German Law Journal (2024), **25**, pp. 1068–1079
doi:10.1017/glj.2024.60

ARTICLE

Special Issue: Strategic Litigation in EU Law

A Challenge to Systematic and Undifferentiated Data Collection Through Strategic Litigation: The *Passenger Name Record* Case (Ligue des Droits Humains) Before the Court of Justice of the EU

Catherine Forget

Lawyer (Brussels Bar), University of Saint-Louis Brussels, Brussels, Belgium
Email: cf@juscogens.be

(Received 19 November 2024; accepted 19 November 2024)

Abstract

At a time when the European Union and its Member States are constantly adopting measures to combat serious crime and terrorism, particularly through the prism of data protection rules, the CJEU is acting as a bulwark by imposing compliance with strict conditions, thereby encroaching on national rules of criminal procedure, which are initially the responsibility of the Member States. In this contribution, we will examine how and on what basis the Ligue des Droits Humains was able to get the CJEU to rule on the Passenger Name Records Directive, and to what extent this action was indeed "strategic."

Keywords Passenger Name Records; protection of personal data; untargeted and systematic surveillance; algorithms

A. Introduction

The adoption of Directive 2016/681[1] on the processing of passenger data ("PNR Directive" for "Passenger Name Record") was the subject of lengthy negotiations and criticism. The measure involves the systematic processing and transfer of all air passenger data in order to determine "risk profiles" using "dynamic" algorithms or pre-established behavioral models.[2] The aim is to explore data in order to "situate" passengers on a risk scale and thus enable the identification of "possible or probable" criminals.[3] According to the Council of Europe, such a mechanism targeting people "who have not committed any offence" could in no way pursue "a legitimate aim," especially as there is an unavoidable risk of error that could lead to discriminatory profiling.[4] Against the backdrop of the Charlie Hebdo attacks in Paris in January 2015, the European Parliament nonetheless agreed to the PNR Directive, in line with the resolutions

[1]Directive 2016/681 of the European Parliament and of the Council of April 27, 2016, On the Use of Passenger Name Record (PNR) Data for the Prevention, Investigation, Detection and Prosecution of Terrorist Offences and Serious Crime, 2016 O.J. (L 119) 132–49 (EU) [hereinafter "PNR Directive"].

[2]*See* Douwe Korff, *Passenger Name Records (PNR), Data Mining and Data Protection: The Need for Strong Safeguards* (2015), https://rm.coe.int/16806a601b.

[3]*Id.*

[4]*Id.*

adopted by the United Nations Security Council in 2017 and 2019, recommending that States introduce such a system.[5]

The Belgian legislature implemented the PNR Directive fairly quickly through the Law of December 25, 2016 on the processing of passenger data[6] (the "PNR Law"). Given the serious interference this law entails in fundamental rights, including the right to privacy and the right to protection of personal data guaranteed respectively by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the "Charter"), in July 2017, the *Ligue des droits Humains* ("LDH") decided to lodge an action for annulment with the Belgian Constitutional Court. Indeed, Belgium offers associations the possibility of directly challenging the legality of a legislative or regulatory measure, in other words, without the intervention of a person concerned, thus facilitating the introduction of strategic appeals. Once the matter had been referred to it, the Constitutional Court in turn asked ten questions for a preliminary ruling to the Court of Justice of the EU ("CJEU") to determine whether the PNR Directive complied with Articles 7, 8, 45 and 52(1) of the Charter.

In this Article, after briefly outlining the PNR Law, we will review the various stages of the proceedings in this strategic dispute. We will see that, via the proportionality test of the interference, the CJEU automatically took up issues that had not been specifically raised by the LDH or by the Constitutional Court. We will conclude by presenting the new Belgian draft law that implements the conditions imposed by the CJEU—an implementation that is not without its challenges given the particularly flexible interpretation of the Belgian legislator.

B. European and National Legislative Context

The PNR Directive requires the systematic transfer of all passenger data[7] on a flight outside the EU, in other words, between a third country and the European Union, to the Passenger Information Unit ("PIU") of the Member State of departure of the flight or of destination for the purposes of combating serious crime and terrorism.[8] This transfer is carried out in order to automatically and systematically compare passenger data with "useful" databases or using pre-established criteria.[9] If a passenger presenting a risk to public security is identified, further checks may be carried out, leading to binding individual decisions.[10] These data are then kept for a period of five years after having been de-identified—by masking—after a period of six months and are made accessible at the request of the competent authorities.[11]

[5]United Nations Security Council Resolution 2396 (2017) (discussing threats to international peace and security caused by returning foreign terrorist fighters):

> *The Security Council: . . . 12. Decides that Member States will enhance their capacity to collect, process and analyze, within the framework of ICAO standards and recommended practices, Passenger Name Record (PNR) data and ensure that such data is shared with and used by all competent national authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offences and terrorist travel[] . . . .*

(second emphasis added). *See also* United Nations Security Council Resolution 2482 (2019) (discussing threats to international peace and security).

[6]Loi du 26 décembre 2016 L'enregistrement du nom des passagers [The Passenger Data Processing Act], M.B., Jan. 25, 2017 [hereinafter "PNR Law"].

[7]This is information initially collected by air carriers for commercial purposes for each journey booked by a passenger, such as the full itinerary, travel agency, seat number, baggage information, check-in and boarding data —type of travel document, document number, nationality, number, weight and identification of baggage, transport number, et cetera—methods of payment, billing address, and, more generally, general remarks about each passenger. *See* PNR Directive at Annex 1.

[8]*Id.* at art. 1.

[9]*Id.* at art. 6(2)(a), (3).

[10]*Id.* at art. 6(5).

[11]*Id.* at art. 12.

Similarly, the PNR Law introduces into Belgian law an obligation for carriers and travel operators in the various international transport sectors—air, rail, road, and sea—to collect information relating to their passengers.[12] This data, which is sent to the PIU,[13] is analyzed prior to a person's arrival, transit, or departure on national territory.[14] Using algorithms based on pre-established criteria, the processing must make it possible to "assess the potential threat and determine which passengers are of interest for the performance of their duties or, for example, require action to be taken (execution of an arrest warrant, search, etc.)."[15] In addition, these data are correlated with databases or lists managed by the competent services or which are directly accessible to them as part of their duties.[16] If a passenger is identified as presenting a risk to public security, further checks may be carried out, leading to binding individual decisions.[17] In practice, a positive "HIT" has to be validated by the PIU within 24 hours and is then translated into a "match." Data processing is therefore not fully automated. Once validated, the result of the assessment is forwarded to the competent services, which must ensure follow-up within an appropriate timeframe, in other words, for example, arrest the person concerned at the airport or control his identity.[18] This data is then kept for a period of five years after being de-identified—by masking—at the end of a six-month period, and is made accessible at the request of the competent services.[19] The latter may carry out ad hoc searches within the limits of their missions and the purposes set out in the law, in particular the fight against terrorism, the investigation and prosecution of certain offenses, and the fight against illegal immigration.[20] The scope of the PNR Law and the purposes for which it applies are therefore particularly broad, and in any case broader than in the PNR Directive.

C. The National Litigation Phase

Given the serious interference of the PNR law into the fundamental rights of all travelers, it was obvious for the LDH to introduce a legal action to challenge the use of automated means without sufficient guarantees and the possibility of using such a system to combat immigration and for border control purposes. This tendency towards "crimimmigration,"[21] which consists of mixing "repressive" and "border management" purposes, had already been criticized on numerous occasions in the past, in the context of discussions on VIS, SIS, and EURODAC, and in the context

[12]The PNR Law distinguishes between API data, in other words, check-in and boarding data, and PNR data, that is, reservation data. API data is authentic data, for example, biographical data on an identity card. PNR data includes more information. This includes the passenger's full itinerary, travel agency, seat number, baggage information, check-in and boarding data—type of travel document, document number, nationality, baggage weight and identification, carriage number, et cetera—payment methods and billing address, et cetera. *Id.* at art. 9.

[13]The PIU, set up within the Federal Public Service Interior, is responsible for analyzing and processing passenger data. It is made up of members seconded from the police, State Security, the General Intelligence and Security Service, and investigation services linked to customs and excise offences. PNR Law at art. 3.

[14]*Id.* at art. 15.

[15]Projet de loi relatif au traitement des données passagers du 4 octobre 2016, Exposé des motifs, *Doc parlementaire,* Chambre, 2015–2016, n° 54–2069/001, p. 28 (drafting law on the processing of passenger data)

[16]PNR Law at art. 24 § 2, *1.

[17]*Id.* at arts. 18–19.

[18]*See e.g.*, Centre de crise national, *Rapport annuel 2023 NTTC* (2023), https://centredecrise.be/sites/default/files/documents/files/Rapport%20annuel%20NTTC%202023.pdf.

[19]PNR Law at art. 14 § 1, 2° (defining "competent services" as police services, State security services, the General Intelligence and Security Service and investigation services for customs and excise offences).

[20]*Id.* at art. 8.

[21]The concept of "crimmigration" was developed by researchers who established a link between immigration and crime. *See* Joanna Parkin, *The Criminalisation of Migration in Europe: A State-of-the-Art of the Academic Literature and Research,* CEPS Liberty and Security in Europe 61 (2013).

of the introduction of smart borders, for example.[22] The interference caused by the PNR Law was all the more significant because the PNR system applied in Belgium not only to air travel, but also to rail, land, and even sea travel, to and from Belgium within the EU, without crossing external borders with third countries.

From the point of view of the litigants, it should be noted that the LDH is organized into different commissions that reflect on human rights topics. These commissions provide reactions to current events and aim to look to the future with the objective to safeguard fundamental rights. The work of the commissions can be disseminated in a variety of forms: Press articles, conferences, papers, and even legal actions. In this case, after discussions and debates held by its members, the *Commission des nouvelles technologies et de la vie privée* suggested to one of its lawyers to take legal action. The LDH has a pool of lawyers, who are prepared to intervene and take legal action on a pro bono basis—with little or no remuneration. This can lead to a few difficulties, particularly when it comes to writing detailed legal arguments or developing a concrete strategy to launch legal proceedings. Lawyers work in their spare time, often in isolation, although they sometimes benefit from the help of legal academics who are willing to devote their time on a pro bono basis.[23] In contrast, the State is often defended by numerous lawyers who are often from large legal firms. It could be compared to David fighting Goliath. The PNR case is even more emblematic in that the subject matter is extremely technical.

However, the need to challenge this legislation was even more pressing given that shortly before the adoption of the PNR Directive, the ECJ invalidated the so-called "data retention" Directive 2006/24/EC[24] on the grounds that there were insufficient safeguards to limit the interference "to what is strictly necessary."[25] This legal instrument required telephone operators to systematically and indiscriminately collect[26] metadata for the purpose of combating serious crime. It therefore entailed a "particularly serious" interference with the right to respect for private life and the protection of personal data.[27] A few years later, the ECJ clearly censured the data retention obligation imposed on operators on the grounds that it was "generalized and indiscriminate" and recommended "targeted" retention of metadata.[28] According to the Court, any intrusion into the right to respect for private life and the protection of personal data must comply with the principle of proportionality and must therefore be within the limits of what is "strictly necessary."[29] Therefore, we were hoping that this case law could be used to invalidate the PNR Directive.

On July 24, 2017, the LDH introduced an action for annulment with the Belgian Constitutional Court. Indeed, such an action needs to be lodged within six months of the adoption of the contested regulation as required by Article 3 of the special law of January 6, 1989. This action could be submitted relatively quickly, as it does not require the intervention of a person concerned. Belgium is unusual in that it allows any natural or legal person to bring an objective dispute, for example when challenging the legality of laws or regulations before the Constitutional Court[30] or

[22]European Data Protection Supervisor, *Opinion 06/2016 on the European Union's Second Smart Borders Package* (Sept. 21, 2016).

[23]We would like to take this opportunity to thank Franck Dumortier, a researcher at the University of Namur (CRIDS) and then at the Vrij Universiteit Brussel, for his invaluable collaboration and his involvement in many of the Ligue des droits Humains projects.

[24]Council Directive 2006/24 of March 15, 2006, Retaining Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54–63 (EC) [hereinafter Directive 2006/24/EC].

[25]EJC, Joined Cases 293 & 594/12, Digital Rights Ireland Ltd. v. Minister for Communications, ECLI:EU:C:2014:238 (Apr. 8, 2014).

[26]Metadata is the data processed and generated during an electronic communication, with the exception of its content.

[27]*Digital Rights Ireland Ltd.*, Joined Cases 293 & 594/12 at paras. 66.

[28]EJC, Joined Cases 203 & 698/15, Secretary of State for the Home Department v. David Davis, ECLI:EU:C:2016:70 (Dec. 21, 2016).

[29]*Digital Rights Ireland Ltd.*, Joined Cases 293 & 594/12 at paras. 51–52; *Secretary of State for the Home Department,* Joined Cases 203 & 698/15 at paras. 96–103.

[30]1994 Const. (Belg.) art. 142.

the Council of State, respectively.[31] It is up to the applicant to justify his or her interest in taking action, in other words, that he or she is likely to be personally, directly, and adversely affected by the contested regulation.[32] However, an *actio popularis* ("popular action") is not permitted.[33] In the case of a non-profit association, the Constitutional Court requires several conditions to be met: Its statutory purpose must be of a particular nature and therefore distinct from the general interest, it must defend a collective interest, the contested regulation must be likely to affect its societal purpose, and that purpose must actually be pursued.[34] The LDH's interest in taking action is rarely challenged by the Constitutional Court, as its association's Articles state that its aim is "to combat injustice and any arbitrary infringement of the rights of an individual or a community [and to defend] the principles of equality, freedom, solidarity and humanism."[35]

D. The Litigation Before the CJEU

In its application to the Constitutional Court, the LDH's request was for the PNR law to be annulled on the grounds that it was incompatible with Articles 7, 8, and 52(1) of the Charter. We also claimed infringement of Article 45 of the Charter, given that the PNR system was implicitly re-establishing border controls. Contextually, it should be noted that two days after the appeal to the Constitutional Court was lodged, the CJEU published an opinion[36] on the PNR agreement signed in 2014 between the European Union and Canada.[37] The CJEU did not invalidate the agreement but imposed strict conditions.[38] Therefore, the LDH already assumed that the PNR Directive would probably not be invalidated by the CJEU, but that the Court would specify the conditions on the PNR Directive. Given that it was a national law implementing EU law that was challenged, in accordance with Article 267 TFEU, the Constitutional Court turned to the CJEU

[31] *Id.* at art. 160.

[32] *Id.* at art. 142, para. 3; Bijzondere wet op het Grondwettelijk Hof of [Special law on the Constitutional Court], Jan. 6, 1989, art. 2, 2° (available at https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=nl&lg_txt=n&type=&sort=&numac_search=1989021001&cn_search=&caller=article&&view_numac=1989021001fx1989021001n).

[33] The interest pursued must therefore be distinct from that of any person placed in the same circumstances. On this question, see, among others, Philippe Coenraets, *La notion d'intérêt à agir devant le Conseil d'Etat: un difficile équilibre entre l'accès au prétoire et la prohibition de l'action populaire*, 349 (Le Conseil d'Etat de Belgique 50 ans après sa création, Bruylant, 1999).

[34] *See* Anne-Sophie Lemaire, Antoine Gillet, Céline Romainville, Evrard de Lophem, Frédéric Georges, Hakim Boularbah, Jean-François van Drooghenbroeck & Nathalie Uyttendaele, *Le droit commun de l'action d'intérêt collectif: l'article 17, alinéa 2, du Code judiciaire*, 52, (Le droit judiciaire et les pots-pourris, Anthemis, 2020).

[35] Association of the Councils of State and Supreme Administrative Jurisdictions of the European Union, Answers to the questionnaire for Council of State of Belgium, § B.6.3. (available at https://www.aca-europe.eu/colloquia/2012/Belgium.pdf).

[36] Opinion 1/2015, 2017, ECLI:EU:C:2017:592 at para. 12.

[37] The envisaged agreement, resulting from negotiations with Canada, was initialed on May 6, 2013. On July 18, 2013, the Commission adopted a proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (European Commission, Proposal for a Council Decision on the conclusion of the envisaged Agreement COM(2013) 528 final)(Proposal for a Council Decision on the conclusion of the envisaged Agreement) and a proposal for a Council Decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (European Commission COM(2013) 529 final).

[38] Thus, the CJEU imposed the clarification of the categories of data transferred, the exclusion of the processing of sensitive data due to the absence of precise and solid justification, the use of specific, reliable and non-discriminatory pre-established models and criteria, the limitation of the cross-checking of data with other databases presenting a link with the intended purpose, the exclusion of vague and general purposes, the data retention period in relation to the objective pursued, access to data based on a reasoned request from the competent authorities meeting objective criteria, coupled with prior checking by a court or an independent administrative body, the communication of PNR data to a third country subject to an agreement between the EU and that third country equivalent to the agreement envisaged or an adequacy decision by the Commission, the existence of the rights of data subjects (access, rectification, individual information), the right to an effective remedy and, lastly, monitoring of compliance with these rules by an independent supervisory authority.

and referred ten questions for a preliminary ruling to the Court of Justice.[39] Let us examine the various arguments put forward by the LDH and the responses of the CJEU.

I. Infringement of the Right to Privacy and the Protection of Personal Data

1. The Absence of a Legitimate Aim

In its initial application, the LDH first pointed to a violation of Articles 7, 8, and 52(1) of the Charter on the grounds that the PNR measures had no legitimate purpose. According to the Council of Europe, the "pre-screening" approach, which consists of assessing the risk posed by passengers in order to anticipate their behavior or establish specific profiles, is not a "legitimate" objective.[40] The CJEU did not rule on this point, considering that the fight against terrorism and serious crime are aims in the general interest capable of justifying "even serious" interferences with fundamental rights.[41] In addition, according to the CJEU, the measure did not affect the essential content of the rights to respect for private life and to the protection of personal data, because the nature of the information processed was limited to certain aspects of privacy relating to a person's travels and did not provide a complete overview of the private life of the data subjects. According to the Court, the interference was therefore not identical to the one involved in the retention of data, which the CJEU had described as "particularly serious."[42]

2. The Absence of Necessity

Moreover, pointing to the high error rate and the risk of discrimination that such a system entails, the LDH regretted that the measure was not necessary, as provided for in Article 52(1) of the Charter. In this respect, during the hearing before the Grand Chamber,[43] the judge-rapporteur von Danwitz expressed particular concern about the large number of false positives mentioned by the European Commission and the resulting lack of reliability of the system. The European Commission's 2020 working document mentions a positive match rate of 0.59% for 2019, of which only 0.11% was transferred to the competent authorities.[44] For 2018, the corresponding percentages were 0.25% and 0.04% respectively.[45] The judge-rapporteur was also concerned that a trivial act—getting on a plane—could result in the processing of data such as address and bank details being retained for five years. Nevertheless, in its ruling, the CJEU, while acknowledging the

[39]CC [Constitutional Court], Oct. 17, 2019, n°135/2019.

[40]Consultative Committee of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *supra* note 2, at 15.

[41]ECJ, Case C-817/19, Ligue des droits humains ASBL v. Conseil des ministres, ECLI:EU:C:2022:491 (June 21, 2022), para. 122.

[42]It emphasized that, in the case of electronic communications data, "such data, taken as a whole, are likely to make it possible to draw very precise conclusions about the private lives of the persons whose data have been stored, such as their daily habits, places of permanent or temporary residence, daily or other movements, activities, social relations and social circles frequented by those persons." The Court went on to state that "it must be concluded that the interference by Directive 2006/24 with the fundamental rights enshrined in Articles 7 and 8 of the Charter is, as the Advocate General also pointed out, in particular in paragraphs 77 and 80 of his Opinion, on a vast scale and must be regarded as particularly serious. In addition, the fact that the data are stored and subsequently used without the subscriber or registered user being informed is liable to give rise in the minds of the persons concerned, as the Advocate General pointed out in paragraphs 52 and 72 of his Opinion, to the feeling that their private lives are under constant surveillance." S*ee Digital Rights Ireland Ltd.*, Joined Cases 293 & 594/12 at paras. 27, 37.

[43]For a detailed account, *see* Christian Thönnes, *On Flights, Rock Concerts and the Needle in a Haystack, A Report from Court of Justice of European Union's Oral Hearing on PNR Directive*, EU Law Analysis blog (Sept. 17, 2021), https://eulawanalysis.blogspot.com/2021/09/on-flights-rock-concerts-and-needle-in.html.

[44]European Commission, *Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM (2020) 305 final, at 28 (July 20, 2020).

[45]*Id.*

high number of "false positives," considered that this was not such as to undermine the system's suitability. Taking up the Commission's figures, the CJEU pointed to the number of air passengers which were successfully identified thanks to the PNR system because they were presenting a risk in the fight against terrorist offenses and serious crime.[46] Furthermore, according to the CJEU, this error rate must be read in conjunction with subsequent checks of the results obtained using non-automated means[47] and therefore did not follow the argument raised by the LDH.

The LDH also pointed to the lack of an impact assessment carried out prior to the introduction of the PNR system. According to the European Data Protection Supervisor (EDPS), an impact assessment can demonstrate why the planned measure is effective and why other, less intrusive measures, would not achieve the desired objective.[48] For example, in the case of large-scale processing of personal data or profiling, the General Data Protection Regulation (GDPR) requires an impact assessment to be carried out,[49] containing the following elements in particular: A systematic description of the operations—nature, scope, and context—the purposes, the categories of data and their retention period, an assessment of the necessity and proportionality with regard to the intended purpose, the rights of the data subjects, the safeguards concerning international data flows, an assessment of the risks to the rights and freedoms of the data subjects, and the measures envisaged to address these risks.[50] This approach would have made it possible to assess the impact of the planned processing operations on the rights and freedoms of the data subjects of the PNR Directive and to demonstrate its compliance with the Charter. Surprisingly, neither the Constitutional Court nor the CJEU responded to this argument.

3. The Absence of Proportionality

As regards the lack of proportionality, in its initial application, the LDH pointed to the systematic, "non-targeted," nature of the measure, resulting in excessive interference with Articles 7 and 8 of the Charter. More specifically, it argued that the safeguards were insufficient, particularly noting the following: The data processed, the categories of data and the databases were not specified, the purposes were too broad—they included the fight against illegal immigration and the fight against ordinary crime and intelligence, the data retention period was excessive, and there was a possible correlation with databases that were not linked to terrorism or serious crime.

In its decision, aligning itself with Opinion 1/2015 and the Opinion of Advocate General,[51] the Court of Justice confirmed the validity of Directive 2016/681 under the Charter but set strict conditions.[52] It held that the PNR Directive entailed a serious interference with the rights guaranteed by Articles 7 and 8 of the Charter, namely the right to respect for private life and the right to protection of personal data. According to the Court, the purpose of such a measure is to establish "a system of continuous, untargeted and systematic surveillance, including the automated evaluation of personal data relating to all persons using air transport services."[53] While such data taken on its own does not seem capable of revealing precise information about

[46]*Ligue des droits humains ASBL,* Case C-817/19 at para 123.

[47]*Id.* at para. 124.

[48]European Data Protection Supervisor, "Guide for assessing the necessity of measures restricting the fundamental right to protection of personal data," at 20 (Apr. 11, 2017).

[49]Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119), 1–88 (EU) (GDPR), art. 35.

[50]*See* Article 29 Data Protection Working Party on the protection of individuals with regard to the processing of personal data, Guidelines on data protection impact assessment (DPIA) and the determination of processing "likely to result in a high risk" for the purposes of Regulation 2016/679, Apr. 4, 2017.

[51]Opinion of Advocate General Pitruzzella, Case C-817/19, Ligue des droits humains *v.* Conseil des ministers, ECLI:EU:C:2022:65, paras. 35-231, (Jan. 27, 2022).

[52]*Ligue des droits humains ASBL,* Case C-817/19 at paras. 112–18.

[53]*Id.* at para. 111.

the private lives of the data subjects, the fact remains that, taken together, such data can—among other things—reveal a complete travel itinerary, travel habits, relationships existing between two or more persons, as well as information about the financial situation of air passengers, their eating habits, their states of health, or even reveal other sensitive information about these passengers.[54]

Thus, in order to limit the interference to what is strictly necessary, the Court has methodically examined the substantive and procedural rules governing the scope of the measures provided for by the PNR Directive and whether the system which it puts in place meets objective criteria establishing a link between the PNR data and the purposes pursued.[55] In this respect, firstly, the data processed under the system must be clearly identifiable and restricted to the headings set out in Annex I.[56] Furthermore, with regard to prior assessment on the basis of PNR data, the PIU may compare this information only with its own databases concerning persons or objects wanted, or for which an alert has been issued.[57] In order to meet the requirement that the criteria laid down be targeted, proportionate, and specific, the databases must be used in connection with the fight against terrorist offenses and serious crime with an objective—or at least indirect—link to the carriage of passengers by air.[58] Moreover, the period for which data is kept must be linked to the objective pursued[59] and access to such data must—in principle, except in duly justified cases of urgency—be subject to prior control either by a court, or by an independent administrative authority, upon a reasoned request from the competent authorities.[60]

In addition, before the hearing, the CJEU asked questions directly to the European Commission, the European Parliament, and the European Union Agency for Fundamental Rights concerning the use of algorithms—an argument not raised by the LDH or the Constitutional Court. Indeed, as the CJEU had already pointed out in *Opinion 1/2015*, the extent to which automated analysis of PNR data interferes with the rights enshrined in Articles 7 and 8 of the Charter depends essentially on the models, pre-established criteria, and the databases on which this type of data processing is based.[61] Asking those questions was an opportunity for the Court to clarify its previous case law by requiring compliance with additional criteria that was not mentioned in its *Opinion 1/2015*. Specifically, the Court added that the pre-established criteria must be additional, proportionate, and include both incriminating and exculpatory elements—as this requirement is likely to contribute to the reliability of these criteria and —in particular—to ensure that they are proportionate—as required by the second sentence of Article 6(4) of the PNR Directive.[62] Therefore, as far as the pre-assessment using pre-established criteria is concerned, artificial intelligence technology cannot be used in the context of machine learning systems.[63] Given the opacity of artificial intelligence technologies,[64] it may be impossible to understand why a given program has obtained a positive match.[65] Under these conditions, the use of these technologies could also deprive the data subjects of their right to an effective judicial remedy

[54]*Id.* at para. 100.
[55]*Id.* at para. 125.
[56]*Id.* at paras. 126–40.
[57]*Id.* at paras. 182–92.
[58]*Id.* at para.191.
[59]*Id.* at para. 262.
[60]*Id.* at para. 223.
[61]*Id.* at para. 103.
[62]*Id.* at para. 200.
[63]*Id.* at para. 194.
[64]*See* Marc Rotenberg, *ECJ PNR Decision Unplugs the "Black Box"*, 3 EUR. DATA PROTECT. L. 431, 435 (2022); Janneke Gerards, *Machine Learning and Profiling in the PNR System,* VERFASSUNGSBLOG (May 8, 2023), https://verfassungsblog.de/ml-pnr/.
[65]*Ligue des droits humains ASBL,* Case C-817/19 at para. 195.

enshrined in Article 47 of the Charter.[66] Furthermore, individuals should be able to find out about the pre-established evaluation criteria and the program applying these criteria so that they can decide—in full knowledge of the facts—whether or not to exercise a judicial remedy.[67] In so doing, the CJEU has for the first time specified the conditions of application of an artificial intelligence system in the context of the fight against serious crime and terrorism.

II. Infringement of Freedom of Movement

In addition to the violation of Articles 7 and 8 of the Charter, the LDH also invoked the infringement of the freedom of movement guaranteed by Article 21(1) TFEU and Article 45 of the Charter. Firstly, the PNR Law expressly authorized the processing of PNR data for the purposes of improving border controls and combating illegal immigration—purposes that are not covered by the PNR Directive. Secondly, the PNR Law was intended to apply to air, rail, bus, and boat travel from third countries as well as "intra-EU," which implies an extremely broad scope. As a reminder, the Schengen Borders Code authorizes Member States to carry out checks at internal borders, provided that these checks do not have an "equivalent effect" to border checks.[68] The only exception is to authorize Member States to temporarily reintroduce checks at internal borders in exceptional circumstances in the event of a serious threat to public order and national security, limited to a maximum of 6 months.[69]

With regard to the purposes pursued, following the CJEU, the application of such a system must be limited to terrorist offenses and serious crime,[70] to the exclusion of any other purpose such as the fight against illegal immigration[71] or the monitoring of activities targeted by intelligence services.[72] In addition, the PNR system may be extended to all or part of intra-EU flights—or even to other means of transport within the Union— only if there are sufficiently specific circumstances to consider that the State concerned is facing a real and present or foreseeable terrorist threat.[73] The measure must be limited in time and subject to review by an independent court or administrative body.[74] In the absence of such a threat, this extension must be limited to intra-Community flights involving particular air routes, modes of travel, or certain airports for which there are—in the assessment of the Member State concerned—indications to justify this application.[75] Limiting the scope of the PNR system was seen as a victory, given that the majority of flights are intra-EU—75%.[76]

E. Post European Litigation Phase

Following the CJEU ruling, the Belgian Constitutional Court applied some of the requirements of C-817/19 to assess the conformity of the PNR Law with the Charter. In doing so, the Court

[66]*Id.*

[67]*Id.* at para 210.

[68]Regulation 2016/399 of the European Parliament and of the Council of March 9, 2016, A Union Code on the Rules Governing the Movement of Persons Across Borders (Schengen Borders Code), as amended by Regulation 2024/1717 of the European Parliament and of the Council of June 13, 2024 (EU), 2024 O.J. (L 1717) art. 23 (EU).

[69]*Id.* at art. 25(a)(5). Schengen Border Code stipulates that if the threat persists, border controls may be prolonged for renewable periods of six months. The maximum duration shall not exceed two years.

[70]*Ligue des droits humains ASBL,* Case C-817/19 at paras. 141–52.

[71]*Id.* at para 288.

[72]*Id.* at para 236.

[73]*Id.* at para 171.

[74]*Id.* at para 172.

[75]*Id.* at para 174.

[76]*See* Council Directive 12856/22, Improving compliance with the judgment in case C-817/19 – comments from Member States, 2022 LIMITE, (available at https://www.statewatch.org/media/3701/eu-council-pnr-judgment-ms-comments-12856-22.pdf).

annulled certain provisions of the PNR Law, limited the scope and the purposes of the measure, and prohibited the PIU's use of artificial intelligence technologies in machine learning systems, which could modify the evaluation process without human intervention and control. It also required the authorization of an independent supervisory authority to allow the competent services to access the data.

Nevertheless, the Constitutional Court ruled that the PNR system in Belgium could be extended to intra-EU flights as well as to various means of transport if national authorities demonstrated a real and present terrorist threat. In October 2023, the *Organe de Coordination pour l'Analyse de la Menace* (OCAM) (Authority for the Coordination of Analysis of Threats) reported a general threat level of 2 out of 4 in Belgium. Level 2 constitutes a "medium" threat level which the Constitutional Court considered as sufficient for extending the application of the PNR system to intra-EU flights and other means of transport. In addition, according to the Constitutional Court:

> [I]n assessing the reality of this threat, account should also be taken of the geographical situation of the country, which has a small territory and easily crossed borders, is located at the center of Europe and is home to numerous European and international institutions. This geographical reality, which is characteristic of the country, significantly increases the risks of using all modes of transport via Belgium to commit terrorist offences or serious crime. The country is thus geographically located at the intersection of multiple air, rail and road transport routes that could be used by terrorist and criminal organizations to commit terrorist offences or serious forms of crime.[77]

As a result, while the CJEU had categorically limited the PNR system, the Constitutional Court stepped into the breach, leaving new doors open to the Belgian legislator.

Following the decision of the Constitutional Court, an initial bill aimed at amending the PNR law as little as possible was tabled[78] and adopted on May 16, 2024, by the Belgian Parliament.[79] The legislator referred to the emergency of the situation and the difficulties experienced by the competent authorities—particularly in the Public Prosecutor's Office—in carrying out ad hoc searches and accessing the PNR database.[80] In accordance with the aforementioned Constitutional Court ruling, the text limits the purposes by removing the possibility of processing the data for border control purposes.[81] Access to the data is possible in the event of an offense having an objective direct or indirect link with international transport.[82] The conditions for accessing the data have been clarified and are now subject to authorization by the investigating judge.[83]

Given the real and present terrorist threat, the scope of the measure is particularly broad, with the PNR system being applied to intra-EU flights. However, a reassessment of the threat must be organized every three years by an independent judicial or administrative authority.[84] However, this period is particularly long given that the threat is regularly re-evaluated by the OCAM on the

[77]CC [Constitutional Court], Oct. 12, 2023, n °131/2023, B.40.2.2., https://www.const-court.be/public/f/2023/2023-131f.pdf.

[78]Proposal for a law amending the Act of December 25, 2016 on the processing of passenger data, *Ch. rep.* sess. 2023–2024, Doc. 55 3871/002, https://www.lachambre.be/FLWB/PDF/55/3871/55K3871001.pdf.

[79]Loi du 16 mai 2024 modifiant la loi du 25 décembre 2016 relative au traitement des données des passagers, M.B. (July 5, 2024), https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=24-07-05&numac=2024006174.

[80]Proposal for a law amending the Act of December 25, 2016, *supra* note 76, at ¶ 5.

[81]Law of May 16, 2024, *supra* note 79, at art. 8, § 1.

[82]*Id.* at art. 15.

[83]*Id.*

[84]*Id.* at art. 12.

basis of current events. According to the legislator, it is also the existence of the threat that justifies the retention of all the passengers' data for five years.[85] After a period of three years, if the circumstances are no longer present, a six-month retention period will have to be introduced.[86] The circumstances would allow a link to be established between the objective pursued and the retention of the data. Because the ECJ has limited the period of data retention to individual circumstances, critics emphasize this makes it possible to establish a link between the retention of the data and the objective pursued.[87]

In addition, regarding the purposes pursued and the concept of serious crime, the legislator considers that "ordinary" offenses may be targeted as long as they meet the three-year penalty threshold—which will depend on the circumstances of the case. Accordingly, the legislator considers that it is not possible to draw up an exhaustive list of the offenses provided for in national law that fall *a priori* within the scope of serious crime as defined by the Directive, and provides that this list will have to be set out in a Royal Decree to be reviewed.[88] In so doing, the legislator entrusts the Executive with the task of determining which offenses are to be classified as serious offenses. But such elements should have been laid down in the law because the principle of formal legality is enshrined in Article 22 of the Constitution.

F. Conclusion

At a time when the European Union just adopted a regulation on artificial intelligence,[89] we can welcome the CJEU's ban on self-adapting algorithms in the fight against serious crime and terrorism because of the difficulty for the individuals concerned to benefit from an effective remedy. This decision may have an impact on other measures such as the ETIAS regulation[90] or the European Commission's proposal for a regulation to combat child pornography (CSAM).[91] On this point, however, some authors wonder whether the CJEU might not authorize the use of artificial intelligence in the case of transparent algorithms involving human intervention.[92] However, it is highly regrettable that the CJEU overlooked the ineffectiveness of the measure due to the false positives it generates and the difficulty of developing algorithms that do not lead to discrimination.[93] Be that as it may, this PNR ruling is undoubtedly the first of many in Belgium.

[85]Proposal for a law amending the Act of December 25, 2016, supra note 76, at ¶ 5.

[86]*Id.* at ¶ 6.

[87]*Ligue des droits humains ASBL,* Case C-817/19 at para. 261.

[88]Law of May 16, 2024, supra note 79, at art. 8, § 3.

[89]European Parliament and European Council Regulation 2024/1689 of June 13, 2024, Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L 1689) 1–144 (EU).

[90]European Parliament and European Council Regulation 2018/1240 of September 12, 2018, Establishing a European Travel Information and Authorization System (ETIAS) and Amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, 2018 O.J. (L 236) 1–71 (EU).

[91]Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse, COM (2022) 209 final (May 11, 2022).

[92]Christian Thönnes, *A Directive Altered Beyond Recognition*, VERFASSUNGSBLOG (June 23, 2022), https://verfassungsblog.de/pnr-recognition/; Douwe Korff, *Opinion on the Implications of the Exclusion of New Binding European Instruments on the Use of AI in Military, National Security and Transnational Law Enforcement Contexts*, *European Centre for Not-for-Profit Law* (Oct. 2022), https://ecnl.org/sites/default/files/2022-10/ECNL%20Opinion%20AI%20national%20security_0.pdf; Elif Mendos Kuşkonmaz, *The Grand Gala of PNR Litigations: C-817/19 Ligue des droits humains v Conseil des ministers*, 19 EUR. CONST. L. REV., 294–319 (2023).

[93]Douwe Korff, *Did the PNR Judgment Address the Core Issues Raised by Mass Surveillance?*, 29 EUR. L. J. 1–2, 223–26 (2023).

We can only hope that the Court will continue to specify its strict conditions. For LDH, the next action against the new law is currently being drafted.

Acknowledgement. We gratefully acknowledge helpful comments from Marta Morvillo and Stefan Salomon; remaining errors are, as always, solely the responsibilities of the authors.

Funding Statement. No specific funding has been declared for this Article.

Competing Interests. The authors declare none.

Cite this article: Forget C (2024). A Challenge to Systematic and Undifferentiated Data Collection Through Strategic Litigation: The *Passenger Name Record* Case (Ligue des Droits Humains) Before the Court of Justice of the EU. *German Law Journal* **25**, 1068–1079. https://doi.org/10.1017/glj.2024.60