*European Papers – A Journal on Law and Integration*
Vol. 11, No. 1, 2026, pp. 533–561

***The Future of Digitalisation in EU Law Enforcement***
***edited by*** **Niovi Vavoula**

# The Never-Ending Story of PNR Profiling and Surveillance of Movement in the EU

*Elif Mendos Kuşkonmaz*[*]



ABSTRACT: Using Passenger Name Record (PNR) in law enforcement has a tumultuous history. Acquired initially by the commercial aviation sector, PNR is repurposed to be fed into automated systems that aim to detect behaviours associated with criminal activities and target air travellers, identifying them as 'risky' individuals. This automated process raises several questions, such as how those systems create the subjects they will govern (i.e., 'risky' travellers), the accountability and the implications of the automated process on fundamental rights. This article focuses on the decades-long controversy surrounding the emergence of PNR data processing in the law enforcement context that has culminated in the EU PNR Directive. It considers the political and legal background of the Directive and analyses the changing legal landscape based on the legal challenges against it, the first of which is *Ligue des droits humains*, delivered in June 2022.

KEYWORDS: passenger name record – profiling – law enforcement cooperation – privacy – data protection – oversight.

## 1. Introduction

The story of the legislative and political background of the EU Passenger Name Record (PNR) Directive can be told from several angles.[1] But the story that this article

[*] Lecturer in Law, City St. George's, University of London, elif.kuskonmaz@city.ac.uk.

[1] Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of

ISSN 2499-8249
doi: 10.15166/2499-8249/882
www.europeanpapers.eu

aims to tell relates to the place of the Directive in the EU's Area of Freedom, Security and Justice (AFSJ) policy areas to resort to large-scale databases to trace cross-border movement.[2] For some of the databases, the EU derived its competence from policies on border checks, asylum, and immigration.[3] For a few (e.g., the EU PNR Directive), it relied on its competence in the police and judicial cooperation in criminal matters.[4] While these areas are separate, scholars have identified a close connection between them as the coverage of the databases crossed these seemingly separated policy areas, yielding expanded access and data processing competencies to law enforcement and security agencies.[5]

Thinking of the PNR schemes within this framework means positioning them as part of the ongoing process of securitisation that shifts border and migration governance into the security domain.[6] The legal implications of this shift have been introducing law enforcement aspects to the databases initially set out for border control and immigration-related purposes and triggering EU competence on external border controls to govern human mobility through automated systems set up to conduct risk profiling.[7] These developments redefine the understanding of border controls that defy their spatial feature with the help of collecting and sharing information relating

terrorist offences and serious crime; J Argomaniz, 'When the EU is the "Norm-Taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms' (2009) 31 *Journal of European Integration* 119; J Faull, 'The Role of the European Commission in Tackling Terrorism: The Example of Passenger Name Records' in A Arnull, C Barnard, M Dougan and E Spaventa (eds), *A Constitutional Order of States? Essays in EU Law in Honour of Alan Dashwood* (Hart Publishing 2011) 609, 616; E Fahey, 'Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program' (2013) 32 *Yearbook of European Law* 368; M Tzanou, *The Fundamental Rights to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017).

[2] J Jeandesboz, 'EU Home Affairs and Technology: How to Make Sense of Information and Data Processing' in A Ripoll Servent and F Trauner (eds), *The Routledge Handbook of Justice and Home Affairs Research* (Routledge 2018) 180; E Brouwer, 'Private Life and Data Protection in the Area of Freedom, Security and Justice' in S Iglesias Sánchez and M González Pascual (eds), *Fundamental Rights in the Area of Freedom Security and Justice* (Cambridge University Press 2021) 373.

[3] Arts 77-80 TFEU.

[4] Arts 82-89 TFEU.

[5] D Bigo, S Carrera, B Hayes, N Hernanz and J Jeandesboz, 'Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals' (CEPS 52-2012), at www.ceps.eu.

[6] E Guild, *Security and Migration in the 21st Century* (Polity 2009).

[7] D Dimitrova, 'Surveillance at the Borders: Travellers and Their Data Protection Rights' in G González Fuster, R Van Brakel and P de Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2022) 303.

to individuals who aim to cross borders.[8] As border and immigration controls remain framed within the security logic, the actors involved in using databases vary from border control authorities to police and intelligence agencies.[9]

The legal and policy developments in creating a PNR scheme are closely associated with this security framework. PNR schemes were seen as the epitome of the surveillance of movement through conducting risk assessment, whereby people are sorted into categories based on their travel patterns and behaviours when they intend to cross borders.[10] In this context, surveillance is construed as the collection of wide-ranging information about individuals and the increased mode of identifying and tracing them in connection with their acts or intention of border crossing. But this is carried out by pursuing the objectives of the fight against terrorism and serious crime, raising the issue of the extent to which the practices of security are intertwined with border control practices and the implications of the relationship between those practices on protecting individuals' fundamental rights. The surveillance of movement through the EU PNR Directive thus raises acute issues on the observance of Charter rights, including the right to privacy, data protection, as well as freedom of movement in pursuance of border control purposes on the one hand and law enforcement purposes on the other. Furthermore, interventions by the CJEU on the permissibility of untargeted data retention and processing and, most recently, automated analysis require the reassessment and redesign of the EU legislative framework on PNR processing.

This article will critically discuss the EU PNR Directive in light of the CJEU case law on data retention and automated personal data processing. Section 2 provides a backdrop of the EU PNR Directive and its provisions but only so far as is necessary to set the scene for the following three central questions on the future of PNR schemes at the EU level. First, when would the extensive use and collection of data be deemed proportionate for the risk assessment feature of PNR schemes, and which authorities can obtain and process the data based on the close connection with border crossing and security practices (Section 3)? The second question is whether automated PNR profiling is permissible under EU law (Section 4). Finally, against the complex assemblages of authorities with powers to process PNR data and the

[8] V Mitsilegas, 'The Law of the Border and the Borders of Law: Rethinking Border Control from the Perspective of the Individual' in L Weber (ed), *Rethinking Border Control for a Globalising World* (Routledge 2015) 15.

[9] D Bigo, 'The (In)securitization Practices of the Three Universes of EU Border Control: Military/Navy – Border Guards/Police – Database Analysts' (2014) 45 *Security Dialogue* 209.

[10] D Lyon, 'Surveillance as Social Sorting: Computer Codes and Mobile Bodies' in D Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003) 13; V Mitsilegas and N Vavoula, 'The Normalisation of Surveillance of Movement in an Era of Reinforcing Privacy Standard' in P Bourbeau (ed.), *Handbook on Migration and Security* (Edward Elgar Publishing 2017) 232.

different features of PNR schemes, from automated profiling to the subsequent access to the retained data, the third question this article aims to answer is designating authorities responsible for the oversight of PNR processing and fundamental rights safeguards.

## 2. The EU PNR Directive: a historical background and main elements

As a technical term covering different types of information commercial airline companies collect about their customers, the travel sector used Passenger Name Record (PNR) data for their business practices and interests before they became closely associated with counter-terrorism. When the United States of America (US) redesigned its counter-terrorism policy after the 9/11 attacks to harvest information in connection with electronic communications, financial transfers, and travel to 'pre-empt' terrorist activities, the travel sector gained a rival with an interest in using PNR data.[11] The US government changed what used to be a voluntary scheme into an obligatory one by mandating commercial airline companies to hand over PNR data when they operate flights to and from the US, even if they might be based outside the US. Thus, at the level of the EU, PNR data were first associated with the conflict of laws between the relevant US law and EU data protection legislation.[12]

Soon, the discussion morphed into needing an internal EU PNR scheme.[13] The 2004 Madrid attacks[14], followed by the revamping of the Justice and Home Affairs policies in the Hague Programme[15], heightened the talks for the EU to intervene in setting up harmonised rules on processing PNR data.[16] These talks were materialised in a draft Framework Decision based on the EU's competence in the now-abolished third pillar.[17]

[11] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States (2004) govinfo.library.unt.edu; E Bentley, 'Homeland Security Law and Policy' in KG Logan and JD Ramsay (eds), *Introduction to Homeland Security* (Westview Press 2012) 19, 24.

[12] E Guild and E Brouwer, 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US' (CEPS 109-2006) www.ceps.eu; P de Hert and R Bellanova, 'Transatlantic Cooperation on Travellers' Data Processing: From Sorting Countries to Sorting Individuals', (2011) *Migration Policy Institute*, www.migrationpolicy.org.

[13] European Commission, 'Communication: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach', COM(2003) 826 final.

[14] Note from the General Secretariat 7906/04 of the Council of the European Union of 29 March 2004 'Declaration on combating terrorism'.

[15] Council of the European Union, 'Communication: The Hague Programme: strengthening freedom, security and justice in the European Union' (2005/C 53/01), 3 March 2005.

[16] C Blasi Casagran, 'The Future EU PNR System: Will Passenger Data be Protected?' (2015) 23 *European Journal of Crime, Criminal Law, and Criminal Justice* 241.

[17] Proposal for a Council Framework Decision from the Commission of 6 November 2007 on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final.

The legal landscape of the EU PNR scheme continued to be shaped by the changes to the institutional framework of the AFSJ[18] and the reactionary political responses to the terrorist attacks on the Member States.[19] The 2015 terrorist attacks in Paris were the last straw for the EU actors to hasten the legislative process to adopt a secondary EU legislation on PNR processing, despite the growing fundamental rights concerns over the previous and existing proposals on the topic.[20] Thus, almost one year after the attacks that triggered the process, a Directive on the processing of PNR data for the fight against terrorism and serious crime, the EU PNR Directive, was adopted in April 2016 with an implementation due date of May 2018.

In brief, the Directive sets out the harmonisation rules for the Member States' national PNR schemes, given that they retain the mandate to receive and process PNR data. Their legal mandate to receive the data covers only flights to and from the Member States. Still, they have the option to introduce obligations for commercial airline companies to share PNR data for flights between the Member States.[21] In either circumstance, the companies share the data with the national Passenger Information Unit (PIU) designated by the national law to carry out the main data processing activities, including the automated analysis of the data as part of the prescreening of incoming passengers[22], communicating the result of the analysis with the relevant national authorities[23], sharing the retained data with the competent authorities and Europol when requested[24], and creating new criteria to execute algorithms as part of the automated data analysis.[25] These processing activities can take place for preventing, detecting, investigating, or prosecuting terrorist offences (as defined under EU law[26]) and serious crimes that are either from the list of crimes

[18] Proposal for a Directive of the European Parliament and of the Council of 2 February 2011 on the use of Passenger Name Record Data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final.

[19] Conclusions EUCO 163/14 of the European Council of 30 August 2014 Special Meeting of the European Council.

[20] Conclusions 14382/15 of the European Council of 20 November 2015, Outcome of the Council Meeting – Justice and Home Affairs; European Data Protection Supervisor, Opinion 5/2015 - Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes of 24 September 2015, at edps.europa.eu.

[21] Directive 2016/681/EU (n 1) Art 2. See also Section 3.1. of this article.

[22] Ibid Art 6(2).

[23] Ibid Arts 6(2)(a) and 6(6).

[24] Ibid Art 6(2)(b).

[25] Ibid Art 6(2)(c).

[26] Directive 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Art 3.

provided by the Directive or punishable with a maximum of three years imprisonment.[27] Once the national PIUs receive the PNR data, they can be retained in a database for five years. The full data would be accessible for the initial six months and be depersonalised for the rest of the retention period.[28]

Since the legislative initiatives to establish harmonisation rules for PNR processing began, there have been significant concerns about the implications of this processing activity on individuals' rights to privacy and data protection.[29] The series of preliminary ruling requests questioning the compatibility of the EU PNR Directive with EU law are quintessential examples of the lack of confidence that the legislation observes the Charter requirement.[30] In June 2022, the Court of Justice of the European Union (CJEU) gave its first findings on the topic in *Ligue des droits humains*.[31] In this detailed and politically salient decision, the Court gave a Charter-compliant reading of the EU PNR Directive with significant ramifications for the future of PNR schemes in the EU. The following sections consider the EU PNR Directive and its implementation post-*Ligue des droits humains* in three main areas: *i)* the question of seeing PNR schemes as tools for border controls or law enforcement cooperation to justify extensive use of data; *ii)* the judicial interpretation of the automated analysis of PNR data through the implementation of algorithmic solutions; and *iii)* the question of finding an oversight authority within the complex assemblages of actors with interests in obtaining the data.

[27] Directive 2016/681/EU (n 1) Art 3(8)-(9).

[28] Ibid Art 12(1)-(2).

[29] V Mitsilegas, 'Extraterritorial Immigration Control in the 21st Century: The Individual and the State Transformed' in B Ryan and V Mitsilegas (eds), *Extraterritorial Immigration Control: Legal Challenges* (Brill/Nijhoff Publishers 2010) 38; P de Hert and V Papakonstantinou, 'The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe', (2010) 26 *Computer Law & Security Review* 368; F Boehm, 'EU PNR: European Flight Passengers under General Suspicion – The Envisaged European Model of Analyzing Flight Passenger Data' in S Gutwirth, Y Poullet, P de Hert and R Leenes (eds), *Computers, Privacy and Data Protection: an Element of Choice* (Springer 2011) 171; S Roda, 'Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union' (2020) 6 *European Data Protection Law Review* 66.

[30] Case C-148/20 *AC v Deutsche Lufthansa AG*, pending; Case C-149/20 *DF v Deutsche Lufthansa SA*, pending; Case C-150/20 *BD v Deutsche Lufthansa SA*, pending; Case C-215/20 *JV v Bundesrepublik Deutschland*, pending; Case C-222/20 *OC v Bundesrepublik Deutschland*, pending; Case C-486/20 *Varuh človekovih pravic Republike Slovenije*, pending.

[31] Case C-817/19 *Ligue des droits humains v Conseil des ministres* EU:C:2022:491.

## 3. PNR profiling as a measure of law enforcement cooperation *stricto sensu* or border control

As mentioned above, the unique feature of PNR data is that they are collected directly in connection with individuals' acts or intentions of border crossing. Within a PNR regime established for security purposes, the PIUs receive the data *en masse* for the inbound and outgoing flights to the EU (i.e., extra-EU flights) when passengers declare their intention to cross borders through check-in. There is thus a close association between the borders crossing and the generation of these types of data. Still, the EU's competence in designing the relevant rules on PNR processing is carved out of the law enforcement cooperation framework to mandate commercial airline companies to hand over the data. When the initiatives to provide harmonised rules on PNR processing started to emerge in the early 2000s, the proposed legal instrument was formed within the EU's competence on measures concerning police and judicial cooperation in criminal matters under the now-abolished third pillar, despite the problems associated with the scope of the secondary data protection legislation governing the processing of data in the law enforcement context.[32] The 2011 legislative initiative focused on the EU's law enforcement and judicial cooperation.[33] It remained the focus of the EU PNR Directive, whose legal bases rest on Articles 82(1)(d) and 87(2)(a) TFEU governing the EU competence on judicial cooperation in criminal matters and law enforcement cooperation, respectively.[34]

However, PNR processing as prescribed by the EU PNR Directive is not limited to law enforcement cooperation in *stricto sensu*, whereby the competent authorities exchange information and coordinate their coercive powers concerning a potential criminal investigation. Instead, a stand-out aspect of PNR processing is the ability to conduct pre-screening of individuals based on (unknown) risk categories because of

[32] The main issue was that the data protection legislation governing personal data processing for law enforcement purposes set out rules and obligations where the data are shared between competent law enforcement authorities. Proposal for a Council Framework Decision COM(2007) 654 (n 17). On the questions regarding the applicable data protection legislation, see European Data Protection Supervisor, Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes of 20 December 2007 edps.europa.eu.

[33] Proposal for a Directive COM(2011) 32 (n 18).

[34] Notice here that the EU legislator did not rely on its competence in data protection under Art 16 of the TFEU. In this way, the law enforcement aspect of the PNR processing rather than its implications on individuals' right to personal data protection is prioritised. The CJEU considered in Opinion 1/15 that the different procedural frameworks applicable to the EU's competence in law enforcement and judicial cooperation on the one hand, and personal data protection on the other could be reconciled. Based on the content and aim of the draft agreement that it asked to review, the CJEU concluded that the international agreement should have been based on Art 87(2)(a) TFEU and Art 16 TFEU. See: Opinion 1/15 *Accord PNR UE-Canada*, EU:C:2017:592, para 118. See also H Hijmans, *The European Union as the Guardian of Internet Privacy: The Story of Article 16 TFEU* (Springer International Publishing 2016).

the premise of automated data processing to reveal mobility patterns. Given that the PNR regimes are inherently linked to the capacity of the data to be used in connection with the border control proceedings, the question remains on the extent to which border control is a relevant purpose for the operation of these regimes, despite what the legal bases of the EU PNR Directive suggest.[35] To answer this question, this section considers the role of PNR data as part of this pre-screening activity, as prescribed by the Directive and its Charter-compliant reading by the CJEU (Section 3.1), the actors involved in the processing and exchange of the data (Section 3.2), and the comparison of the PNR schemes with the other schemes involved in the data sharing for border control purposes (Section 3.3).

## 3.1. The 'pre-screening' purpose of PNR processing

The EU PNR Directive mainly governs PNR processing in connection with extra-EU flights to fight terrorism and serious crimes. However, it also gives discretion to the Member States to extend data processing to flights between the Member States (i.e., the intra-EU flights) in accordance with the rules applicable to the processing of extra-EU flights. Each scope of data processing bears unique issues with the inherent connection of PNR data with border crossing. For processing in connection with the extra-EU flights, the scheme's legality depends on where the PNR scheme sits within the other databases used in EU external borders, given that its processing must be strictly limited to the fight against terrorism and serious crimes. The legality of the PNR schemes for intra-EU flights resurrects issues with the extent to which the restrictions on the freedom of movement can be justified under EU law. The following sections discuss those issues, focusing on the judicial interpretation in *Ligue des droits humains*.

### *3.1.1 PNR processing for the extra-EU flights*

There is a complex legal regime governing the management of the EU's external borders, with specific rules on entry conditions and border control checks for the beneficiaries and non-beneficiaries of free movement, and comprising measures of migration, asylum, and visa policy on the one hand, and the police and judicial cooperation

[35] The choice of the legal basis for EU measures must be based on objective factors, including the aim and content of the measure. Where the measure pursues a 'twofold purpose', it must be based on a single basis if one of the purposes is merely incidental. Where the purposes are indissociably linked, the measure must be based on the various corresponding legal bases. Case C-94/03 *Commission v Council*, EU:C:200:2, paras 34-36. This article does not intend to challenge the legal basis of the EU PNR Directive and instead to consider the implication of the pre-screening activity in determining the proportionate PNR processing in light of the public security aim pursued through border control proceedings.

in criminal matters on the other.[36] The question in this context is the role of PNR processing in border checks carried out at the external borders in light of the stated counter-terrorism and serious crime-related purpose under the EU PNR Directive.[37] If PNR processing does not pursue a 'border control' purpose, it cannot be used to consider whether the incoming passengers satisfy the conditions for crossing external borders. On this issue, the CJEU explicitly rejected using PNR data 'to improve border controls'.[38] But at the EU level, the purpose of border control is to prevent threats to the internal security of the Member States.[39] Where PNR data are processed automatically for the pre-screening of incoming passengers to detect 'unwanted' individuals, the distinction between data processing purposes of border control on the one hand and the fight against terrorism and serious crime on the other becomes less clear because the former is not merely incidental to the latter. Instead, a 'border security' logic emerges as responses to border crossing shift from administrative to security actions.[40] Thinking about PNR processing at this intersection is a complex equation that involves determining how much this indiscriminate PNR processing is proportionate to the 'greater' security purpose.

The starting point is the judicial interpretation of the purpose of PNR processing in connection with the pre-screening of incoming passengers. In Opinion 1/15, the CJEU upheld the EU-based air carriers' indiscriminate transfer of PNR data to Canada. A greater volume of data would achieve a better pre-screening of incoming passengers based on the security risk they pose to the country.[41] It further reiterated the same finding, but this time in connection with the PNR processing for the extra-EU flights in *Ligue des droits humains*.[42] If not for the indiscriminate PNR data sharing of extra-EU flights, public security could not be achieved because any requirement to target the

[36] M Fink and JJ Rijpma, 'The Management of the European Union's External Borders' in E Tsourdi and P De Bruycker (eds), *Research Handbook on EU Migration and Asylum Law* (Edward Elgar Publishing 2022) 407. Note here that the application of the EU PNR Directive is not limited to the Schengen States.

[37] Directive 2016/681/EU (n 1) Art 1(2).

[38] *Ligue des droits humains* (n 31) para 288.

[39] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification), Art 6.

[40] V Mitsilegas, 'The Borders Paradox: The Surveillance of Movement in a Union without Internal Frontiers' in HK Lindahl (ed), *A Right to Inclusion and Exclusion: Normative Fault Lines of the EU's Area of Freedom, Security and Justice* (Hart Publishing 2009) 33-~~63~~.

[41] Opinion 1/15 (n 34) para 187 ['As several of the interveners have stated, that processing is intended to identify the risk to public security that persons, who are not, at that stage, known to the competent services, may potentially present, and who may, on account of that risk, be subject to further examination. In that respect, the automated processing of that data, before the arrival of the passengers in Canada, facilitates and expedites security checks, in particular at borders'].

[42] *Ligue des droits humains* (n 31) para 161.

sharing to certain areas or people would make it harder to conduct automated data analysis and detect people who may be liable to present a public security risk.[43] As the aim of the PNR sharing and its real-time processing was set as automated border checks, the Charter rights to privacy and personal data protection could justifiably be limited.[44] In this way, the Court's approach was balancing the rights of an individual against a public interest, which is 'border security', as opposed to balancing the rights of everyone to be free from automated pre-screening activity for the same interest.

However, where the pre-screening involves cross-checking the data against the available databases, the CJEU might seem to limit this activity to the purpose of the fight against terrorism and serious crime. This approach emphasises the capacity of the data to enhance law enforcement cooperation for terrorist offences and serious crimes with a cross-border element. However, the use of various databases in EU external border management and the interaction of PNR processing with those databases once again raises questions on the objective of PNR data processing. The EU PNR Directive was ambiguous about which databases the data may be cross-checked against.[45] The CJEU tried to clarify this issue in *Ligue des droits humains* by giving a Charter-compatible reading of the provisions relating to the features of those databases. It thus limited the databases to those used for the fight against terrorism and serious crime and have a cross-border element.[46] The managing authorities for those databases must have competence for preventing, detecting, investigating, and prosecuting terrorist offences and serious crimes.[47] The CJEU's findings on determining terrorism-related databases are essential in revisiting the Member States' practices with their PNR schemes because cross-checking PNR data with non-terrorism-related databases would be incompatible with the Charter.

A strict reading of this judicial interpretation may suggest that PNR data can be cross-checked with counter-terrorism and serious crime components of Interpol (e.g., the Stolen and Lost Travel Document database) or those of national police databases. Far more contentious is the role of PNR data within the complex structure of the information systems implemented as part of the EU's external border checks, such as the Schengen Information System (SIS), Visa Information System (VIS), and Eurodac. There are growing contentions on the evolving status of the VIS and Eurodac, from migration and asylum databases to intelligence databases, with the

[43] Ibid para 162.

[44] Note there that the CJEU did not make a distinction between the justification analysis of the interference with the Art 7 right enshrining privacy and the interference with the Art 8 right enshrining personal data protection.

[45] Directive 2016/681/EU (n 1) Art 6(3)(a).

[46] *Ligue des droits humains* (n 31) para 191.

[47] Ibid para 189.

legislative changes allowing law enforcement authorities access to these databases.[48] These issues require their fundamental rights analysis in and of themselves, and without diverging too much on the topic, it can be assumed that the outcome of the *Ligue des droits humains* decision might disallow PNR data to be matched with these databases whose initial use concerned management of migration and asylum.[49]

Unlike the VIS and Eurodac, the SIS has a law enforcement aspect because it can contain alerts created by national law enforcement authorities on wanted or missing persons and objects, people sought for criminal activity and those who do not have the right to enter the Schengen area.[50] These alerts and the law enforcement aspect of the SIS have an objective broader than the fight against terrorism and serious crimes. Some of the SIS alerts partly pertain to terrorism and serious crime-related purposes because they include alerts on children who are victims of trafficking or involved in terrorist offences.[51] The inclusion of these purposes largely correlates with the PNR data processing purposes approved by the CJEU in *Ligue des droits humains*, such as trafficking in human beings listed in Annex II as a serious crime and the fight against terrorism.[52] Some SIS alerts, however, do not match the threshold set by the CJEU.[53] National authorities can insert an alert on a person wanted under a European Arrest Warrant (EAW), which can be issued, among other purposes, for offences carrying a maximum of one year imprisonment.[54] The CJEU,

[48] N Vavoula, *Immigration and Privacy in the Law of the European Union – The Case of Information Systems* (Brill/Nijhoff 2022); T Quintel, *Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond* (Hart Publishing 2022).

[49] E Brouwer, '*Ligue des droits humains* and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in Times of New Technologies' (2023) 60 *Common Market Law Review* 839, 853.

[50] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU. See also Vavoula (n 48).

[51] Regulation (EU) 2018/1862 (n 50) Art 32.

[52] *Ligue des droits humains* (n 31) para 149.

[53] Suffice to note here that the European Commission questioned the Member States' practices of running PNR data against the SIS alerts in its 2020 report on the implementation of the EU PNR Directive where the crime-related data processing purposes in PNR schemes on the one hand and the purposes of inserting an SIS alert on the other did not correlate. See European Commission, 'Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the Review of the Directive 2016/681 on the use of passenger name record (PNR) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', SWD(2020) 128 final, 47.

[54] Regulation (EU) 2018/1862 (n 50) Art 26. See also Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States – Statements made by certain Member States on the adoption of the Framework Decision, Art 2(1).

however, had reservations about how the EU PNR Directive defined serious crime based on a maximum of three years imprisonment, which could be deemed ordinary as opposed to serious crimes and could lead to an unjustified interference with the rights to privacy and personal data protection.[55] An offence that is punishable by a maximum of one year imprisonment, as in the case of SIS alerts based on an EAW issued for such an offence, can hardly satisfy the threshold of severity that the CJEU sought in Ligue *des droits humains*.[56] Thus, the interaction between the PNR scheme and the SIS must be revised following this decision. PNR data must be cross-checked with the data contained in the SIS to reach the severity of terrorism and serious crime-related purposes.[57]

### *3.1.2. PNR processing for the Intra-EU flights*

PNR processing has been put forward as an essential feature of law enforcement cooperation in the absence of internal borders.[58] The direction that the Member States take to introduce PNR schemes for intra-EU flights has become a point of contention, especially where it could be argued that those schemes would be considered checks equivalent to border controls, requiring compatibility with the rules on reinstating internal border controls.[59] When those flights were included in the 2011 legislative initiatives to close the security gap[60], the Council Legal Service carefully considered its impact on individuals entitled to free movement.[61] Among the several requirements indicative of police checks as opposed to checks equivalent to border controls, the Legal Service focused on the non-systematic feature of the former because the indiscriminate sharing

[55] *Ligue des droits humains* (n 31) para 150. The CJEU did not set the thresholds; instead, it left the matter to the Member States.

[56] Ibid para 151. The Court deferred the question of setting a threshold based on the length of imprisonment as opposed to the inherent nature of the crime in defining serious crimes to the Member States.

[57] Brouwer (n 49) 853.

[58] Proposal for a Regulation of the European Parliament and of the Council of 14 December 2021 amending Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders, COM(2021) 891 final.

[59] J Jeandesboz, '*Ceci n'est pas un controle*: PNR Data Processing and the Reshaping of Borderless Travel in the Schengen Area' (2021) 23 *European Journal of Migration and Law* 431.

[60] Proposal for a Council Framework Decision 16457/08 of 28 November 2008 on the use of Passenger Name Records (PNR) for law enforcement purposes – Report on thematic work carried out from July to November 2008, 2; Proposal for a Council Framework Decision 9514/1/08 of 29 May 2008 on the use of Passenger Name Record (PNR) for law enforcement purposes – State of Play, 3.

[61] Proposal for a Directive 8230/11 of the European Parliament and of the Council of 28 March 2011 on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime – Possible extension of the scope of the Directive to internal flights between EU Member States – Compatibility with the principle of free movement of persons and the Schengen Borders Code, at www.statewatch.org.

of data in connection with intra-EU flights could undermine observance of this requirement.[62] To mitigate this problem, the Legal Service suggested that the legislator allow the Member States to request PNR data of flights deemed at *risk*.[63] The Legal Service's suggestion was not considered in the final version of the Directive.

The CJEU thus reverted the position to that suggestion because its interpretation of proportionate PNR processing of the intra-EU routes bears an uncanny similarity with the Service's risk-based approach. The Court considered the Member States' optional power in light of the right to free movement based on its observations on limiting access to PNR data in light of the rights to privacy and data protection. In doing so, it created somewhat nuanced yet interrelated requirements for the Charter-compliant application of the Directive to the intra-EU routes. The stand-out condition is the different treatment between the PNR data processing extension for terrorist offences and serious crime based on the interference that either extension causes for the rights to privacy and data protection. Because terrorist offences may lead to greater harm to the stability of a country and its national security interests, they are deemed distinguishable from serious crimes.[64] Thus, if there is a 'genuine and present or foreseeable' terrorist threat, the Member States may extend PNR processing to *all* intra-EU routes.[65] But such an extension must be time-limited and subject to effective review by a court or an independent administrative body.[66] If there is no genuine and present or foreseeable terrorist threat, an indiscriminate extension of PNR processing to all intra-EU routes would be disproportionate to the interests protected by rights to privacy and data protection.[67] Still, the Member States can select specific routes, travel patterns, and airports to obtain PNR data without a terrorist threat, presumably in preventing, detecting, investigating, and prosecuting serious crimes.[68] The Member States must regularly review those selections.[69]

These requirements have disrupted the collection of PNR data relating to all intra-EU flights in the short term. Shortly after *Ligue des droits humains*, the Council initiated discussions with the Member States on implementing the Court's findings.[70] There is a

[62] Ibid 16.
[63] Ibid [Emphasis added].
[64] *Ligue des droits humains* (n 31) para 170.
[65] Ibid paras 171 and 173.
[66] Ibid paras 171–172. See Section 5 of this article.
[67] Ibid para 173.
[68] Ibid para 174.
[69] Ibid para 291.
[70] Note from the Presidency of the Council of the European Union 12856/22 of 27 October 2022 'Improving compliance with the judgment in case C-817/19 – comments from Member States'.

sense of discontent about the selection procedure that most Member States find technically and organisationally challenging.[71] For some Member States, equally challenging is to determine a common terrorist threat threshold to justify the selection.[72] Thus, with many other issues arising from the impact of *Ligue des droits humains* on the Member States' practices of obtaining intra-EU PNR data, some of them called to amend the EU PNR Directive accordingly or to adopt new legislation focusing on the intra-EU PNR data collection.[73] This gradual shift to the mandatory application of intra-EU PNR processing, which was not agreed upon in previous readings of the predecessors to the EU PNR Directive, is highly concerning. The Court's upcoming decisions on the pending preliminary requests on the EU PNR Directive might further elaborate on the requirements it set out in *Ligue des droits humains*, such as the differential treatment of terrorist offences and serious crimes to justify the intra-EU travel processing and what qualifies as an effective review of decisions to extend such processing.[74]

### 3.2. Old friends with new powers: Passenger Information Units

At the heart of the PNR schemes are the PIUs, which are mandated to receive PNR data from commercial airlines and process the collected data. With these PIUs, the Member States retain the power to control the processing of PNR data at the national level. Viewing them as intermediaries between the private sector and the designated competent authorities with whom they share information might be superficial because they refine the raw PNR data obtained by the former to make it intelligible and actionable.[75] Plus, they have to design the pre-determined criteria to execute algorithms, exchange the data and their analysis with the competent authorities, and – as mentioned below, conduct internal revisions about PNR processing. The PIUs' data processing mandate and how they interact with the other PIUs and national authorities are thus important features of the national PNR schemes. In this context, there are several issues on their legal mandate as regards data protection legislation and the broader law enforcement cooperation framework.

[71] Ibid. For example, Cyprus noted that the filtering mechanism proposed by the Council to implement the risk-based approach to intra-EU route selection would amount to data protection in and of itself and the permissibility of this processing must be considered under the secondary EU data protection legislation.

[72] Ibid. For example, Austria rejected the Council's solution to use the TE-SAT as the threshold.

[73] Ibid. For example, Belgium supported the introduction of a new legislative act for the intra-EU PNR collection for the sake of clarity and uniformity.

[74] *AC v Deutsche Lufthansa AG* (n 30); *DF v Deutsche Lufthansa SA* (n 30); *BD v Deutsche Lufthansa SA* (n 30); *JV v Bundesrepublik Deutschland* (n 30); *OC v Bundesrepublik Deutschland* (n 30); *Varuh človekovih pravic Republike Slovenije* (n 30).

[75] G Glouftsios and M Leese, 'Epistemic Fusion: Passenger Information Units and the Making of International Security' (2023) 49 *Review of International Studies* 125.

The first issue is the secondary data protection legislation applicable to the PNR processing alongside the data protection provisions of the EU PNR Directive because different rules apply to data processing in connection with administrative or commercial purposes and law enforcement purposes.[76] As data move from the private sector to the public sector, a fracture in the applicable data protection legislation occurs – commercial airlines (or their commercial intermediaries) are bound by the General Data Protection Regulation (GDPR) when they collect and process PNR data in connection with their business operations.[77] Where they are required to send the data to the PIUs for their subsequent use in the fight against terrorism and serious crime, this raises the long-standing question of their data protection obligations because the 'privatisation' of surveillance in this manner blurs the applicability of the GDPR with a carve-out of processing for public security.[78] In fact, the first time the PNR processing – *albeit* in relation to the international sharing of data to the US authorities – was challenged before the CJEU raised a legal issue on the applicability of the predecessor to the GDPR to this data sharing conducted for security purposes.[79]

The CJEU clarified the GDPR carve-out in *Ligue des droits humains*, where it considered the data protection *lex generalis* applicable to the sharing of data from the private sector to the PIUs and the subsequent data processing by those Units and competent public authorities. The answer to this legal issue turned on designating competent authorities responsible for the transfer within the meaning of the data protection legislation governing the data processing for law enforcement purposes (i.e.,

[76] Different versions of the applicable secondary data legislation question arise in the other AFSJ measures. In the context of the co-operation among the Financial Information Units for anti-money laundering and terrorism financing, a similar grey area concerns the data protection legislation that governs this co-operation among the national Units. See F Mouzakiti, 'Cooperation between Financial Information Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive' (2020) 11 *New Journal of European Criminal Law* 351.

[77] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).

[78] Ibid Art 2(2)(d).

[79] C-317/04 *Parliament v Council* EU:C:2006:346. Note there that the CJEU later diverged from its findings in this decision for the legal dispute concerning the applicability of the EU secondary legislation on the collection of electronic communications data by communications service providers because the carve-out contained therein for national security interests was appliable to those providers. See Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier Ministre and Others* EU:C:2020:791, para 104; Case C-623/17 *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others* EU:C:2020:790, paras 30-49. See also V Mitsilegas, E Guild, E Kuskonmaz and N Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) 29 *European Law Journal* 176.

the Law Enforcement Directive (LED)).[80] Commercial airlines could not be deemed competent authorities because they were not in charge of exercising public authority or were entrusted with public powers, even if the law enforcement purpose for which PNR data may be transferred satisfied the material scope of that data protection legislation.[81] The GDPR would govern PNR data transfer from the commercial sector to the PIUs. However, once the PIUs receive and process the data, they must do so in accordance with their obligations under the LED.[82] The GDPR would apply to the PIUs' processing of PNR data had the purpose of PNR sharing been to improve border controls.[83] The practical implications of the difference in the applicable data protection *lex generalis* are that individuals may have more robust data protection rights under the GDPR as the data moves from the private sector to the PIUs compared to the rights they can claim against the PIUs' data processing under the LED.[84]

Given that the PIUs are deemed competent authorities in preventing, investigating, detecting, and prosecuting terrorist offences and serious crimes within the meaning of the LED, the next question concerns their relationship with the national law enforcement authorities. According to the EU PNR Directive, the PIUs may exchange PNR data with the designated national authorities competent for preventing, detecting, investigating, or prosecuting terrorist offences or serious crimes.[85] However, countering terrorism and serious crimes is a grey area where national security agencies or ordinary law enforcement agencies with national security and intelligence competencies might operate. Border authorities might also be included in the list of agencies competent in this field, depending on the national system. In fact, the Member States' authorities designated to receive and request PNR data are not limited to the police and include immigration and customs authorities and intelligence services.[86]

[80] Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[81] *Ligue des droits humains* (n 31) para 81.

[82] Ibid para 80.

[83] This is by analogy with the CJEU's findings on the data processing under the API Directive. See: *Ligue des droits humains* (n 31) paras 75 and 77.

[84] P Vogiatzoglou, KQ Tavárez, S Fantin and P Dewitte, 'From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives' (2020) 11 *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* 274.

[85] Directive 2016/681/EU (n 1) Arts 6(2)(b) and 7.

[86] Passenger Name Records (PNR) — Competent authorities — List of competent authorities referred to in Directive 2016/681/EU (n 1) Art 7. (This list reflects the authorities entitled, in each Member State, to request or receive PNR data or the result of processing those data from their national Passenger Information Unit (PIU) or for the purpose Directive 2016/681/EU (n 1) Art 9(3) directly from the PIU of any other Member State only when necessary, in cases of emergency. See also European Commission, 'Report

So far as access by intelligence services is concerned, there is a heated debate over the applicability of EU law where the national security interests of the Member States are at stake.[87] For this reason, much attention was paid to the mandate given to these authorities on accessing PNR data in *Ligue des droits humains*. In this instance, the legal dispute did not concern a national security interest. Still, the CJEU seemed to carve out counter-terrorism and serious crime from the broader national security interests and subject the measures implemented for the former to scrutiny.[88] For the Court, the PNR processing purposes for preventing, detecting, investigating, or prosecuting terrorist offences or serious crimes were listed exhaustively in the EU PNR Directive.[89] Thus, granting security and intelligence authorities access to PNR data for national security interests other than the fight against terrorism and serious crime was not permissible under EU law.[90] Any such practice at the national level must cease following the *Ligue des droits humains* decision. PNR data must be separated from the databases that intelligence and security agencies consult for national security purposes other than fighting terrorism and serious crime.[91]

The mandate of border control and customs authorities to access PNR data invokes the complex relationship between border control and law enforcement. When irregular entry into a country is framed as a criminal offence, it seems there is a (controversial) relationship between border control and law enforcement.[92] Boundaries between those authorities to process PNR data for the relevant serious crimes with cross-border elements based on their powers for crime prevention and administrative practices must be defined appropriately because processing data for the latter to regulate entry and exit into the country would be *ultra vires* post-*Ligue des droits humains*. However, delineating the different powers for data processing (i.e., crime prevention v. administrative purposes) has not always been easy given that the EU policy actors and legislators shift the purpose of certain data processing schemes from border control to law enforcement, as in the case of processing of Advanced Passenger Information (API). The following section turns to this issue by comparing the nature of API and PNR and the EU legislative framework on their processing.

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 13.

87 Mitsilegas, Guild, Kuskonmaz and Vavoula (n 79).

88 E Kuskonmaz and E Guild, 'EU Exclusive Jurisdiction on Surveillance related to Terrorism and Serious Transnational Crime, Case Review on Opinion 1/15 of the CJEU' (2018) 43 *European Law Review* 583.

89 *Ligue des droits humains* (n 31) paras 229-233.

90 Ibid para 236.

91 Ibid para 235.

92 V Mitsilegas, *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law* (Springer 2015).

### 3.3. Advanced Passenger Information as the companion to Passenger Name Record

PNR is one of many types of information the commercial air travel sector collects about passengers in connection with their travel. API, an electronic replica of passengers' travel documents and details about their travel itinerary, has generally been compared with its limited capability to detect 'risky' travellers based on automated data analysis compared to the opportunities the automated PNR processing yields. However, API data were not initially associated with their potential use in states' counter-terrorism and serious crime policies. Instead, the commercial airline companies' obligation to collect and share API data with the competent public authorities became prominent at the EU level as those companies were tasked with the border enforcement powers with the air carriers' liability schemes.[93]

The API Directive 2004/82 was thus enacted to provide harmonised rules for the legal obligation of airline companies to share API data with competent public authorities.[94] The objective of this data-sharing obligation is framed as facilitating border controls and combatting illegal immigration.[95] The Member States could mandate that commercial airline operators collect API data and share them with the authorities in charge of border controls by the end of the check-in.[96] Most Member States have designated border authorities as the first recipient of the data, while some also include the national police force as the other recipient.[97] To achieve the objective of border control improvement and illegal immigration prevention, these authorities can use API data to verify the travel documents or the entry entitlement of passengers and cross-check the data with other databases.[98] Unless the authorities need the data to carry out checks at the EU external borders, the operators must delete the data within twenty-four hours after the data sharing.[99]

While the API sharing and processing are enunciated primarily in connection with preventing illegal immigration and improving border controls, the Directive

[93] S Scholten, *The Privatisation of Immigration Control through Carrier Sanctions* (Brill/Nijhoff 2015).

[94] Directive 2004/82/EC of the European Parliament and of the Council of 29 April 2004 on the obligation of carriers to communicate passenger data.

[95] Ibid Art 1.

[96] Ibid Art 3(1).

[97] European Commission, Evaluation on the Implementation and Functioning of the Obligation of Carriers to Communicate Passenger Data set up by Directive 2004/82, 17 September 2012, 42 at home-affairs.ec.europa.eu.

[98] The exact processing activities for which API data can be utilised are not considered in the API Directive. The Directive is seen as part of the Schengen acquis, and thus the data is used to carry out border checks as per Regulation (EU) 2016/399 (n 39) Art 8(2)(a). The identity verification and the cross-checking of databases are mentioned as two means through which API data processing can improve border control and increase the prevention of illegal entry. See European Commission (n 97) 53-54.

[99] Directive 2004/82/EC (n 94) Art 6(1).

gives leeway for the Member States to oblige the operators to share the data for law enforcement purposes.[100] The Directive, however, refers to a broader approach to these purposes with references to enforcing the laws and regulations on entry and immigration, including protecting public policy and national security.[101] In using this discretionary power, the Member States have recognised a range of law enforcement purposes to impose data-sharing obligations, from preventing terrorism and serious crimes to ordinary crimes.[102] Those Member States that have adopted a law enforcement purpose for the API processing use the data they receive in criminal proceedings.[103] In contrast, others implement it in the automated risk assessment analysis to detect routes with a higher risk of irregular migration.[104]

Even though the API data processing purpose was initially framed as border control, the discussions on considering it as a law enforcement tool intensified as API data were seen as a companion to PNR data. When the PNR schemes were discussed at the EU level, the interconnection between API data and PNR data started to emerge because the former was considered an essential part of identity verification to prevent the erroneous detection of risky travellers caused by the unverified nature of the latter.[105] But not all Member States had exercised the law enforcement discretion provided by the API Directive, or where they had done so, they limited data sharing to certain routes.[106] Thus, the EU PNR Directive limited the operators' API data sharing obligations under the EU PNR Directive (presumably where they collect for their business purposes or in accordance with the national legislation implementing the Member States' discretionary power in the law enforcement field[107]) to data that have already been collected.[108] It did not impose additional API data collection obligations upon the operators.

The potential overlap between the EU PNR Directive and the draft proposals revising the API data-sharing rules in the law enforcement context raises acute issues for observing passengers' privacy and data protection rights under the Charter. Based on the current legal framework, the CJEU warned national practices that collect both

[100] Ibid; See also European Commission, 'Commission Staff Working Document Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive)', SWD(2020) 174 final, 26.

[101] Directive 2004/82/EC (n 94) Recital 12.

[102] Staff Working Document Evaluation SWD(2020) 174 (n 100). 50-52; Ibid 12-13.

[103] Ibid 52.

[104] Ibid.

[105] Proposal for a Council Framework Decision 14592/08 of 21 October 2008 on the use of Passenger Name Record (PNR) data for law enforcement purposes General discussion of matters relating to the analysis and transmission of PNR data and data-protection.

[106] Staff Working Document Evaluation SWD(2020) 174 (n 100) 45.

[107] Directive 2016/681/EU (n 1) Recital 10.

[108] Ibid Art 12.

data types in a single database of their incompatibility with the Charter. The data processing purposes under the EU PNR Directive, on the one hand, and the API Directive, on the other, are different. Consequently, the authorities responsible for the data processing and the purposes they can carry out that processing must differ. However, some Member States process API data together with PNR data and mandate their PIUs to carry out that processing.[109] In this overlapping organisational and legal structure exemplified in the Belgian national legislation subject to the preliminary ruling request in *Ligue des droits humains*, the CJEU required differentiating the purposes for which PNR data may be processed on the one hand and API data on the other.[110] Collecting both data types in a single database thus did not conform to the Charter standard of right to privacy and data protection.[111]

With the growing emphasis on verifying the potentially inaccurate PNR data to enhance the added value of PNR schemes in law enforcement, the Member States and EU officials insisted on extending API data sharing to this field.[112] With a mission to streamline the EU PNR Directive with the rules on API data sharing, the European Commission proposed revisions to API Directive to mandate the processing of API data for law enforcement purposes.[113] These revisions were materialised in its proposal for two Regulations on sharing API data for border control purposes[114] and law enforcement.[115] The latter recognises the CJEU's approach in targeting intra-EU flights for which data may be shared. Like the EU PNR Directive, the PIUs are the first point of contact in accessing API data shared by commercial flight operators, but this time, through a router that Eu-LISA manages.[116] On the surface, the router is framed as a

[109] Staff Working Document Evaluation SWD(2020) 174 (n 100) 17-18.

[110] *Ligue des droits humains* (n 31) para 288.

[111] Ibid para 289.

[112] Staff Working Document Evaluation SWD(2020) 174 (n 100) 69; European Commission, 'Communication: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond', COM(2020) 795 final 14.

[113] European Commission, Study on Advance Passenger Information (API) – Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, February 2020.

[114] Proposal for a Regulation of the European Parliament and of the Council of 13 December 2022 on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC, COM(2022) 729 final.

[115] Proposal for a Regulation of the European Parliament and of the Council of 13 December 2022 on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818, COM(2022) 731 final.

[116] Proposal for a Regulation COM(2022) 729 (n 114), Chapter 3; Proposal for a Council Framework Decision COM(2007) 654 (n 17), Chapter 2.

technical solution allowing PIUs to access specific API data while ensuring that commercial airlines are unaware of this confidential information.[117] Under the surface, fundamental rights concerns are ready to erupt. The filtering of flights through the router must meet the targeting standards that the CJEU set out in *Ligue des droits humains*.[118] These standards must be met for the proposed Regulations to be compatible with the Charter. The controversy surrounding the router continues with the applicable data protection legislation, mainly because, as far as the API data processing for law enforcement is concerned, the proposed Regulation, as *lex specialis*, does not set out the data processing rules for the router satisfactorily.[119] There is a fracture in the applicable *lex generalis* on data protection. Eu-LISA manages the processing of *all* API data as the data processor and thus does not satisfy the personal scope required for the applicability of the LED. This means a second legislative fracture occurs as the data moves from airlines to the PIUs at the stage where the (selected) data are processed through the router until the Units access them.

These exemplary issues around the router are among many concerns over the legality of the proposed Regulations under EU law.[120] But for this contribution, I will focus on one aspect of the possible changes for its re-designing of the interaction between the processing conducted for border control and law enforcement. The proposed API Regulation on law enforcement does not address the subsequent use of the data by other public authorities because, according to the European Commission, this is already covered by the EU PNR Directive.[121] The existing practice mentioned above indicates that the competent border authorities are mandated to receive the data where they are shared under the legal route for external border management. A potential legal issue here would be the access by border control authorities to API data for law enforcement purposes when they do not receive the data for that purpose in the first place. This subsequent access would be a breach of Charter rights to privacy and data protection, which require a clear separation between the purposes for which data may be accessed because each access on its own amounts to a rights interference and can only be justified in light of the specific purpose for which the access is granted.

[117] Proposal for a Council Framework Decision COM(2007) 654 (n 17), 11.

[118] See Section 3.1 of this article.

[119] N Vavoula and V Mitsilegas, 'Advanced Passenger Information (API) – An analysis of the European Commission's Proposals to Reform the API Legal Framework' (European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, 8 June 2023) www.europarl.europa.eu 49.

[120] European Data Protection Supervisor, Opinion 6/2023 on the Proposals for Regulations on the collection and transfer of advance passenger information (API) of 8 February 2023 www.edps.europa.eu; Meijers Committee, Comment on the Legislative Proposals Providing for Collection and Transfer of Advanced Passenger Information (API), CM2304, March 2023, www.commissie-meijers.nl; Vavoula and Mitsilegas (n 119).

[121] Proposal for a Regulation COM(2022) 731 (n 115) 10.

## 4. A fundamental right framework for the automated PNR profiling

Section 3 offered an insight into the pre-screening feature of PNR schemes, focusing on using PNR data to reveal matches with existing databases. The other aspect of the pre-screening activity is the simultaneous automated profiling of incoming passengers based on 'the pre-determined criteria', which are essential for components for running algorithms.[122] The system can automatically execute a decision based on those pre-determined criteria introduced in algorithms. The way this automated profiling is regulated in the EU PNR Directive thus becomes a pertinent issue, considering the legal debates on algorithmic solutions' fundamental rights impact, particularly in advancing public security interests.[123]

The Directive explicitly refers to several qualities that the pre-determined criteria must have to provide safeguards against the adverse effects of automated analysis on individuals' enjoyment of fundamental rights. In this regard, the automated analysis 'shall be carried out in a non-discriminatory manner.'[124] There is an explicit prohibition on programming the pre-determined criteria based on individuals' protected characteristics.[125] Those criteria 'must be targeted, proportionate and specific' and must be 'regularly reviewed' by the authorities that can process and access PNR data.[126] Additionally, the EU PNR Directive requires human intervention before formalising a positive match resulting from the automated analysis of PNR data, similar to the prohibition against automated decision-making found in the *lex generalis* data protection legislation.[127]

The provisions on the automated analysis of PNR data bear similarities to the CJEU's interpretation of the same type of analysis prescribed under the draft EU-Canada PNR data sharing agreement in Opinion 1/15. The judicial interpretation of the PNR data analysis in light of the Charter right to privacy and data protection conditioned the justification of that analysis on observing non-discriminatory, reliable, and specific pre-determined criteria.[128] These qualities were later upheld in *La Quadrature du Net*, where the CJEU applied its precedent in Opinion 1/15 to the

[122] Directive 2016/681/EU (n 1) Art 6(3)(b).

[123] P de Hert and V Papakonstantinou, 'Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling' (2015) 6 *New Journal of European Criminal Law* 160.

[124] Directive 2016/681/EU (n 1) Art 6(4).

[125] Ibid.

[126] Ibid Directive 2016/681/EU (n 1) references Art 7 that defines the authorities entrusted with the powers to access PNR data for fighting terrorism and serious crimes. For discussion on those authorities see Section 3.2 of this article.

[127] Directive 2016/680/EU (n 80) Art 11.

[128] Opinion 1/15 (n 34) paras 172-173.

permissibility of the automated analysis of the traffic and location data of users of electronic communications services to detect suspicious patterns and behaviours.[129]

This evolving case law challenged the automated analysis of PNR data under the EU PNR Directive in *Ligue des droits humains*. In summary, the CJEU was satisfied with the safeguards contained in the Directive, and it accompanied them with additional safeguards. First, it recognised that the principle of discrimination covers direct and indirect discrimination, whereby a neutral treatment puts people with the same protected characteristics at a disadvantage.[130] Second, to ensure that the predetermined criteria are reliable to target people who are involved in the commission of terrorist offences and serious crimes, they must apply both 'incriminating' and 'exonerating' circumstances.[131] For example, the PIUs might consider 'the factual conduct of the persons when preparing and engaging in air travel', suggesting that the passenger might have been involved in commissioning those activities based on the findings following the automated analysis and the authorities' experience.[132] When the automated analysis returns with a match, the PIUs can only communicate the analysis results with the competent authorities when they have reasonable suspicion of the individual's involvement in the relevant activities.[133] Moreover, the predetermined criteria must be reviewed to limit their application to the fight against terrorism and serious crime with a cross-border element and to reduce the number of 'false positives'.[134] It is the PIUs' mandate to conduct such revisions of the algorithmic systems in accordance with the clear and precise guidance provided by the Member States.[135] This guidance must involve objective criteria according to which the PIUs can verify that a positive match involves people under reasonable suspicion of

[129] *La Quadrature du Net and Others* (n 79) paras 170-171.

[130] *Ligue des droits humains* (n 31) para 197. The CJEU may have retracted its limited observation in *La Quadrature du Net* that the pre-determined criteria used to execute the automated analysis cannot be based on sensitive data in isolation. See ibid para 181. See also Mitsilegas, Guild, Kuskonmaz and Vavoula (n 79). For a different conceptualisation of 'associative discrimination' to cover the potential discriminatory practices that are not covered by the existing categories of the prohibition against discrimination resulting from implementing algorithmic solutions see C Derave, N Genicot, and N Hetmanska, 'The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System' (2022) 13 *European Journal of Risk Regulation* 389.

[131] *Ligue des droits humains* (n 31) paras 198-200.

[132] Ibid para 200.

[133] Ibid para 204.

[134] Ibid para 201.

[135] Ibid paras 203 and 205.

having involved in terrorist offences or serious crimes and does not yield discriminatory outcomes.[136] They must keep records of the internal review for the subsequent revision by national supervisory authorities.[137]

Another novelty of the CJEU's approach to automated analysis in *Ligue des droits humains* is its recognition of the overlapping issues between the transparency of the pre-determined criteria to execute a decision and the remedial rights of the subject of that decision.[138] The main point of contention was the opacity that transpires from self-learning systems that do not execute decisions based on pre-determined criteria, as the they would train themselves on unlabelled data to extract patterns and draw conclusions. The CJEU dismissed the claim that the PNR processing involved self-learning algorithms because of the explicit reference to the pre-determined criteria found in the Directive, indicating that the PNR scheme is based on algorithmic models involving a set of coded rules designed by human agent rather than of self-learning algorithms.[139] The latter would not be permissible because they would deprive individuals of their right to an effective remedy under Article 47 of the Charter due to their opaque nature.[140]

Recognising the importance of the effective remedy rights allowed the Court to consider the observance of the same rights when rule-based systems such as the PNR schemes are in place. The PIUs and the competent authorities are tasked with a duty to explain to the data subjects how the automated analysis of the data resulted in a particular decision about them without having to unearth the pre-determined criteria and the programs applied.[141] Where the data subject contests the decision through the available channels under the EU PNR Directive, the court hearing the challenge 'must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken … including the pre-determined assessment criteria and the operation of the programs applying those criteria' except in the cases of State security.[142]

The CJEU's interpretation of the Directive provisions on automated processing opens further debates on regulating algorithmic solutions at the EU constitutional level and streamlining the pre-determined criteria among the Member States in light of the

[136] Ibid para 206.

[137] Ibid para 207.

[138] C Thönnes, 'A Directive Altered Beyond Recognition' (Verfassungsblog, 23 June 2022) verfassungsblog.de; EM Kuşkonmaz, 'The Grand Gala of PNR Litigations: Case C-817/19, Ligue des droits humains v Conseil des ministers' (2023) 19 *European Constitutional Law Review* 294.

[139] *Ligue des droits humains* (n 31) paras 194-195.

[140] Ibid para 195.

[141] Ibid para 210.

[142] Ibid para 211.

Court's findings in *Ligue des droits humains*. However, the Member States are sceptical about sharing their risk assessment for administrative and national security reasons.[143]

## 5. Oversight of PNR processing

By prescribing different oversight mechanisms throughout the life cycle of PNR processing, the EU PNR Directive introduces different institutions in the complex institutional assemblages of national PNR schemes. Those mechanisms are a data protection officer to be appointed within each PIUs[144] and a supervisory authority established by the LED.[145] Their status and duties have not raised any particular issues, not least because the Directive either explicitly refers to their independent status (as in the case of data protection officers) or the manner of appointment as laid out in the *lex generalis* on data protection.[146] There were far more disputable instances of monitoring activities, or in the words of the CJEU, 'review' activities that it identified in *Ligue des droits humains*.

The first instance was where the CJEU interpreted the rules on the retrospective access to the PNR data retained by the PIUs. The Directive treats access to data during the first six months of the five-year retention period differently from the remaining period. For six months, starting with the receipt of the data by the PIUs, the competent authorities can request access from the PIU on a case-by-case basis.[147] The Directive does not prescribe a procedure to authorise that request.[148] After this

[143] Presidency of the Council of the European Union (n 70).

[144] Directive 2016/681/EU (n 1) Art 5(1). It is sufficient to note that the Directive uses the terms 'monitoring' and 'supervision' to indicate that an administrative body is entrusted with powers to oversee PNR processing and safeguards.

[145] Directive 2016/681/EU (n 1) Art 15.

[146] Directive 2016/680/EU (n 80) Art 41. The European Commission reported in its review of the EU PNR Directive that some Member States have mandated data protection authorities established under the GDPR to oversee national PNR schemes while others have opted for the authorities they have appointed under the LED. See European Commission, Report COM(2020) 305 (n 86).

[147] Directive 2016/681/EU (n 1) Art. 6(2)(b).

[148] Still, there must be 'sufficient grounds' to process the data for preventing, detecting, investigating, and prosecuting terrorist offences and serious crimes according to Directive 2016/681/EU (n 1) Art 6(2)(b). For the access request post-six-month period, the Directive adds an extra layer of protection and requires a reasonable belief that the data requested is necessary for preventing, detecting, investigating, and prosecuting terrorist offences and serious crime. For the CJEU, a Charter-compliant Directive would require a priori authorisation and the necessity requirement applicable throughout the life cycle of data. For the latter, the CJEU required that access would be permitted where there is 'objective evidence capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air' in relation to serious crimes. See *Ligue des droits humains* (n 31) para 220. For

period, access requests must be authorised by a judicial or another national authority to verify that the disclosure conditions are met.[149] The request is subject to a necessity analysis.[150] The CJEU remedied these different data access rules in *Ligue des droits humains* by rejecting the artificial breakdown of different periods within the overall retention period. It thus required a priori authorisation by a court or an *independent* administrative body throughout the five-year retention period.[151] The next question was what qualities the administrative body designated to authorise the requests must possess in place of a judicial body. This was a central question because some Member States designated the PIUs as the authorising body.[152] At the core of the legal issue lay the independence of those PIUs for access authorisation.

The EU PNR Directive is silent on the qualities of an *a priori* authorisation body to grant access to PNR data other than requiring the administrative body to be independent. When interpreting what independence means in *Ligue des droits humains*, the CJEU relied heavily on its precedent on law enforcement access to electronic communications data. The necessity of a priori review the access requests by a court or an independent administrative body was first enunciated in *Digital Rights Ireland*[153] and reiterated in the subsequent cases concerning data retention.[154] To satisfy independence, the body must carry out its tasks objectively and impartially and be free from external influences.[155] There must be an institutional distance from the authority making the access request. Applying this requirement in the criminal justice field means that the authorising body should not be involved in the criminal investigation and must have 'a neutral stance vis-à-vis the parties to the criminal proceedings'.[156]

Based on that precedent[157] and the observation that the administrative body designated to authorise the access request must have a level of independence similar to

terrorist offences, the CJEU did not enforce a link between the individual concerned and the data requested because it was satisfied that the access would be permissible where objective evidence suggests that the data would contribute to the fight against terrorism. See ibid.

[149] Ibid Art 12(3)(b).

[150] Ibid Art 12(3)(a).

[151] *Ligue des droits humains* (n 31) paras 222-224. [Emphasis added].

[152] Ibid para 238.

[153] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12) EU:C:2014:238 para 62.

[154] Joined Cases C-203/15 and C-698-15 *Tele2 Sverige AB v Post –och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970, para 120; Case C-746/18 *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* EU:C:2021:151. Also see Opinion 1/15 (n 34); Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650.

[155] *Prokuratuur* (n 154) para 53.

[156] Ibid para 54.

[157] *Ligue des droits humains* (n 31) para 244.

the judicial body[158], a PIU that is mandated to process PNR data for criminal proceedings and to authorise retrospective access requests by the other competent authorities in connection with counter-terrorism and serious offences would not entail an independence status.[159] With reference to the criminal justice field, the CJEU seemed to confirm that the PIUs are agencies within the criminal justice system. However, the more immediate effect of the Court's finding is that the Member States that had appointed their PIUs as the authorising body would need to designate a third party that should satisfy the independence status to authorise the data access requests.

The second instance where the CJEU shaped oversight of the PNR scheme was by subjecting the extension of PNR processing to all intra-EU routes for counter-terrorism purposes to effective review by a court or an independent administrative body.[160] Because no such review mechanism existed in the EU PNR Directive, the CJEU did not elaborate on the independence requirement and which type of authority might be the most appropriate review mechanism. However, like in its findings on a priori authorisation, the CJEU relied on its precedent on law enforcement access to electronic communications. The acknowledgements on what qualifies as an independent administrative body – such as its neutrality and institutional detachment from the supervisee – would be required in appointing a body overseeing the extension of PNR processing to all intra-EU routes for terrorism purposes.

Further independence requirements can be traced in the different strands of the CJEU case law that may be influential in redesigning oversight mechanisms. For example, the CJEU's findings on the independent supervision of personal data processing as required explicitly by the Charter can become operational, given that the PNR scheme also involves data processing.[161] The need for such control was a determining factor in declaring the draft legal framework for transferring PNR data from the EU to Canada incompatible with the Charter in Opinion 1/15. In this instance, the supervisory authority was subordinate to the authority receiving the data. It thus failed to comply with the independence requirement in Article 8(3) of the Charter, which explicitly refers to an independent supervisory body.[162] The CJEU reached this decision based on its earlier findings on the status of supervisory bodies required under the relevant Article. Thus, those findings may also be applicable in

[158] Ibid para 243.

[159] Ibid para 245.

[160] Ibid paras 171-172. However, where the Member States apply the PNR processing to selected intra-EU flights, the CJEU does not require a similar review and instead leaves it to the Member States to review the selection regularly. Ibid para 174.

[161] Supervision by data protection authorities on matters relating to the processing of personal data is guaranteed under EU primary law, mainly under Art 8(3) of the Charter and Art 16 TFEU. See also Case C-614/10 *Commission v Austria* EU:C:2012:631, para 36.

[162] Opinion 1/15 (n 34) para 230.

setting out the underlying principles of independence necessary for the PNR schemes in *Ligue des droits humains*.

As a starting point, it was suggested that the level of independence required from the supervisory authorities for personal data processing under Article 8(3) of the Charter comes close to the independence principles needed by the judiciary.[163] This is because the secondary legislation that implements the constitutional principle of supervision refers to the 'complete independence' of the relevant bodies.[164] Thus, the CJEU observed that 'complete independence' required the body to 'act completely freely, without taking any instructions or being put under any pressure'.[165] To act completely freely, the body must be independent from any external pressures, not limited to the pressure from the authority it supervises.[166] Any institutional structure or operational rules exhibiting the risk of 'a priori compliance' of the supervisory authority with its supervisee would be deemed to hinder the independent performance of their tasks.[167]

The CJEU's findings on the independence requirement indicate that in designating a priori body authorising access requests in place of a judicial body and a body to review the PNR processing extension to the intra-EU-flights (albeit only for counter-terrorism purposes) in accordance with the Charter, the Member States must consider several factors, including the operational and institutional detachment of those bodies from the authorities implicated in the activities they are designated to review. An authorisation process internal to the PIU structure or the structure of an existing agency of which the PIU is part will not satisfy the independence requirement for an a priori authorisation process. The same observations can be made for the body reviewing the PNR processing extensions. A single body may be tasked to carry out both types of oversight. However, it must be ensured that the body is independent of the other bodies implicated in data processing in connection with the PNR schemes.

## 6. Conclusion

To detect 'suspicious' travel and disrupt potential cross-border criminal activities, the data captured in connection with travel activities, such as PNR data, have become instrumental in fighting terrorism and serious crime. However, the story of PNR

[163] H Hijmans, 'Article 51. Supervisory authority' in C Kuner, LA Bygrave, C Docksey and L Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 863.

[164] Regulation (EU) 2016/679 (n 77) Art 22; Directive 2016/680/EU (n 80) Art 1.

[165] Case C-518/07 *Commission v Germany* EU:C:2010:125, para 18.

[166] Ibid para 19.

[167] Ibid para 36. See also *Commission v Austria* (n 161) paras 45-46; Case C-288/12 *Commission v Hungary* EU:C:2014:237, para 54.

schemes in EU law is a story of a constant conflict over the justification of the extensive use of data to conduct pre-screening activities in border control proceedings. They involve a complex assemblage of public authorities interested in obtaining the data with multiple layers of rules governing data processing, from automated data analysis to retention of and access to the data. This article considered the EU legislative framework for PNR processing, the EU PNR Directive, based on three prevailing areas: i) determining proportionate PNR processing in light of the pre-screening feature of the schemes at the EU external borders and as implemented for the flights among the Member States; ii) permissibility of automated PNR profiling under the Charter; iii) designating independent authorities to oversee various façades of PNR processing.

The CJEU's *Ligue des droits humains* decision provides essential requirements for redesigning these three areas of the PNR schemes. The Court emphasised the purpose of the PNR processing as that of fighting terrorism and serious crime – thus limiting the application of the PNR schemes only to limited public security threats. At the same time, it recognises a cross-border element that must be observed in counter-terrorism and serious criminal activities. In so doing, the question of differentiating between law enforcement cooperation and border control purposes prevails. As the purposes of the different large-scale databases implemented in the AFSJ start to blur, the risk of using PNR data for border control becomes more significant. Related to this issue is the data processing powers of PIUs seconded from various existing authorities that are competent in a somewhat grey area of counter-terrorism and the potential of *ultra vires* processing of PNR data.

Moreover, the judicial interpretation of the automated PNR profiling will affect how algorithms are reviewed to satisfy the Charter requirements and broader questions on the governance of algorithmic solutions at the EU constitutional level. Finally, the independence of administrative authorities that the CJEU sought in reviewing several decisions of the PIUs and the competent authorities raises another issue in considering the permissibility of the PNR schemes under EU law. The CJEU precedent on this topic requires an arm's length distance from the authorities involved in PNR processing. Overall, *Ligue des droits humains* is the start of a laborious process of redesigning PNR schemes within the EU fundamental rights framework that will continue with more preliminary ruling requests on the EU PNR Directive in the pipeline.