispoziție, îndeplinește cerințele de claritate și de precizie.

162. Dispozițiile articolului 4 alineatul (3) din acordul preconizat, care prevăd obligația Canadei de a șterge orice date PNR care i-au fost transferate în cazul în care ele nu sunt prevăzute în lista din anexa la acest acord, nu permit să se înlătorească impreciziile care afectează rubricile 5, 7 și 17 din această anexă. Astfel, întrucât această listă nu delimitează, ca atare, cu suficientă claritate și precizie datele PNR care trebuie transferate, aceste dispoziții nu sunt de natură să elimine incertitudinea în privința datelor PNR care trebuie să facă obiectul transferului.

163. În aceste condiții, în ceea ce privește datele PNR care trebuie transferate către Canada, rubricile 5, 7 și 17 din anexa la acordul preconizat nu stabilesc suficient de clar și de precis limitele ingerinței în drepturile fundamentale consacrate la articolele 7 și 8 din cartă”.

- 56 Întrucât unele dintre aceste observații ar putea fi transpuse în speță, în ceea ce privește caracterul exemplificativ și neexhaustiv al anumitor date cuprinse în anexa I la Directiva PNR, pe care articolul 9 din Legea PNR o transpune, instanța de trimitere decide să adreseze o a treia întrebare preliminară.

*Cu privire la noțiunea de „pasager” (articolul 4 punctul 10 din Legea PNR)*

- 57 Reclamanta critică caracterul larg al noțiunii de „pasager”, care conduce la o prelucrare automatizată sistematică, nedirecționată, a datelor tuturor pasagerilor.
- 58 Definiția noțiunii de „pasager” (articolul 4 punctul 10 din Legea PNR) are drept consecință faptul că colectarea, transferul și prelucrarea datelor PNR ale „pasagerilor” constituie obligații generale și nediferențiate, care se aplică oricărei persoane transportate sau care trebuie să fie transportată și înregistrată pe lista pasagerilor. Obligațiile pe care le impune Legea PNR se aplică, astfel, independent de existența unor motive serioase de a crede că persoanele respective au săvârșit o infracțiune sau sunt pe punctul de a săvârși o infracțiune sau au fost condamnate pentru săvârșirea unei infracțiuni.
- 59 În Avizul din 19 august 2016, Comitetul consultativ al Convenției nr. 108 a observat în această privință că *„[p]relucrarea datelor PNR – care are avantajul unic de a permite identificarea persoanelor de interes - este o filtrare generală și neselectivă a tuturor pasagerilor, inclusiv a celor care nu sunt suspectați de săvârșirea vreunei infracțiuni, de către diferite autorități competente, și vizează date colectate inițial în scopuri comerciale de entități private. Având în vedere amploarea atingerii aduse drepturilor la viața privată și la protecția datelor care ar decurge din prelucrarea datelor PNR, trebuie să se stabilească cu claritate că prelucrarea menționată este o măsură necesară într-o societate democratică într-un scop legitim; în plus, trebuie instituite garanții adecvate. Este indispensabil să fie demonstrată în mod expres necesitatea colectării și a exploatării ulterioare a datelor PNR”* (Avizul din 19 august 2016, T-PD(2016)18rev, p. 5).
- 60 În domeniul comunicațiilor electronice, Curtea s-a pronunțat cu privire la o reglementare națională care prevedea o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică, precum și obligația furnizorilor de servicii de comunicații electronice de a păstra aceste date în mod sistematic și continuu, fără nicio excepție (Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții, C-203/15 și C-698/15, EU:C:2016:970).

*Aceasta a considerat că, „deși eficacitatea combaterii infracționalității grave, în special combaterea crimei organizate și a terorismului, poate să depindă în mare măsură de utilizarea tehnicilor moderne de investigație, un astfel de obiectiv de interes general, oricât de fundamental ar fi, nu poate, în sine, să justifice ca o reglementare națională care prevede păstrarea generalizată și nediferențiată a datelor de transfer și a datelor de localizare să fie considerată necesară în scopul acestei combateri”* (punctul 103).

Curtea a statuat, pe de o parte, că o astfel de reglementare are ca efect, pe de o parte, că păstrarea datelor de transfer și a datelor de localizare este regula, în timp ce sistemul instituit de Directiva 2002/58 impune ca această conservare a datelor

să fie excepția și, pe de altă parte, că „o reglementare națională [...] care acoperă în mod generalizat toți abonații și utilizatorii înregistrați și privește toate mijloacele de comunicare electronică, precum și toate datele de transfer, nu prevede nicio diferențiere, limitare sau excepție în funcție de obiectivul urmărit. Aceasta privește în mod global ansamblul persoanelor care utilizează servicii de comunicații electronice, fără ca aceste persoane să se regăsească, fie și în mod indirect, într-o situație susceptibilă să declanșeze începerea urmăririi penale. Ea se aplică, așadar, chiar și acelor persoane în privința cărora nu există niciun indiciu de natură să sugereze că comportamentul lor poate avea o legătură, chiar indirectă sau îndepărtată, cu infracțiuni grave. În plus, aceasta nu prevede nicio excepție, astfel încât ea se aplică chiar și acelor persoane ale căror comunicații sunt supuse, potrivit normelor dreptului național, secretului profesional (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctele 57 și 58).

106. O astfel de reglementare nu impune nicio relație între datele a căror păstrare este prevăzută și o amenințare pentru securitatea publică. În special, aceasta nu este limitată la o păstrare care privește fie datele aferente unei perioade și/sau unei zone geografice și/sau unui cerc de persoane care pot fi implicate într-un fel sau altul într-o infracțiune gravă, fie persoane care, din alte motive, ar putea să contribuie, prin păstrarea datelor lor, la combaterea infracționalității (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 59).

107. O reglementare națională precum cea în discuție în litigiul principal depășește, așadar, limitele strictului necesar și nu poate fi considerată justificată, într-o societate democratică, astfel cum se prevede la articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă.

108. În schimb, articolul 15 alineatul (1) din Directiva 2002/58, interpretat în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, nu se opune ca un stat membru să adopte o reglementare care să permită, cu titlu preventiv, păstrarea direcționată a datelor de transfer și a datelor de localizare, în scopul combaterii infracționalității grave, cu condiția ca păstrarea datelor să fie, în ceea ce privește categoriile de date care trebuie păstrate, mijloacele de comunicare vizate, persoanele în cauză, precum și durata de păstrare reținută, limitată la strictul necesar.

109. Pentru a îndeplini cerințele menționate la punctul anterior din prezenta hotărâre, această reglementare națională trebuie, în primul rând, să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei astfel de măsuri de păstrare a datelor și să impună un minim de cerințe, astfel încât persoanele ale căror date au fost păstrate să dispună de garanții suficiente care să le permită să protejeze în mod eficient datele lor cu caracter personal împotriva riscurilor de abuz. Aceasta trebuie în special să indice în ce împrejurări și în ce condiții poate fi luată, cu titlu preventiv, o măsură de păstrare a datelor,



garantând astfel că o asemenea măsură este limitată la strictul necesar (a se vedea prin analogie, în ceea ce privește Directiva 2006/24, Hotărârea Digital Rights, punctul 54 și jurisprudența citată).

110. În al doilea rând, în ceea ce privește condițiile materiale pe care trebuie să le îndeplinească reglementarea națională care permite, în cadrul combaterii infracționalității, păstrarea cu titlu preventiv a datelor de transfer și a datelor de localizare, pentru a garanta că aceasta este limitată la strictul necesar, trebuie să se arate că, deși aceste condiții pot varia în funcție de măsurile adoptate pentru prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor grave, păstrarea datelor trebuie să răspundă întotdeauna unor criterii obiective, care să stabilească un raport între datele care trebuie păstrate și obiectivul urmărit. În special, astfel de condiții trebuie să se dovedească, în practică, de natură să delimiteze în mod efectiv amploarea măsurii și, în consecință, publicul în cauză.

111. Referitor la delimitarea unei asemenea măsuri în ceea ce privește publicul și situațiile potențial vizate, reglementarea națională trebuie să se întemeieze pe elemente obiective care să permită să fie vizat un public ale cărui date pot prezenta o legătură, cel puțin indirectă, cu acte de infracționalitate gravă, să contribuie într-un mod sau altul la combaterea infracționalității grave sau să prevină un risc grav pentru securitatea publică. O astfel de delimitare poate fi asigurată prin intermediul unui criteriu geografic în cazul în care autoritățile naționale competente consideră pe baza unor elemente obiective că există, într-una sau în mai multe zone geografice, un risc ridicat privind pregătirea sau comiterea unor asemenea acte.

112. Având în vedere toate considerațiile care precedă, trebuie să se răspundă la prima întrebare în cauza C-203/15 că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică”.

La cea de a doua întrebare preliminară în cauza C-203/15 și la prima întrebare preliminară în cauza C-698/15, Curtea răspunde că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat „în sensul că se opune unei reglementări naționale care guvernează protecția și securitatea datelor de transfer și a datelor de localizare și în special accesul autorităților naționale competente la datele păstrate, fără a limita acest acces, în cadrul combaterii infracționalității, numai la combaterea infracționalității grave, fără a supune respectivul acces unui control prealabil din partea unei instanțe sau a unei autorități administrative independente și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii” (punctul 125).

- 61 La rândul său, Curtea Europeană a Drepturilor Omului s-a pronunțat între timp cu privire la legislația suedeză referitoare la interceptarea masivă a comunicațiilor electronice în conformitate cu articolul 8 din Convenția europeană a drepturilor omului, în Hotărârea *Centrum for Rättvisa* împotriva Suediei din 19 iunie 2018. În special, aceasta a indicat următoarele:

*„Curtea a recunoscut în mod expres că autoritățile naționale dispun de o amplă marjă de apreciere pentru a alege mijloacele de apărare a securității naționale [...]. În cauzele Weber și Saravia și Liberty și alții, Curtea a admis că regimurile de interceptare masivă nu depășesc în sine această marjă de apreciere. Având în vedere motivarea Curții în aceste decizii și ținând seama de amenințările cu care se confruntă numeroase state contractante (dintre care flagelul terorismului internațional și alte infracțiuni grave, precum traficul de stupefiante, traficul de ființe umane, exploatarea sexuală a copiilor și criminalitatea informatică), de progresele tehnologice care le permit teroriștilor și infractorilor să se sustragă mai ușor detectării pe internet și de imposibilitatea de a prevedea căile pe care vor fi transmise comunicațiile electronice, Curtea consideră că decizia de a recurge la un regim de interceptare masivă pentru a repera amenințări necunoscute până atunci de securitatea națională ține de marja de apreciere a statelor” (Curtea Europeană a Drepturilor Omului, 19 iunie 2018, *Centrum for Rättvisa* împotriva Suediei, § 112).*

Aceeași instanță a statuat, în schimb, că legislația engleză privind interceptarea comunicațiilor încalcă articolul 8 din CEDO, deoarece nu respecta criteriile enunțate în jurisprudența sa. Aceasta a considerat de asemenea că *„funcționarea regimurilor de interceptare în masă ține în principiu de marja de apreciere a statului. Interceptarea în masă este prin definiție nedirecționată și a o condiționa de prezența unei «suspiciuni rezonabile» ar face imposibilă punerea sa în aplicare”* (Curtea Europeană a Drepturilor Omului, 13 septembrie 2018, *Big Brother Watch și alții* împotriva Regatului Unit, §317).

- 62 Se ridică problema măsurii în care jurisprudența citată anterior, care privește păstrarea generalizată și nediferențiată a datelor în materie de comunicații electronice, poate fi transpusă în ceea ce privește colectarea, transferul și prelucrarea generalizate și nediferențiate ale datelor pasagerilor, astfel cum sunt organizate de Legea din 25 decembrie 2016.
- 63 În Avizul 1/15, citat anterior, din 26 iulie 2017, Curtea s-a pronunțat cu privire la un sistem PNR analog, însă cu un domeniu de aplicare mai limitat, întrucât proiectul de acord dintre Canada și Uniunea Europeană privind transferul și prelucrarea datelor din registrul cu numele pasagerilor prevedea *„transferul sistematic și continuu al datelor PNR ale tuturor pasagerilor aerieni care efectuează zboruri între Uniune și Canada”* (punctul 127). Aceasta a considerat că *„transferul datelor PNR către Canada și prelucrările lor ulterioare sunt apte să garanteze realizarea obiectivului privind protecția securității și a siguranței publice urmărit de acordul preconizat”* (punctul 153).

În ceea ce privește pasagerii vizați, Curtea a considerat:

„186. Acordul preconizat acoperă datele PNR ale tuturor pasagerilor care efectuează zboruri între Uniune și Canada. Transferul acestor date spre Canada are loc independent de orice element obiectiv care permite să se considere că pasagerii pot să prezinte un risc pentru securitatea publică în Canada.

187. În această privință trebuie arătat că, după cum s-a amintit la punctele 152 și 169 din prezentul aviz, datele PNR sunt destinate în special să fie supuse unei prelucrări automate. Or, după cum au susținut mai mulți intervenienți, această prelucrare vizează identificarea riscului pentru securitatea publică pe care l-ar putea eventual prezenta persoane care, la acest stadiu, nu sunt cunoscute de serviciile competente și care ar putea fi supuse unei examinări amănunțite din cauza acestui risc. În această privință, prelucrarea automată a acestor date, anterior sosirii pasagerilor în Canada, facilitează și accelerează controalele de securitate, în special la frontieră. În plus, 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.

188. De altfel, conform articolului 13 din Convenția de la Chicago, la care s-au referit în special Consiliul și Comisia în răspunsurile lor la întrebările adresate de Curte, toți pasagerii aerieni trebuie să respecte, la intrare, la ieșire, precum și în limitele teritoriului unui stat contractant, legile și regulamentele acestui stat contractant privind intrarea sau ieșirea pasagerilor aerieni de pe teritoriul său. Toți pasagerii aerieni care doresc să intre în Canada sau să iasă din această țară sunt supuși, așadar, în temeiul acestui articol, la controale la frontieră și sunt obligați să respecte condițiile de intrare și de ieșire prevăzute de legislația canadiană în vigoare. În plus, astfel cum reiese din cuprinsul punctelor 152 și 187 din prezentul aviz, identificarea, prin intermediul datelor PNR, a pasagerilor care pot prezenta un risc pentru securitatea publică face parte din controalele la frontieră. În consecință, din moment ce fac obiectul acestor controale, pasagerii aerieni care intenționează să facă uz de dreptul de intrare și de ședere în Canada sunt supuși, prin însăși natura acestei măsuri, verificării datelor lor PNR.

189. În aceste condiții, nu rezultă că acordul preconizat depășește limitele strictului necesar în măsura în care permite transferul datelor PNR ale tuturor pasagerilor aerieni către Canada”.

- 64 Cour constitutionnelle [Curtea Constituțională] ridică problema dacă aceste considerații ar putea fi transpuse în privința Directivei PNR și a unei legislații naționale precum Legea PNR, care, transpunând Directiva PNR, instituie colectarea, transferul și utilizarea generalizate și nediferențiate ale datelor „PNR” pentru toți pasagerii care utilizează transportul aerian, feroviar sau cu autobuzul, independent de o trecere a frontierelor externe ale Uniunii. Acest sistem se aplică



astfel unor persoane în privința cărora nu există niciun indiciu de natură să sugereze că comportamentul lor poate avea o legătură, chiar indirectă sau îndepărtată, cu infracțiuni grave și este mai larg decât sistemul prevăzut de Acordul „PNR” cu Canada. Având în vedere amploarea datelor vizate, se ridică întrebarea dacă această măsură respectă limitele „strictului necesar”. Înainte de a se pronunța cu privire la fond, aceasta decide așadar să adreseze Curții o a patra întrebare preliminară.

*Cu privire la scopurile prelucrării datelor „PNR” (articolul 8 din Legea PNR)*

- 65 Reclamanta critică definiția scopurilor prelucrării datelor „PNR”, care figurează la articolul 8 din Legea PNR, care ar fi mult mai largă decât „scopurile specifice”, care sunt limitate doar la infracțiunile de terorism și la infracțiunile grave prevăzute de Directiva PNR. Aceasta apreciază că scopurile respective depășesc limitele „strictului necesar”.

Scopurile prelucrării datelor „PNR”, astfel cum sunt prevăzute la articolul 1 alineatul (2) și la articolul 6 alineatul (2) din Directiva PNR, constituie numai obiective privind prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave [a se vedea de asemenea considerentul (7) al Directivei PNR].

Unele dintre scopurile prelucrării prevăzute la articolul 8 din Legea PNR corespund infracțiunilor prevăzute în anexa II la Directiva PNR, în conformitate cu obiectivele privind prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave prevăzute de directiva menționată. În schimb, alte scopuri ale prelucrării datelor „PNR” se adaugă celor prevăzute de această directivă. Aceasta este situația, printre altele, în cazul „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” (articolul 8 alineatul 1 punctul 4).

Instanța de trimitere examinează dacă aceste alte scopuri sunt exprimate prin norme clare, precise și limitate la strictul necesar și are îndoieli în ceea ce privește scopul prevăzut la articolul 8 alineatul 1 punctul 4 din Legea PNR.

Expunerea motivelor Legii PNR arată că acest „scop are legătură cu competențele serviciilor de informații, și anume Siguranța statului și Serviciul general de informații și de securitate (SGRS). Pentru a-și îndeplini misiunile de cercetare, de analiză și de prelucrare a informațiilor referitoare la activitățile care pot amenința interesele fundamentale ale statului, aceste servicii trebuie să fie în măsură să analizeze datele pasagerilor pentru a detecta cât mai curând posibil amenințări concrete, pentru a monitoriza deplasările unor persoane determinate sau pentru a efectua analize ale unor fenomene sau ale unor tendințe mai largi. Misiunile privind cercetarea, analiza și prelucrarea informațiilor referitoare la activitățile serviciilor de informații străine pe teritoriul belgian intră în acest scop.” (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 19 și 20).

Deși misiunile serviciilor de informații și de securitate contribuie, în mod general, la securitatea națională și internațională, prelucrarea datelor „PNR” în lumina scopului prevăzut la articolul 8 alineatul 1 punctul 4 din Legea PNR pare foarte vagă și generală.

Acest scop face în plus obiectul, în ceea ce privește evaluarea prealabilă a pasagerilor, al aceluiași tratament precum scopurile prevăzute la articolul 8 alineatul 1 punctele 1, 2 și 5 din Legea PNR [articolul 24 alineatul (2) și articolul 26 alineatul (2)].

În acest context, Cour constitutionnelle [Curtea Constituțională] decide să adreseze Curții o a cincea întrebare preliminară pentru a statua dacă acest scop este suficient de clar, precis și limitat la strictul necesar.

*Cu privire la administrarea băncii de date privind pasagerii și la prelucrarea datelor în cadrul evaluării prealabile a pasagerilor și al cercetărilor care vizează informații specifice (articolele 16, 24-27, 50 și 51 Legea PNR)*

66 Reclamanta apreciază că diferitele prelucrări și fluxuri de date cu caracter personal sunt vădit disproportionale.

67 Articolul 16 din Legea PNR prevede că, în cadrul scopurilor prevăzute la articolul 8 alineatul (1), datele pasagerilor fac obiectul prelucrărilor prevăzute la articolele 24-27.

– *Evaluarea prealabilă a pasagerilor (articolele 24-26)*

68 Datele pasagerilor sunt prelucrate în vederea realizării unei evaluări prealabile (pre-screening) a pasagerilor înainte de sosirea, plecarea sau tranzitul lor prevăzut pe teritoriul național, pentru a determina persoanele care trebuie supuse unei examinări mai aprofundate. „Este vorba despre evaluarea amenințării potențiale și despre determinarea pasagerilor care prezintă un interes pentru exercitarea misiunilor lor sau, de exemplu, necesită luarea unei măsuri (executarea unui mandat de arestare, percheziție etc.)”. (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 28).

Evaluarea prealabilă se întemeiază pe două axe: pe de o parte, corelarea datelor pasagerilor cu băncile de date și, pe de altă parte, corelarea datelor cu criterii prestabilite.

69 În ceea ce privește corelarea cu băncile de date, lucrările pregătitoare ale Legii PNR arată că „[p]rima axă constă în căutarea unor corespondențe pozitive prin intermediul corelării datelor pasagerilor cu datele prelucrate în băncile de date administrate de serviciile competente. Aceasta permite de exemplu să se evalueze dacă o persoană prezintă un grad ridicat de pericol, întrucât este cunoscută într-o bancă de date a poliției în cadrul unui dosar de terorism și din analiza datelor de pasager reiese că aceasta călătorește în mod regulat în țări în care există baze de

antrenament pentru teroriști sau în țări de tranzit către astfel de locuri. Poate fi vorba de asemenea, de exemplu, de o persoană cu privire la care informații disponibile la serviciile de informații arată că aceasta ar pregăti o luare de ostatici, iar aceasta călătorește, potrivit datelor de transport, într-o țară în care serviciile de informații știu, pe baza informațiilor primite, că această persoană ar putea recruta pentru a-și pune planurile în aplicare. În plus, cu cât corespondențele pozitive descoperite de mai multe servicii sunt mai numeroase pentru aceeași persoană, cu atât este mai mare probabilitatea de amenințare.

Corespondența pozitivă poate impune de asemenea luarea unei măsuri la ordinul autorităților judiciare, precum executarea unui mandat de arestare a unei persoane care se pregătește să părăsească Belgia.

Corespondența pozitivă poate reieși de asemenea dintr-o corelare cu bănci de date internaționale precum SIS II, Interpol (SLTD).

Evident, obiectivul nu este de a lega toate băncile de date ale serviciilor cu banca de date privind pasagerii, ci de a limita tehnic corelările cu băncile de date în legătură directă cu scopuri precum cele stabilite de lege.

[...]

Această corelare va putea fi făcută de asemenea prin liste de persoane elaborate în mod specific de serviciile competente în acest scop. În conformitate cu Legea privind protecția vieții private și, mai specific, cu articolul 4 alineatul 1 punctul 4 din aceasta, aceste liste vor trebui actualizate în mod regulat” (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 28 și 29).

- 70 În ceea ce privește corelarea cu criterii prestabilite, lucrările pregătitoare ale Legii PNR arată:

„A doua axă constă în căutarea unor corespondențe pozitive prin intermediul unor criterii prestabilite de UIP (unul sau mai multe) aplicate datelor privind pasagerii. Aceste criterii sunt compuse dintr-unul sau mai mulți indicatori obiectivi pe baza cărora se poate deduce că persoanele care fac obiectul acestora prezintă un comportament cu risc specific care poate constitui o amenințare în raport cu scopurile articolului 8 alineatul 1 punctele 1, 4 și 5 din lege.

Aceste criterii pot integra, de exemplu, anumite comportamente specifice în materie de rezervare sau de călătorii.

Utilizarea lor prezintă avantajul de a putea face vizibile profiluri ale unor pasageri cu risc care nu sunt în mod necesar cunoscuți sau menționați în băncile de date ale serviciilor.

Aceste criterii pot privi, de exemplu, o țară de destinație sau de plecare coroborată cu anumite informații cu privire la călătorie, precum modul de plată și data rezervării” (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 29 și 30).

„Evaluarea prealabilă realizată în cadrul scopului referitor la monitorizarea fenomenelor de poliție administrativă și a grupărilor legat de radicalizarea violentă este supusă unor condiții mult mai restrictive decât celelalte scopuri [...].

Pentru evaluarea prealabilă realizată în cadrul celorlalte scopuri este autorizat accesul la toate datele pasagerilor enumerate la articolul 9” (*ibid.*, p. 31).

„Corespondența pozitivă trebuie să fie în toate cazurile validată de UIP. Astfel, pentru a asigura respectarea totală a dreptului la protecția datelor personale [...] nicio decizie cu consecințe juridice pentru o persoană sau care o poate prejudicia grav nu poate fi adoptată doar pe baza prelucrării automatizate a datelor din registrul cu informații despre călătoria sa. Acesta este motivul pentru care evaluarea umană va preceda întotdeauna orice decizie obligatorie pentru persoana respectivă.

Această validare trebuie să intervină în 24 de ore pentru a deschide dreptul de acces la banca de date privind pasagerii.

După validarea corespondenței pozitive, serviciile care sunt la originea acestei corespondențe asigură monitorizarea utilă într-un termen adecvat. O monitorizare utilă ar putea însemna o intervenție activă (percheziție, arestare etc.), însă poate fi vorba și despre a nu întreprinde provizoriu nicio intervenție activă. Această apreciere operațională aparține pe deplin serviciilor competente” (*ibid.*, p. 30 și 31).

- 71 În ceea ce privește criteriile de evaluare prestabilite de UIP, acestea nu pot fi întemeiate pe date care să dezvăluie rasa sau originea etnică a unei persoane, convingerile sale religioase sau filozofice, opiniile sale politice, apartenența la un sindicat, starea sa de sănătate, viața sexuală sau orientarea sexuală. Evaluarea pasagerilor înainte de sosirea, tranzitul sau plecarea lor în raport cu criterii prestabilite se realizează în mod nediscriminatoriu. Aceste criterii nu pot privi identificarea unei persoane și trebuie să fie direcționate, proporționale și specifice.
- 72 În Avizul din 19 august 2016, Comitetul consultativ al Convenției nr. 108 a observat următoarele:

*„Prelucrarea datelor cu caracter personal poate privi toți pasagerii, iar nu numai persoanele vizate suspectate de a fi implicate într-o infracțiune sau de a constitui o amenințare imediată pentru securitatea națională sau pentru ordinea publică.*

*[...]*

*Evaluarea pasagerilor prin corelarea datelor poate ridica problema previzibilității, în special atunci când aceasta este efectuată pe baza unor algoritmi predictivi care utilizează criterii dinamice care pot evalua permanent potrivit capacităților de autoînvățare.*

*Dezvoltarea unor algoritmi de explorare a datelor ar trebui să se întemeieze pe rezultatul unor evaluări regulate privind impactul probabil al prelucrării datelor asupra drepturilor și libertăților fundamentale ale persoanelor vizate.*

*Structura de bază a analizelor ar trebui să se întemeieze pe indicatori de risc predefiniți care au fost stabiliți clar în prealabil.*

*Relevanța rezultatelor individuale ale acestor evaluări automate ar trebui examinată cu atenție de la caz la caz, de către o persoană, iar nu în mod automatizat” (Avizul din 19 august 2016, T-PD(2016)18rev, p. 8).*

- 73 În speță, băncile de date prevăzute la articolul 24 sunt definite cu precizie și sunt în legătură directă cu scopurile prevăzute la articolul 8 din Legea PNR. Este vorba, astfel, despre băncile de date ale „serviciilor competente”, și anume serviciile de poliție, de siguranță a statului, Serviciul general de informații și de securitate și serviciile vamale.

În plus, articolul 24 alineatele 4 și 5 din Legea PNR garantează că, în caz de concordanță pozitivă, prelucrarea sistematică automatizată face obiectul unei verificări individuale prin mijloace neautomatizate, pentru a aprecia dacă autoritatea competentă trebuie să ia măsuri în temeiul dreptului național, astfel cum prevede articolul 6 alineatul (5) din Directiva PNR.

- 74 În Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (EU:C:2017:592), Curtea de Justiție a insistat de asemenea cu privire la necesitatea unei reexaminări individuale prin mijloace neautomatizate înainte de adoptarea unei măsuri individuale (punctul 173).

Cerința unei intervenții umane, după o corespondență pozitivă, constituie o garanție care este de natură să asigure că evaluarea prealabilă nu se întemeiază numai pe mijloace automatizate și contribuie astfel la eficacitatea sistemului.

O evaluare prealabilă sistematică a pasagerilor constituie prin urmare, în principiu, o măsură pertinentă în raport cu obiectivul care constă în identificarea și prevenirea amenințărilor pentru securitatea publică.

Astfel cum a constatat totuși Curtea de Justiție în Avizul 1/15, citat anterior, din 26 iulie 2017, prelucrările care decurg din evaluarea prealabilă „*po[t] furniza informații suplimentare cu privire la viața privată a pasagerilor aerieni*” (punctul 131); în plus, „*respectivul analiză sunt efectuate fără să existe motive întemeiate pe circumstanțe individuale care să permită să se considere că persoanele vizate ar putea prezenta un risc pentru securitatea publică*” (ibid., punctul 132).

Constatând că prelucrarea automatizată a datelor „PNR” întemeiată pe modele și pe criterii prestabilite prezintă o marjă de eroare care nu este neglijabilă (ibid., punctele 169-170), Curtea a considerat totuși că „*modelele și criteriile prestabilite ar trebui, pe de o parte, să fie specifice și fiabile, pentru a permite să se ajungă*



[...] la rezultate care vizează indivizi cu privire la care ar putea exista o bănuială rezonabilă de participare la infracțiuni de terorism sau la infracțiuni transnaționale grave, și, pe de altă parte, să fie nediscriminatorii” și că „bazele de date cu care sunt confruntate datele PNR trebuie să fie fiabile, actuale și limitate la baze de date exploatate de Canada în raport cu combaterea terorismului și a altor infracțiuni transnaționale grave” (ibid., punctul 172). În sfârșit, pentru a garanta că această evaluare nu are un caracter discriminatoriu și că este limitată la strictul necesar, Curtea a considerat că „fiabilitatea și actualitatea acestor modele și a acestor criterii prestabilite, precum și a bazelor de date utilizate ar trebui să facă obiectul unei examinări comune a punerii în aplicare a acordului preconizat, [...] ținând seama de datele statistice și de rezultatele cercetărilor internaționale”, la un an după intrarea în vigoare a acestuia, apoi la intervale regulate (ibid., punctul 174).

- 75 În plus, pare a fi imposibil din punct de vedere tehnic să fie definite mai amplu criteriile prestabilite care vor servi la stabilirea profilurilor de risc. Astfel cum s-a precizat mai sus, aceste criterii trebuie să fie specifice, fiabile și nediscriminatorii.
- 76 Deși Directiva PNR și Legea PNR nu dau indicații cu privire la modul în care criteriile aflate la baza evaluării prealabile sunt prestabilite de UIP, garanțiile care însoțesc elaborarea acestor criterii par suficiente pentru ca măsura atacată să nu fie considerată disproporționată. Este totuși necesar, pentru a decide dacă această evaluare prealabilă sistematică este suficient de clară, precisă și limitată la strictul necesar, să fie adresată Curții o a șasea întrebare preliminară.

– *Cercetările care vizează informații specifice (articolele 27, 50 și 51)*

- 77 Articolul 27 din Legea PNR autorizează prelucrarea datelor pasagerilor pentru a efectua cercetări care vizează informații specifice în scopurile prevăzute la articolul 8 alineatul 1 punctele 1, 2, 4 și 5 și în condițiile prevăzute la articolul 46septies din Codul de procedură penală sau la articolele 50 și 51 din Legea PNR. În conformitate cu articolul 20 din Legea PNR, condițiile de aplicare a articolului 27 sunt valabile de asemenea pentru cererile de acces la expirarea perioadei de șase luni prevăzute la articolul 19.
- 78 Articolul 46septies din Codul de procedură penală privește cercetări care vizează informații specifice în cadrul scopului prevăzut la articolul 8 alineatul 1 punctele 1, 2, 4 și 5 din Legea PNR. Această măsură este însoțită de mai multe garanții, între care autorizarea prealabilă a procurorului Regelui.
- 79 Articolul 16/3 din Legea din 30 noiembrie 1998 privește, la rândul său, cercetări care vizează informații specifice în cadrul scopului prevăzut la articolul 8 alineatul 1 punctul 4 din Legea PNR. Această măsură este însoțită de mai multe garanții, între care informarea și controlul Comitetului permanent R.



- 80 Reclamanta apreciază că membrii detașați ai serviciilor de poliție care aparțin UIP nu ar fi suficient de independenți pentru a răspunde la cererile de acces în cadrul acestor cercetări care vizează informații specifice.
- 81 Articolul 14 alineatul 1 din Legea PNR stabilește compunerea UIP. Lucrările pregătitoare menționează cu privire la acest aspect: *„Modelul belgian se întemeiază pe un concept de unitate multidisciplinară compusă dintr-un funcționar cu funcție de conducere care asigură o misiune de conducere, din membri administrativi și din membri detașați din serviciile competente.*

*UIP va fi compusă:*

- *dintr-un funcționar cu funcție de conducere, asistat de un serviciu de suport care, în cadrul SPF de Afaceri Interne, va fi responsabil, printre altele, cu administrarea băncii de date, cu respectarea obligațiilor transportatorilor și a operatorilor de turism, cu raportarea, cu încheierea de protocoale cu serviciile competente și cu respectarea condițiilor de prelucrare. Serviciul de suport va fi compus, printre altele, din analiști, juriști, experți ICT și din delegatul cu protecția datelor, care vor dispune de abilitățile de securitate necesare.*
- *din membri detașați din serviciile competente, enumerate limitativ la alineatul 1 punctul 2, și anume: serviciile de poliție, serviciile de informații și cele vamale. Scopurile precise constituie în sine prima limitare. De exemplu, la nivelul serviciilor de poliție integrată, este evident că un agent de cartier din cadrul poliției locale nu va putea niciodată să ia cunoștință de datele pasagerilor, din moment ce scopurile nu intră în misiunile sale.*

*Detașarea serviciilor competente are ca obiectiv să garanteze un anumit grad de expertiză, însă nu exclude în niciun mod acorduri între acestea pentru ca detașările să fie reciproce” (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 22).*

*Ministrul de securitate și de interne a adăugat că „[v]a fi desemnat de asemenea un data protection officer responsabil cu raportarea către Comisie cu privire la protecția vieții private” (Doc. parl, Chambre, 2015-2016, DOC 54-2069/003, p. 24).*

*Decretul regal din 21 decembrie 2017 privind punerea în aplicare a Legii PNR stabilește modalitățile de compunere și de organizare a UIP. Raportul către Rege care precedă acest decret regal precizează că „[b]anca de date poate [...] fi consultată numai în cadrul UIP și numai de către membrii UIP în cadrul misiunilor lor, precum și de delegatul cu protecția datelor”<sup>3</sup>.*

Procedura de detașare este organizată la articolele 12-21 din același decret regal. Faptul că membrii detașați ai serviciilor competente participă la funcționarea UIP

<sup>3</sup> Moniteur belge din 29 decembrie 2017, a doua ediție, p. 116833.

urmărește să garanteze că această UIP este compusă din persoane care dețin o anumită expertiză, pentru a consolida astfel eficacitatea UIP. Această posibilitate de detașare este de altfel prevăzută în mod expres la articolul 4 alineatul (3) din Directiva PNR.

Nimic nu permite să se considere că aceste persoane, chiar dacă își păstrează statutul în serviciul de origine, nu își exercită funcțiile în mod independent în cadrul UIP. În plus, membrii UIP sunt pasibili de sancțiuni penale dacă nu respectă secretul profesional sau dacă rețin cu bună știință și în mod voluntar informații și date care se opun scopurilor prevăzute la articolul 8 (articolele 48 și 49).

- 82 În ceea ce privește accesul la datele „PNR” în cadrul unor cercetări care vizează informații specifice după un termen de șase luni, Curtea a considerat, în Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017 (EU:C:2017:592), că utilizarea datelor PNR astfel stocate ar trebui să se întemeieze *„pe criterii obiective pentru a defini împrejurările și condițiile în care autoritățile canadiene vizate de acordul preconizat pot avea acces la aceste date în vederea utilizării lor”* și că *„această utilizare ar trebui să fie condiționată, cu excepția situațiilor de urgență justificate corespunzător, de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă, a căror decizie de autorizare a utilizării intervine în urma unei cereri motivate a acestor autorități, formulată, printre altele, în cadrul procedurilor de prevenire, de detectare sau de urmărire penală”* (punctul 208).
- 83 Pentru a verifica dacă UIP poate fi considerată ca fiind această „altă autoritate națională competentă” în sensul articolului 12 alineatul (3) din Directiva PNR, trebuie adresată Curții de Justiție, înainte de pronunțare, o a șaptea întrebare preliminară.

*Cu privire la durata de păstrare a datelor „PNR” (articolul 18 din Legea PNR)*

- 84 Reclamanta consideră că perioada de cinci ani pentru care sunt păstrate datele „PNR” ar fi disproporționată.
- 85 Considerentul (25) al Directivei PNR are următorul cuprins:

*„Datele din PNR ar trebui să fie păstrate atât timp cât este necesar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave și proporțional cu acest scop. Din cauza naturii datelor și scopurilor pentru care acestea sunt utilizate, este necesar ca datele din PNR să fie păstrate o perioadă suficient de îndelungată pentru efectuarea de analize și pentru utilizarea în investigații. În vederea evitării utilizării disproporționate, după perioada inițială de păstrare datele ar trebui să fie depersonalizate prin mascarea elementelor de date. Pentru a asigura cel mai înalt nivel de protecție a datelor, accesul la datele complete din PNR care permit identificarea directă a persoanei vizate, ar trebui acordat numai în condiții foarte stricte și limitate după perioada inițială respectivă”.*

- 86 Potrivit jurisprudenței Curții de Justiție, perioada de păstrare a datelor trebuie „să răspundă întotdeauna unor criterii obiective, care să stabilească un raport între datele cu caracter personal care trebuie păstrate și obiectivul urmărit” (Hotărârea din 6 octombrie 2015, Schrems, C-362/14, EU:C:2015:650, punctul 93, Ordonanța din 16 martie 2017, Tele2 Sverige și Watson și alții, C-203/15 REC și C-698/15 REC, EU:C:2017:222, punctul 110, Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, EU:C:2017:592, punctul 191).
- 87 În ceea ce privește, mai precis, datele „PNR”, Curtea de Justiție a considerat, în Avizul 1/15, citat anterior, din 26 iulie 2017, că perioada de cinci ani „*nu pare să depășească limitele a ceea ce este strict necesar în vederea combaterii terorismului și a altor infracțiuni transnaționale grave*” (punctul 209), sub rezerva că „*în ceea ce privește pasagerii aerieni pentru care nu a fost identificat un astfel de risc la sosirea lor în Canada și până la plecarea din această țară terță, nu rezultă că există, după plecarea lor, vreun raport, nici chiar indirect, între datele lor PNR și obiectivul urmărit de acordul preconizat, care ar justifica [...] o stocare continuă a datelor PNR ale tuturor pasagerilor aerieni după plecarea lor din Canada în vederea unui eventual acces la aceste date, independent de vreo legătură cu combaterea terorismului și a altor infracțiuni transnaționale grave (a se vedea prin analogie Hotărârea din 21 decembrie 2016, Tele2 Sverige și Watson și alții, C-203/15 și C-698/15, EU:C:2016:970, punctul 119)*” (punctul 205).
- 88 Articolul 18 din Legea PNR prevede că datele pasagerilor sunt păstrate în banca de date privind pasagerii pentru o perioadă maximă de cinci ani începând de la înregistrarea lor și că, la finalul acestei perioade, ele sunt distruse. În conformitate cu articolul 21 alineatul 1 din aceeași lege, UIP se asigură că datele pasagerilor sunt șterse din banca sa de date în mod definitiv la finalul perioadei prevăzute la articolul 18.

Totuși, perioada de cinci ani trebuie interpretată în coroborare cu articolul 19 și următoarele din aceeași lege, care organizează de asemenea modalitățile de păstrare a datelor. Articolul 19 din această lege trebuie interpretat el însuși în coroborare cu articolul 4 punctul 14, care definește „depersonalizarea prin mascarea unor elemente de date”, precum „faptul de a face invizibile pentru un utilizator elementele de date care ar putea servi la identificarea directă a persoanei în cauză, prevăzută la articolul 19”.

Articolul 20 din Legea PNR prevede că, la expirarea perioadei de șase luni prevăzute la articolul 19, comunicarea tuturor datelor pasagerilor este autorizată numai pentru prelucrarea datelor prevăzută la articolul 27 și numai în condițiile prevăzute de această dispoziție.

Pe de altă parte, rezultatul prelucrării prevăzute la articolul 24 este păstrat de UIP numai pentru perioada necesară pentru a informa autoritățile competente și UIP din celelalte state membre cu privire la existența unei corespondențe pozitive (articolul 21 alineatul 3 primul paragraf).

Articolul 22 din Legea PNR garantează că funcționarul cu funcție de conducere și delegatul cu protecția datelor au acces la toate datele relevante numai în cadrul îndeplinirii misiunilor lor.

În sfârșit, prelucrarea datelor face obiectul unei înregistrări și este în corelație directă cu scopurile prevăzute la articolul 8 (articolul 23 alineatul 1). UIP asigură înregistrarea păstrând timp de cinci ani o documentație referitoare la toate sistemele și procedurile de prelucrare aflate în responsabilitatea sa (articolul 23 alineatul 2 primul paragraf).

- 89 Perioada de păstrare a datelor pasagerilor trebuie să fie stabilită ținând seama de scopurile prelucrării acestor date, în legătură directă cu obiectivele de prevenire, cercetare și urmărire penală a infracțiunilor de terorism și a infracțiunilor grave.
- 90 Comisia pentru protecția vieții private a constatat totuși că, atunci când perioada de păstrare a datelor este lungă, iar datele sunt stocate masiv, „riscul de profilare a persoanelor vizate crește, precum și riscul de deturnare a scopului (*fonction creep*), adică deturnarea potențială a utilizării de date pentru alte infracțiuni pentru care nu a existat inițial un acord (politic) de schimb de date” (Comisia pentru protecția vieții private, Avizul din proprie inițiativă nr. 01/2010 din 13 ianuarie 2010 referitor la proiectul de lege de aprobare a Acordului între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și la transferul de date din registrul cu numele pasagerilor (PNR) de către transportatorii aerieni către Departamentul pentru Securitate Internă al Statelor Unite (DHS) (Acordul PNR 2007), semnat la Bruxelles la 23 iulie 2007 și la Washington la 26 iulie 2007, punctul 3.3, p. 17 și 18).

În Avizul nr. 55/2015 din 16 decembrie 2015 cu privire la anteproiectul de lege devenit Legea PNR, Comisia pentru protecția vieții private aprecia de asemenea că necesitatea perioadei de păstrare a datelor de cinci ani trebuia să fie justificată în mod mai precis și argumentat.

În Avizul din 19 august 2016, Comitetul consultativ al Convenției nr. 108 a precizat de asemenea că „datele mascate permit totuși identificarea persoanelor și rămân în acest temei date cu caracter personal, iar păstrarea lor ar trebui de asemenea să fie limitată în timp pentru a preveni o supraveghere permanentă generalizată” (Avizul din 19 august 2016, T-PD(2016)18rev, p. 9).

- 91 Cour constitutionnelle [Curtea Constituțională] consideră că, pentru a verifica dacă această perioadă de păstrare de cinci ani autorizată de Directiva PNR este, ținând seama de ceea ce precedă și de diferitele garanții enumerate la punctul 88 de mai sus, compatibilă cu observațiile Curții de Justiție menționate la punctul 87 de mai sus, din moment ce nu efectuează nicio distincție după cum reiese, în cadrul evaluării prealabile, că pasagerii vizați pot sau nu să prezinte un risc pentru securitatea publică, este necesar să fie adresată Curții o a opta întrebare preliminară.

### 3. *Cu privire la al doilea motiv*

92 Reclamanta apreciază că, prin extinderea sistemului „PNR” la zborurile intra-UE, dispozițiile atacate restabilesc indirect controale la frontieră, care ar fi contrare libertății de circulație a persoanelor.

93 În ceea ce privește domeniul de aplicare al Legii PNR, lucrările pregătitoare arată:

„Includerea intra-UE în colectarea datelor va permite să se obțină un tabel mai complet al deplasărilor pasagerilor care constituie o amenințare potențială pentru securitatea intracomunitară și națională. Practica a demonstrat deja că unii «*returnees*» (denumiți de asemenea *foreign fighters* care se întorc în Europa) se îmbarcă la bordul a diferite zboruri înainte de a ajunge la destinația lor finală.

Directiva UE PNR prevede în mod expres posibilitatea statelor membre de a prelucra datele pasagerilor din UE pentru traficul internațional în cadrul Uniunii Europene. În plus, toate statele membre au aprobat, la 21 aprilie 2016, în Consiliul de Miniștri de interne și ai justiției, o declarație privind transpunerea Directivei UE PNR în legislațiile naționale și pentru traficul intra-Uniunea Europeană” (Doc. Parl., Chambre, 2015-2016, DOC 54-2069/001, p. 7).

94 Cour constitutionnelle [Curtea Constituțională] arată că pasagerii prevăzuți la capitolul 11 din Legea PNR, precum și datele prevăzute și termenul de păstrare, sunt limitați.

Lucrările pregătitoare arată astfel că „[...] sunt vizați numai pasagerii care doresc să treacă sau au trecut frontierele externe ale Belgiei pentru a intra sau pentru a ieși din aceasta, indiferent de tipul de transport utilizat (maritim, feroviar, terestru, aerian). Prin urmare, numai datele acestor pasageri vor fi prelucrate de serviciile de poliție responsabile cu controlul la frontiere și de Oficiul pentru străini.

Pasagerii care intenționează să treacă prin zona internațională de tranzit, de exemplu, a unui aeroport situat în Belgia sunt de asemenea vizați, în măsura în care normele privind accesul pe teritoriu, șederea, stabilirea și îndepărtarea străinilor li se aplică de asemenea. Astfel, aceste persoane trebuie să dispună de documentele de călătorie necesare. Anumite persoane sunt supuse obligației de a deține o viză de tranzit aeroportuar; controalele în aceste zone sunt autorizate și pot conduce, în anumite cazuri, la o măsură de returnare.

[...] numai datele pasagerilor denumite «API» vor fi transmise serviciilor de poliție și Oficiului pentru străini în temeiul prezentului capitol. Aceste date sunt enumerate la articolul 9 alineatul 2 din anteproiectul de lege.

Acestea corespund, în esență, cu cele pe care transportatorii aerieni trebuie să le transmită deja în temeiul Decretului regal din 11 decembrie 2006.

[...]



Utilizarea datelor este limitată de asemenea la 24 de ore. Dincolo de acestea, în cazul în care accesul la datele pasagerilor este necesar în cadrul exercitării misiunilor sale legale, Oficiul pentru Străini adresează UIP o cerere motivată” (*ibid.*, p. 34 și 35).

- 95 Astfel cum s-a menționat mai sus, considerentul (10) al Directivei PNR organizează procedura privind extinderea domeniului de aplicare.

Scopul referitor la combaterea imigrației ilegale și la îmbunătățirea controlului la frontiere privește numai categoriile de pasageri enumerate la articolul 29 alineatul 2 din Legea PNR și se limitează la datele „API” prevăzute la articolul 9 alineatul 1 punctul 18 din această lege. Prelucrările efectuate în cadrul acestui scop sunt de asemenea limitate. Dispozițiile atacate se înscriu în cadrul transpunerii Directivei „API”, care urmărește de asemenea ca obiective combaterea imigrației ilegale și îmbunătățirea controlului la frontiere.

- 96 În Avizul nr. 55/2015 din 16 decembrie 2015 privind anteproiectul de lege devenit Legea din 25 decembrie 2016, Comisia pentru protecția vieții private ridică totuși problema compatibilității cu principiul liberei circulații a persoanelor a sistemului „PNR” instituit, care privește „atât transporturile având ca destinație și punct de plecare spațiul Schengen (extra-Schengen), cât și transporturile care intră și ies din spațiul Schengen (intra-Schengen)”, ceea ce ar putea duce „în mod indirect la o restabilire a controlului la frontierele” (punctele 21-25).
- 97 Având îndoieli cu privire la interpretarea și la validitatea Directivei 2004/82 „API” în raport cu carta și cu TUE, Cour constitutionnelle [Curtea Constituțională] decide să adreseze Curții o nouă întrebare preliminară.
- 98 Cour constitutionnelle [Curtea Constituțională] adresează o ultimă întrebare referitoare la eventuala organizare a efectelor în timp ale hotărârii sale.

#### **IV. Întrebările preliminare**

Cour constitutionnelle [Curtea Constituțională] adresează, prin urmare, următoarele întrebări:

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 același regulament trebuie interpretat în sensul că se aplică unei legislații naționale precum Legea din 25 decembrie 2016 privind prelucrarea datelor pasagerilor, care transpune Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și 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?

2. Anexa I la Directiva (UE) 2016/681 este compatibilă cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene în măsura în care datele pe care aceasta le enumeră sunt foarte largi – în special datele prevăzute la punctul 18 din anexa I la Directiva (UE) 2016/681, care depășesc datele prevăzute la articolul 3 alineatul (2) din Directiva 2004/82/CE – 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 la Directiva (UE) 2016/681 sunt compatibile cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene în măsura în care, având în vedere termenii „inclusiv” și „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?

4. Articolul 3 punctul 4 din Directiva (UE) 2016/681 și anexa I la aceeași directivă sunt compatibile cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene 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 (UE) 2016/681 coroborat cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene trebuie interpretat în sensul că se opune unei legislații naționale precum legea atacată, care admite, ca scop al prelucrării datelor „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 (UE) 2016/681 este compatibil cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene 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 (UE) 2016/681, poate fi interpretată în sensul că vizează UIP creată prin Legea din 25 decembrie 2016, care ar putea, prin urmare, să autorizeze accesul la datele „PNR” după o perioadă de șase luni, în cadrul unor cercetări care vizează informații specifice?

8. Articolul 12 din Directiva (UE) 2016/681 coroborat cu articolul 7, cu articolul 8 și cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene 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 2004/82/CE este compatibilă cu articolul 3 alineatul (2) din Tratatul privind Uniunea Europeană și cu articolul 45 din Carta drepturilor fundamentale a Uniunii Europene în măsura în care obligațiile pe care aceasta le instituie se aplică zborurilor din interiorul Uniunii Europene?

b) Directiva 2004/82/CE coroborată cu articolul 3 alineatul (2) din Tratatul privind Uniunea Europeană și cu articolul 45 din Carta drepturilor fundamentale a Uniunii Europene 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 (UE) 2016/681, încalcă una sau mai multe dintre obligațiile care decurg din dispozițiile menționate în aceste întrebări, ar putea să mențină provizoriu efectele Legii din 25 decembrie 2016 privind prelucrarea datelor pasagerilor 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 lege?