The Grand Gala of PNR Litigations: Case C-817/19, *Ligue des droits humains* v *Conseil des ministers*

Elif Mendos Kuşkonmaz*

*University of Essex, United Kingdom, email: e.m.kuskonmaz@essex.ac.uk

Introduction

In June 2022, the European Court of Justice handed down a judgment, *Ligue des droits humains*,[1] that will open a new chapter in the ongoing discussions on the fundamental rights implications of the extensive use of personal data, including their automated analysis. The subject of contestation in this judgment was the legality of EU secondary legislation, mainly the EU Passenger Name Record (PNR) Directive on processing certain types of information relating to air travel for the fight against terrorism and serious crimes.[2] This information is technically referred to as the PNR. It consists of a digital file that contains various types of information that extend beyond the travel itinerary and the passenger's identity as specified in their travel documents to cover the seat reserved, the weights of the luggage, frequent flyer status, payment details and special requests (e.g. in-flight meal preferences or health assistance). The PNR data are retained in the systems operated by the airlines or companies that enable transactions in the travel sector. In this context, the PNR data were not initially created for counter-terrorism and

[1]ECJ 21 June 2020, Case C-817/19, *Ligue des droits humains* v *Conseil des ministres*, ECLI:EU:C:2022:491.

[2]Directive (EU) 2016/681 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 terrorist offences and serious crime, OJ L 119 (4 May 2016).

European Constitutional Law Review, page 1 of 26, 2023

doi:10.1017/S1574019623000111

serious crime purposes. Instead, the private sector generates and maintains the data.[3]

Over the years, state authorities have grown interested in accessing and using the PNR data. With their potential to unravel passengers' travel behaviours, the PNR data have been associated with pre-emptive counter-terrorism policies since the 9/11 attacks. This is because these data are not simply used to track people sought by public authorities for their involvement in committing criminal offences. Instead, the systems that implement the PNR data processing have been praised for their aid in targeting incoming passengers who allegedly pose a risk to the security of the country they seek to enter based on the automated processing of their data.[4]

The EU PNR Directive, which was subject to a preliminary ruling request in *Ligue des droits humains*, provides the main rules for introducing the PNR processing schemes in the member states' external border controls as part of law enforcement cooperation. In this context, the Directive was criticised for elevating border control and immigration issues to the security domain, resulting in more intrusive fundamental rights infringements in pursuing security interests.[5] Mitsilegas considers the impact of the PNR schemes in flexing the spatial nature of border controls, thus resulting in constant monitoring of incoming passengers through the extensive collection and automated profiling of their

[3]Data collection from the private sector leads to discussions around the privatisation of surveillance. *See* V. Mitsilegas, 'The Privatisation of Surveillance in the Digital Age', in V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart Publishing 2021) p. 101. The privatisation of surveillance in the specific context of PNR data processing raises a question on the multi-layered data protection rules emerging from the EU secondary data legislation applicable to the sharing of data from air carriers to competent national authorities and among those authorities once they receive the data. The ECJ considered that the General Data Protection Regulation captures the former. In contrast, the Law Enforcement Directive captures the latter, which governs data processing for law enforcement-related purposes: *Ligue des droits humains*, *supra* n. 1, paras. 77-81. The immediate result of this finding could be that different standards are applicable to the enjoyment of data protection rights under the respective secondary legislation. *See* P. Vogiatzoglou et al., 'From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives', 11 *JIPITEC* (2020) p. 274; T. Quintel, *Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond* (Hart Publishing 2022).

[4]*See*, for example, European Commission, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final (6 December 2007).

[5]C. Baker-Beall, 'The Threat of the "Returning Foreign Fighter": The Securitization of EU Migration and Border Control Policy', 50(5) *Security Dialogue* (2019) p. 437; E. Orrù, 'The European PNR Directive as an Instance of Pre-emptive, Risk-based Algorithmic Security and its Implications for the Regulatory Framework', 27(2) *Information Polity* (2022) p. 131.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

personal data.[6] According to Mitsilegas, this growing emphasis on risk assessment conducted through automated data analysis introduces intelligence-led practices in border controls.[7] It weakens individuals' fundamental rights due to the generalised profiling of everyone who intends to cross borders, without objective evidence indicating a link between the person concerned and their contribution to the commission of criminal offences.[8] This aspect of the automated PNR data analysis is associated with mass surveillance regimes and the rights-based concerns that arise as a result of their use.[9]

Understanding the context in which the PNR schemes are operated as part of the 'border security' provision is essential when considering the consequent legal issues for the authorities involved (e.g. law enforcement, border control authorities, and customs authorities) in accessing and processing the data. These schemes sit in a grey field where the traditional lines between law enforcement and border control are blurred because, in basic terms, the latter consists of controlling whether an individual satisfies entry conditions.[10] There is thus a greater risk of data misuse related to the long-running question of establishing a review body to oversee how the competent authorities exercise their data processing powers and the qualities that such bodies must satisfy for fundamental rights protection.[11] The automated processing of PNR data raises further fundamental rights issues, as it risks compounding discriminatory practices because it codifies assumptions between personal characteristics and particular risks and weakens the remedial protection due to the opacity and lack of understanding of such automation.[12]

In *Ligue des droits humains*, the European Court of Justice addressed the impact of the automated processing of PNR data as part of pre-screening incoming passengers and the legal accountability of the PNR schemes while analysing the legality of the EU PNR Directive under EU law. This decision is the first of many preliminary requests on PNR processing pending before the

[6]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 2010) p. 39.

[7]Ibid., p. 57.

[8]Ibid.

[9]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 2017) p. 231.

[10]V. Mitsilegas, *EU Criminal Law* (Hart Publishing 2022) p. 586.

[11]T.J. McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective', in M. Scheinin et al. (eds.), *Judges as Guardians of Constitutional and Human Rights* (Edward Elgar 2016) p. 136.

[12]M. Leese, 'The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union', 45(5) *Security Dialogue* (2014) p. 494.

European Court of Justice.[13] It serves as a turning point for the member states to redesign how they process PNR data in light of the EU fundamental rights framework. This case note aims to consider the future ramifications of the Court's *Ligue des droits humains* decision on three critical areas: (i) setting up proportionate PNR schemes implemented for the pre-screening activity; (ii) the Charter standards for the algorithmic decision-making systems; and (iii) introducing an independent body to oversee the compliance of the PNR schemes with the fundamental rights framework. The case note starts with a brief political and legal background of the EU PNR Directive so far as necessary to consider these three areas. It then considers the main points arising from the Opinion of Advocate General Pitruzella and the European Court of Justice's decision of June 2022, followed by main discussion points for those three critical areas. The case note argues that the decision is a turning point for three reasons. First, it set out a constitutional framework for the member states' PNR schemes that must be redesigned, including adopting a targeted approach for extending the PNR processing to intra-EU flights. Second, it provides a *de facto* ban on machine-learning algorithms and sets constitutional standards for algorithmic systems based on pre-determined rules. Finally, it reinforces the independence requirements that a review body must possess.

Background of the EU PNR Directive

The road to enacting the EU PNR Directive has been long and tumultuous. It started when the US government reacted quickly to the 9/11 attacks and adopted policies and legislation to revamp its counter-terrorism practices.[14] A drastic change in this context obliged all commercial air carriers operating US-bound flights to share their PNR data with the then newly formed US border control agency, the Department of Homeland Security.[15] In this way, one of the areas where counter-terrorism operations had been found to lack information was targeted: air travel.[16]

[13]ECJ Case C-148/20, *AC* v *Deutsche Lufthansa AG*, OJ C 279/21; ECJ Case C-149/20, *DF* v *Deutsche Lufthansa SA*, OJ C279/21; ECJ Case C-150/20, *BD* v *Deutsche Lufthansa SA*, OJ C279/22; ECJ Case C-215/20, *JV* v *Bundesrepublik Deutschland*, OJ C 279/27; ECJ Case C-222/20, *OC* v *Bundesrepublik Deutschland*, OJ C 279/30; ECJ Case C-486/20, *Varuh človekovih pravic Republike Slovenije*, OJ C414/24.

[14]R.D. Howard et al. (eds.), *Homeland Security and Terrorism: Readings and Interpretations* (McGraw-Hill Publishing 2006).

[15]Aviation and Transportation Security Act, 49 USC § 44909; 19 CFR § 4.64; and 19 CFR § 122.

[16]The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States' (2004) p. 385, https://www.9-11commission.gov/report/911Report.pdf, visited 21 June 2023.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

The extraterritorial effect of this requirement was imminent since it did not target those air carriers who had retained the data in the US. A conflict of laws thus emerged between US law and EU law because the latter set out restrictive requirements for personal data transfers, which still needed to be observed for the transfers to the US.[17] The air carriers operating in the EU were caught in the middle of this tension and had been given no choice other than to decide which law to disobey. Both sides started to forge a legal solution to break this deadlock, which was materialised into several agreements.[18]

As these events unfolded, the European Commission Communication of 2003 introduced an EU PNR policy that voiced the member states' interests in establishing national schemes to process and analyse the PNR data.[19] Soon, there were concerns over the inefficiency of the schemes, the lack of communication among the member states, and the technical problems should each member state establish their national schemes without the guidance of the EU legislator. Following the calls from the Council of the EU to strengthen border controls through the use of passenger data,[20] the first attempt to provide the EU guidance on PNR data processing came in 2007 with a Commission proposal for a Framework Decision under the now-abolished third pillar.[21] The introduction of the Lisbon Treaty stalled developments in this area until the legislative initiative to establish EU rules on PNR data processing came back in February 2011 as a proposal for a directive.[22] As questions grew over the value of PNR schemes and

[17]E. Guild and E. Brouwer, *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US* (CEPS No. 109 July 2006), https://www.ceps.eu/ceps-publications/political-life-data-ecj-decision-pnr-agreement-between-eu-and-us/, visited 3 June 2023; P. de Hert and V. Papakonstantinou, 'The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe', 26 *Computer Law & Security Review* (2010) p. 368.

[18]The first of these agreements was struck down by the ECJ following concerns over its shortcomings in protecting fundamental rights, and the institutional tensions in the EU: ECJ 30 May 2006, Joined Cases C-317/04 and C-318/04, *European Parliament* v *Council of the European Union and Commission of the European Community*, ECLI:EU:C:2006:346.

[19]Communication from the Commission to the Council and the Parliament, Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, Brussels, 16 December 2003 COM(2003) 826 final.

[20]Note from the General Secretariat of the Council of the European Union 'Declaration on combating terrorism' (7906/04, 29.3.2004); The Hague Programme: strengthening freedom, security and justice in the European Union (2005/C 53/01), OJ C 53, 3 April 2005.

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

[22]European Commission, *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 crime*, COM(2011) 32 final (2 February 2011).

their implications for the exercise of data protection rights,[23] voting on the proposal was suspended until the proposed Directive resurfaced in the wake of the 2015 terrorist attacks in France.[24] After negotiations, in April 2016, the Council adopted the Directive to be implemented by May 2018.

In brief, the Directive provides the harmonisation rules for PNR data processing as the member states establish their PNR schemes. It requires them to designate a Passenger Information Unit to receive the PNR data from air carriers.[25] Each national unit must process the PNR data they received for preventing, investigating, detecting, and prosecuting terrorist offences and serious crimes. This legal mandate consists of automated data processing as part of the pre-screening of incoming passengers to identify those who might need further examination at borders,[26] sharing the retained data with the competent authorities on a case-by-case basis,[27] and updating the pre-determined criteria used to execute automated decisions as part of the pre-screening activity.[28] The EU PNR Directive further provides a five-year data retention period with a stricter access regime for the first six months after the receipt of the data[29] and a list of the PNR data to be transferred to the Passenger Information Units.[30]

From the beginning, the EU intervention in harmonising rules for the PNR schemes has been the subject of criticism from academic circles for the disproportionate interference it causes with the rights to privacy and data protection enshrined in the EU fundamental rights framework.[31] Special attention has been paid to the automated profiling conducted by the PNR data processing that involves a preliminary assessment of the individuals' involvement

[23]E. Brouwer, *Ignoring Dissent and Legality: the EU's Proposal to Share the Personal Data of All Passengers* (CEPS 17 June 2011), https://www.ceps.eu/ceps-publications/ignoring-dissent-and-legality-eus-proposal-share-personal-information-all-passengers/, visited 21 June 2023.

[24]D. Bigo et al., *The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards and EU Security and Liberty Agenda* (CEPS February 2015) https://www.ceps.eu/wp-content/uploads/2015/03/LSE81Counterterrorism.pdf, visited 21 June 2023; N. Vavoula, 'Prevention, Surveillance and the Transformation of Citizenship in the Security Union: The Case Foreign Terrorist Fighters', in U. Sieber et al. (eds.), *Alternative Systems of Crime Control: National, Transnational and International Dimensions* (Duncker & Humblot 2018).

[25]EU PNR Directive, Art. 4.

[26]Ibid., Art. 6(2)(a).

[27]Ibid., Art. 6(2)(b).

[28]Ibid., Art. 6(2)(c).

[29]Ibid., Art. 12(1)-(3).

[30]Ibid., Annex I.

[31]P. de Hert and V. Papakonstantinou, 'The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe', 26 *Computer Law & Security Review* (2010) p. 368; F. Böhm, 'EU PNR: European Flight Passengers under General Suspicion – The Envisaged European Model of Analyzing Flight Passenger Data', in S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: An Element of Choice* (Springer 2011) p. 171.

in committing terrorist offences and serious crimes based on probabilities, thus threatening the presumption of innocence.[32] The European Data Protection Supervisor and the Fundamental Rights Agency echoed concerns over the fundamental rights impact of the extensive use of the PNR data and the automated profiling prescribed in the predecessors to the EU PNR Directive.[33] The debate over the fundamental rights impact of the Directive escalated following Opinion 1/15, in which the European Court of Justice was asked about the Charter compatibility of an international agreement on the transfer of PNR data from the EU to Canada.[34] In this Opinion, the Court laid out the Charter requirements for the PNR data processing in fighting against terrorism and serious crimes, including the extent to which the data may be processed automatically and the existence of an independent body to oversee the competent authorities' exercise of PNR data processing.[35] These requirements have raised questions about how the EU PNR Directive is justified under the EU fundamental rights framework.[36]

Despite these mounting questions on the lawfulness of the EU PNR Directive, the European Commission spoke highly of the results that the PNR systems had produced in achieving EU security in its review of the implementation of the

[32]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', 6(2) *New Journal of European Criminal Law* (2015) p. 160 at p. 163.

[33]EDPS, *Opinion of the European Data Protection Supervisor 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 crime* (25 March 2011) https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_en.pdf, visited 21 June 2023; FRA, *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final),* (14 June 2011), https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf, visited 21 June 2023.

[34]Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592.

[35]For commentaries *see* M. Mendez, 'Opinion 1/15: The Court of Justice Meets PNR Data (Again!)', 2(3) *European Papers* (2017) p. 803; A. Vedaschi, 'The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017', 14 *EuConst* (2018) p. 410; E.M. Kuskonmaz and E. Guild, 'EU Exclusive Jurisdiction on Surveillance Related to Tterrorism and Serious Transnational Crime, Case review on Opinion 1/15 of the CJEU', 43 *European Law Review* (2018) p. 583.

[36]S. Roda, 'Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union', 6 *European Data Protection Law Review* (2020) p. 66. For opposite views, *see* C. Blasi Casagran, 'The Future EU PNR System: Will Passenger Data be Protected?', 23 *European Journal of Crime, Criminal Law, and Criminal Justice* (2015) p. 241; H. Palmer Olsen and C. Wiesener, 'Beyond Data Protection Concerns – the European Passenger Name Record System', 13(2) *Law, Innovation and Technology* (2021) p. 398.

Directive.[37] In parallel, several requests for preliminary rulings on the compatibility of the EU PNR Directive with EU law were made to the European Court of Justice.[38] The *Ligue des droits humains* decision is the Court's first decision on the topic. It arose from an action for annulment that a not-for-profit organisation, Ligue des droits humains, lodged before the Belgian Constitutional Court against the Belgian law transposing the EU PNR Directive. In the proceedings, the Belgian Constitutional Court referred ten questions to the European Court of Justice for a preliminary ruling. In brief, those questions concerned the *lex generalis* secondary data protection legislation applicable to PNR processing (Question 1), the compatibility of the EU PNR Directive with the Charter rights to privacy and data protection, taking into account the broad scope of data to be transferred (Questions 2 and 3), the systematic and continuous PNR data transfer prescribed therein (Question 4), the automated PNR analysis as part of the pre-screening of incoming passengers (Question 6) and the generalised five-year retention period (Question 8); the authority competent to access the retained PNR data (Question 5) and to authorise such access (Question 7).

This case note focuses on these questions so far as necessary to consider the *Ligue des droits humains* decision in light of its ramifications for the proportionate PNR processing for extra- and intra-EU flights, the constitutional framework for automated decision-making systems, and the independence requirement for the body overseeing the implementation of data processing rules.

The Opinion of Advocate General Pitruzella

In his Opinion of January 2022, Advocate General Pitruzzella suggested that the EU PNR Directive be declared compatible with the Charter.[39] The Advocate General raised concerns about some aspects of the Directive, such as the definition of serious crimes in Annex 2[40] and the PNR data categories to be shared with the Passenger Information Units.[41] For this case note, his observations on

[37]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, 24 July 2020, https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_com-2020-305-review_en.pdf, visited 21 June 2023.

[38]*See*, for example, *AC* v *Deutsche Lufthansa AG*; *JV* v *Bundesrepublik Deutschland*, *OC* v *Bundesrepublik Deutschland*.

[39]27 January 2022, Opinion of AG Pitruzzella in Case C-817/19, *Ligue des droits humains* v *Conseil des ministers*, ECLI:EU:C:2022:65.

[40]Ibid., paras. 115-124.

[41]Ibid., paras. 127-150.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

the proportionate PNR processing (e.g. indiscriminate data transfer and automated data processing) and the review body authorising data access are central to comparing the findings of the European Court of Justice.

As regards the former issue, the Advocate General's Opinion must be seen within the broader debate on the applicability of the European Court of Justice's case law on data retention to PNR data processing. Starting from *Digital Rights Ireland*, the European Court of Justice considered the permissibility of communications data retention without any objective evidence indicating the individual's involvement in terrorist offences or serious crimes under EU law.[42] In each preliminary ruling request on the topic, it developed the Charter requirements to justify the data retention, which suggested targeting the retention based on an objective link between the data retained and the commission of terrorist offences or serious crimes.[43] Most of those requirements concerning access to the retained data, the length of the retention period and the existence of a review body for the data access requests were influential in the European Court of Justice's findings in Opinion 1/15 on considering the permissibility of the EU-Canada PNR data transfer under EU law.[44] However, the Court did not apply the targeting requirement to the indiscriminate PNR data transfer. Instead, it distinguished this data transfer by emphasising the states' sovereignty in their border control proceedings (as recognised by the Chicago Convention, which sets out principles about international transport by air).[45] If not for this indiscriminate data transfer, the algorithmically enhanced border security checks performed based on Canada's sovereignty claims over its borders could not detect passengers liable to present a risk to public security.[46]

Based on this precedent, particularly on the European Court of Justice's proportionality finding for the indiscriminate PNR data transfer, the Advocate General rejected limiting the PNR data transfer from air carriers to the Passenger Information Units based on a targeting criterion. In so doing, he acknowledged that in Opinion 1/15, the European Court of Justice recognised the role of automated data processing in facilitating border security checks and the states' sovereign power over prescribing entry and exit conditions.[47] The Advocate General differentiated the PNR processing from the communications data

[42]ECJ 8 April 2014, 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), ECLI:EU:C:2014:238.

[43]ECJ 21 December 2016, Case C-203/15, *Tele2 Sverige AB* v *Post –och telestyrelsen and Secretary of State for the Home Department* v *Tom Watson and Others*, ECLI:EU:C:2016:970, para. 110.

[44]*See*, for example, Opinion 1/15, *supra* n. 34, paras. 140-141, 191-192, 207 and 220.

[45]Ibid., para. 188.

[46]Ibid., para. 187.

[47]Opinion of AG Pitruzzella, *supra* n. 39, para. 193.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

retention measures on two grounds. First, he noted that the PNR data differed from the electronic communications data because the former was limited to certain aspects of travellers' private lives. Access to this type of data would be deemed less intrusive.[48] Second, he considered that the risks associated with accessing communications data were graver than those related to accessing the PNR data because the former was more deeply embedded in the essential foundations of a democratic and pluralistic society for their effect on exercising the freedom of expression.[49]

On the question of the proportionality of the automated processing of the PNR data, the Advocate General was satisfied that the relevant provisions of the EU PNR Directive conform to the Charter requirements, given that they contain safeguards against the solely automated decision-making and lay out the qualities that those criteria must possess.[50] Far more interesting was the Advocate General's reference to the pre-determined criteria to execute the automated processing of the PNR data. He noted that this automated processing does not involve self-learning systems.[51] As discussed below, this will be a crucial point of discussion in the European Court of Justice's decision.

Finally, on the issue of designating a body to authorise the PNR data access requests, the Advocate General interpreted the relevant provisions where that body was referred to as an alternative option in the absence of *a priori* judicial authorisation.[52] This meant that the designated body must observe the independence and impartiality qualities required by a judicial body.[53] Where the member states designated their Passenger Information Units as the authorising body, they would fail to observe those qualities given that the units are involved in criminal investigations and cannot exercise the authorisation powers fully independent of the body making the access requests.[54]

The decision of the Court of Justice

The European Court of Justice delivered its decision on 21 July 2022 and largely followed the Advocate General's Opinion, occasionally directly referring to his findings. The judicial outcome was that the EU PNR Directive survived based on

[48]Ibid., para. 195.
[49]Ibid., para. 197.
[50]Ibid., paras. 223-228 and paras. 229-232.
[51]Ibid., para. 228.
[52]Ibid., para. 267.
[53]Ibid.
[54]Ibid.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

the Court's Charter-compatible reading of its substantive provisions.[55] Far more critical for this case note were the European Court of Justice's interpretations of the procedure for which the PNR data may be accessed, the general and systematic data transfer, and the automated processing of the PNR data.

Regarding the access procedure permissible under the Charter, the European Court of Justice emphasised that the retained PNR data could be disclosed to the competent authorities where there is an indication that the data subject may be involved in terrorist offences and serious crimes that have an objective link to air travel.[56] Except where the data are disclosed following a hit as a result of the automated processing, they must be disclosed to the relevant authorities based on a new circumstance (other than the circumstance associated with automatic processing) relating to fighting terrorist offences and serious crimes.[57]

Where the request relates to serious crime, the Directive requires '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' to air travel.[58] Thus, the Court restricted the access condition for serious crime purposes to a certain degree of suspicion that must fall upon the data subject. However, the Court dropped this restrictive condition for offences relating to terrorism. This is because for the Court, if 'there is objective evidence from which it can be inferred that the PNR data could, in a given case, contribute effectively to combating [terrorist offences]', the objective link between the data subject's involvement in the commission of these offences and air travel would be deemed to exist.[59] This is quite a departure from seeking an individualised reasonable suspicion because the Court seemed satisfied with the general assessment of the effective contribution of a given data set for combating terrorist offences. Still, in either circumstance, the European Court of Justice required that a body approves access requests by national authorities.[60]

But what qualities should that approval body possess? The European Court of Justice largely followed the Advocate General's Opinion in addressing this question. Using the data retention cases as the precedent, the Court insisted on the independence of the administrative review body.[61] It held that the body would only act objectively and impartially if it were a *third party* to the authority who made the access request because it could review the request without any external

[55]For the ECJ's in *dubio pro libertate* interpretation *see Ligue des droits humains*, *supra* n. 1, paras. 86-91.

[56]Ibid., para. 217.

[57]Ibid., para. 218.

[58]Ibid., para. 220 (emphasis added).

[59]Ibid., para. 220.

[60]Ibid., paras. 221-225.

[61]Ibid., para. 225.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

influence.[62] These elements were also essential in answering whether the Passenger Information Units could be designated as the competent national authority to approve the disclosure requests. The Court quickly rejected this practice because the units were involved in preventing, detecting, investigating, and prosecuting terrorist offences and serious crimes and could not be considered third parties to access requests.[63]

Regarding the proportionality of the general and systematic PNR data transfer on incoming and outbound flights to the EU (i.e. extra-EU flights), the European Court of Justice followed its precedent in Opinion 1/15. It found such transfer proportionate to attain the public security purpose since it is the pre-requisite for the automated processing of PNR data before passengers arrive at or depart from a member state, as it facilitates security checks at borders.[64] A targeted data transfer based on a particular group of passengers would frustrate this objective.[65] While departing from its precedent on data retention for PNR processing on extra-EU flights, the Court largely followed the same precedent in limiting the PNR processing in connection with the flights between the member states (i.e. intra-EU flights).

As a starting point, the European Court of Justice noted that the EU PNR Directive does not impose a general obligation on the member states to apply the PNR system to intra-EU flights.[66] Instead, they are given the discretion to do so if it is *strictly necessary* to achieve the objective of the fight against terrorism and serious crime.[67] To meet this strict necessity test, which was heavily developed from the *La Quadrature du Net* decision on data retention,[68] the member states must observe a link between the threats to internal security and the PNR processing.[69] The existence of terrorist threats in and of itself satisfied the link to extend PNR processing to all or certain intra-EU flights.[70] The Court also required certain limitations: the extension must be time-limited, and an abstract terrorist threat would not meet the test.[71] The threat must be genuine and present or foreseeable.[72] The decision to extend processing based on such a threat must be subject to effective review by a court or an independent administrative body.[73]

[62]Ibid., para. 226.
[63]Ibid.
[64]Ibid., paras. 161-162
[65]Ibid., para. 162.
[66]Ibid., paras. 167-168.
[67]Ibid., paras. 165-169 (emphasis added).
[68]ECJ 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* v *Premier Ministre and Others*, ECLI:EU:C:2020:791.
[69]*Ligue des droits humains*, *supra* n. 1, para. 169.
[70]Ibid., para. 171.
[71]Ibid., para. 172.
[72]Ibid.
[73]Ibid.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

Where the member states cannot provide evidence of a terrorist threat, they cannot extend the processing to *all* intra-EU flights because doing so would not satisfy the necessity test.[74] They can apply PNR processing to selected intra-EU flights based on specific routes, travel patterns or airports.[75] The Court did not explicitly mention the grounds for which the extension could be deemed to satisfy the strict necessity test. Possibly, the selection is justified based on serious crimes – as opposed to ordinary crimes, because of the Court's earlier references to the strict necessity test in light of the objectives of the EU PNR Directive.[76] What is interesting in this cross-reference is that the Court explicitly excluded the paragraph in which it required an effective review of the extension, which suggests that where the member states seek to extend PNR processing to selected flights for preventing, detecting, investigating and prosecuting serious crimes, that extension would not be subjected to a review by a court or an independent administrative body.[77] Instead, the member states themselves are required 'to review that assessment regularly in accordance with changes in the circumstances that justified their selection, to ensure that the application of the system established by that directive to intra-EU flights continues to be limited to what is strictly necessary'.[78]

On the validity of the rules on the automated processing of PNR data, the European Court of Justice initially noted that the EU PNR Directive precluded the use of self-learning (or machine-learning) systems because these systems modify themselves without human intervention, which is not what the Directive prescribes.[79] According to the Court, the PNR scheme did not implement machine-learning systems because the processing was based on 'pre-determined criteria', which are rules coded by system designers; thus, developing these does not rest merely on finding initial patterns through data clusters. The Court also referred to the opacity of the systems created by machine-learning algorithms and their significant ramifications for data subjects to enjoy their right to legal remedies.[80]

Later, the European Court of Justice considered how the algorithmic systems based on the pre-determined criteria, such as the automated PNR data processing system, should be implemented by requiring those criteria to be targeted,

[74]Ibid., para. 173.

[75]Ibid., para. 174.

[76]Ibid.

[77]For a similar interpretation *see* Council of the EU, *Improving Compliance with the Judgment in Case C-817/19 – Ideas for Discussion*, 11911/22 (9 September 2022) p. 8, https://www.statewatch.org/media/3496/eu-council-pnr-way-forward-discussion-paper-11911-22.pdf, visited 21 June 2023.

[78]*Ligue des droits humains*, *supra* n. 1, para. 174.

[79]Ibid., para. 194.

[80]Ibid. (emphasis added).

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

proportionate, specific, and non-discriminatory. To be deemed targeted and specific, the criteria must be able to identify 'individuals who might be *reasonably suspected* of involvement in terrorist offences or serious crimes'.[81] The proportionality of the rules would be achieved by including both 'incriminating' and 'exonerating' circumstances which may suggest that the passenger may be involved in terrorist offences or serious crime in their definition.[82] To ensure that the pre-determined criteria do not result in discrimination, the member states are prohibited from defining the rules on the specific protective characteristics and are required to ensure that the application of the rules does not result in indirect discrimination.[83] To avoid the risk of discrimination, the rules must be based on the factual conduct of the passengers.[84]

Commentary

A green light for extra-EU flights and an amber light for intra-EU flights

An important aspect of *Ligue des droits humains* is the different applications of the constitutional framework for PNR processing on extra-EU flights and intra-EU flights. Requiring targeted processing for the latter, while considering the former proportionate despite its indiscriminate nature, deals with a prominent question in this field: how to limit the mass surveillance regime that is implicit in this indiscriminate data transfer (and the subsequent data processing in connection with determining whether an individual must undergo secondary screening).[85] The more untargeted a surveillance practice is, the harder it becomes to justify the interference caused by that practice – or such has been the argument against data retention measures before the European Court of Justice.[86] As mentioned above, regarding extra-EU flights, the Luxembourg Court permitted such extensive data transfer by finding it proportionate to conducting border security checks for

[81]Ibid., para. 198.

[82]Ibid., paras. 199-200.

[83]Ibid., para. 197.

[84]Ibid., para. 199.

[85]C.C. Murphy, *EU Counter-Terrorism Law: Pre-emption and the Rule of Law* (Hart Publishing 2015); M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Bloomsbury 2017); E.M. Kuşkonmaz, *Privacy and Border Controls in the Fight Against Terrorism: A Fundamental Rights Analysis of Passenger Data Sharing* (Brill/Nijjhof 2021).

[86]P. Bernal, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate', 1(2) *Journal of Cyber Policy* (2016) p. 243; N. Ni Loideain, 'The Approach of the European Court of Human Rights to the Interception of Communications' (13 November 2020), https://ssrn.com/abstract=3699386, visited 21 June 2023.

fighting terrorism and serious crime. The question is whether the departure from the precedent on data retention was caused not by the different nature of the data processed (i.e. PNR data versus communications data) but by the primary purpose of data transfer, i.e. performing border controls incorporating public security purposes.

The European Court of Justice was silent on this point in Opinion 1/15.[87] The Advocate General provided reasons for rejecting the classification of PNR data as communications data in his Opinion in *Ligue des droits humains*.[88] However, unlike the Advocate General, the Court did not explicitly state that its departure from the data retention case law was because of the less intrusive nature of PNR data compared to communications data for individuals' private lives.[89] It declared the indiscriminate data transfer for extra-EU flights proportionate, based on the added value of automated analysis of the PNR data for external border controls while following the necessity test set out in data retention jurisprudence to restrict PNR processing for intra-EU flights. Had the European Court of Justice distinguished its findings based on the difference between the PNR data and communications data, it would have been harder to justify why the precedent on the latter was applied to its observations on the extension of the PNR processing for intra-EU flights.

The limitations to PNR processing for intra-EU flights are possibly indirectly connected to the obligations under Article 45 of the Charter on the EU citizens' right to free movement. The referring court did not question the validity of the PNR processing with free movement. Instead, it disputed the validity of the Advance Passenger Information data processing concerning intra-EU routes. For the European Court of Justice, this was a void question, given that this data processing concerned border checks at external borders as opposed to internal borders.[90] Still, the Court emphasised the ramifications of extending PNR processing to intra-EU flights and other means of transportation.[91] If the system

[87]The ECJ considered the nature of the PNR data in considering whether PNR data processing, as prescribed under the disputed international agreement, breaches the essence of the right to privacy and data protection, but it did not explicitly rely on the same observation in distinguishing the interference caused by the indiscriminate data transfer from the interference caused by the data retention. *See* Opinion 1/15, *supra* n. 34, para. 120.

[88]Opinion of AG Pitruzzella, *supra* n. 39, paras. 193-199.

[89]Note here that the ECJ considered the types of information that the PNR data reveal and their risk of revealing individuals' private lives in determining the gravity of the interference caused by the EU PNR Directive. The Court deemed the interference serious based on the further information revealed by the automated PNR data processing: *Ligue des droits humains*, *supra* n. 1, paras. 92-111. As regards the proportionality of the indiscriminate PNR data transfer, the Court did not reiterate its findings on the nature of the data.

[90]*Ligue des droits humains*, *supra* n. 1, paras. 265-266.

[91]Ibid., para. 273.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

applies to intra-EU flights and other means of transport (as was the case under Belgian law), it might disadvantage EU citizens who have exercised their free movement right by conducting the systematic and continuous transfer of their PNR data.[92] The restriction on the free movement right must be proportionate to be justified. On this point, the Court reiterated the necessity test for PNR processing for intra-EU flights in light of privacy and data protection rights.[93] Consequently, the Court's final iterations of how the rules extending PNR processing of intra-EU flights must be interpreted in light of Article 45 of the Charter were similar to its findings on the proportionality of the processing developed through references to the precedent on data retention.[94]

Given that most PNR processing concerns intra-EU flights,[95] the strict necessity test to extend the processing accordingly might be the one that will give the biggest headache to the member states in redesigning their PNR schemes.[96] An immediate question here is what qualifies as 'terrorist threats', the existence of which justifies the extension of PNR processing to all or selected flights. Terrorism is defined under EU law,[97] and there are threat reports (e.g. Terrorism Situation & Threat Report) conducted by Europol that, according to the Council, may give a preliminary understanding of what those terrorist threats are.[98] In response to the Council's questions on post-*Ligue des droits humains*, the member states did not agree to refer to the Europol reports to justify the existence of terrorist threats in processing PNR data for intra-EU flights.[99] An agreement has not been reached on how to select intra-EU flights should such threats be deemed to exist. The Council suggested implementing a filtering mechanism that would allow selection by the member states without involving air carriers.[100] There is an apparent disagreement on the compatibility of this mechanism with the European Court of Justice's findings in *Ligue des droits humains*. For example, while

[92]Ibid., paras. 282-285. *See also* Opinion of AG Pitruzzella, *supra* n. 39, para. 205.

[93]*Ligue des droits humains*, *supra* n. 1, paras. 278-291.

[94]Ibid., para. 291.

[95]Council of the EU, *Improving Compliance – Ideas for Discussion*, *supra* n. 77, p. 2.

[96]For proposals on the technological solutions to target intra-EU flights and questions concerning the sector expected to bear the financial burden, *see* ibid.

[97]Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L88/6 (31 March 2017), Art. 3.

[98]Council of the EU, *Improving Compliance – Ideas for Discussion*, *supra* n. 77. However, the Directive mentions that '[e]ach Member States should be responsible or assessing the potential threats related to terrorist offences and serious crime'. *See* EU PNR Directive, Recital 19.

[99]Council of the EU, *Improving Compliance with the Judgment in Case C-817/19 – Comments from Member States*, 12856/22, https://www.statewatch.org/media/3701/eu-council-pnr-judgment-ms-comments-12856-22.pdf, visited 21 June 2023.

[100]Council of the EU, *Improving Compliance – Ideas for Discussion*, *supra* n. 77, p. 3.

reiterating their dismay with intra-EU flight selection, the French authorities argued that a filtering mechanism could be feasible whereby the Passenger Information Units would collect all PNR data and process only the selected ones.[101] The German authorities, on the other hand, considered that a filtering mechanism as such would mean processing the PNR data of all passengers indiscriminately and thus would be incompatible with the European Court of Justice's requirements.[102] These examples are previews of the long road ahead of addressing the complex legal and practical issues arising from the constitutional standards that the Court set for the PNR processing of intra-EU flights.

The next question is how to review the member states' claims to extend PNR processing to intra-EU flights. The European Court of Justice required a mandatory revision only when the processing covers all flights and is carried out due to a perceived terrorist threat. No similar review mechanism is imposed on the member states when they introduce the PNR processing for threats relating to serious crimes. The Court only required the member states to review their decisions regularly – which is not equal to monitoring by an independent third party not involved in the initial decision process. It may thus fall upon the European Commission as the guardian of Treaties to ensure that the relevant extensions are introduced in line with EU law.

While these questions loom large, the *Ligue des droits humains* decision's immediate effect would be to validate the indiscriminate PNR data transfer under the current or potential international agreements with third countries on PNR sharing and processing. The existing agreements had tumultuous backgrounds – the events leading up to Opinion 1/15 are the most recent evidence of the tensions.[103] This does not mean that the legality of the agreements will not be questioned after the *Ligue des droits humains* decision – quite the opposite. There are many further requirements, not least for the automated analysis of data and the scope of databases to cross-check PNR data that these agreements need to satisfy. Nevertheless, one core argument – the impermissibility of indiscriminate transfer of PNR data – seems to be weakened.

A new dawn for governing automated decision-making systems within the European constitutional framework

The Court's observations on the self-learning/machine-learning systems and the algorithmic systems based on pre-determined criteria will have ramifications for

[101]Council of the EU, *Improving Compliance – Comments from Member States*, *supra* n. 99, p .38.
[102]Ibid., p. 45.
[103]*See* P. Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters* (CEPS September 2008) http://aei.pitt.edu/11745/1/1704.pdf, visited 21 June 2023.

the EU constitutional framework for artificial intelligence (AI)-based systems.[104] As for the former, the starting point is the Court's acknowledgement of the human input in the final decision process where there is a hit and how this input would have been rendered 'redundant' if machine-learning methods were deployed.[105] Their inherent opaque nature would constrain the final human input because how the system produces a 'hit', flagging a passenger for further inspection, would be hard to interpret.[106] In other words, having a 'human in the loop' is not a panacea for the opacity of machine-learning systems. More importantly, without understanding why the model produces a hit, data subjects would be deprived of their right to an effective judicial remedy.[107] Taken as a whole, the findings of the Court in upholding the concerns over machine-learning systems can be considered as a *de facto* ban over their use to the extent that they do not guarantee individuals' Charter rights to an effective remedy.

Thönnes provided a cautious reading of a potential ban. For him, this was instead a qualified prohibition because the Court's observations rested on two conditions that the machine-learning systems must possess: the first condition is that they should adapt without human intervention, and the second condition is that they are too opaque for the detriment of the right to legal remedies.[108] The public authorities could find just 'the right AI' based on these conditions to circumvent the prohibition in the future.[109] Those who are familiar with the broader debate on the human rights implications of mass surveillance practices would not be surprised if authorities tried to circumvent or deny the application of the European Court of Justice's findings to particular uses of machine-learning systems.[110] The obstacles that Derave, Genicot and Hetmanska had faced in accessing the information on an upcoming automated risk assessment system for the Schengen-visa exempt travellers, the European Travel Information and

[104] *See*, for example, O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart Publishing 2021).

[105] *Ligue des droits humains*, *supra* n. 1, para. 195.

[106] Ibid.

[107] Ibid.

[108] C. Thönnes, 'A Directive Altered Beyond Recognition', *Verfassungsblog*, 23 June 2022, https://verfassungsblog.de/pnr-recognition/, visited 21 June 2022. For supporting views, *see* D. Korff, *Opinion on the Implications of the Exclusion from New Binding European Instruments on the Use of AI in Military, National Security and Transnational Law Enforcement Contexts* (European Center for Not-for-Profit Law October 2022) https://ecnl.org/sites/default/files/2022-10/ECNL%20Opinion%20AI%20national%20security.pdf, visited 21 June 2023.

[109] Thönnes, *supra* n. 108.

[110] *See*, for example, M.H. Murphy, 'Algorithmic Surveillance: the Collection Conundrum', 31(2) *International Review of Law, Computers & Technology* (2017) p. 225.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

Authorisation System,[111] could be a foreshadowing of the future spectacle of denial by public authorities.[112] There is thus a legitimate concern that public authorities (broadly defined as covering law enforcement and security agencies) would seek to circumvent this (potential) prohibition on using machine-learning systems. In this context, the concerns voiced by Thönnes on the European Court of Justice's limited constitutional framing of machine-learning systems are persuasive.

However, finding the 'right AI', as Thönnes put it, to avoid the European Court of Justice's *de facto* ban on machine-learning systems would not be easy for public authorities. Each system must be analysed separately to determine how much it operates on machine-learning algorithms and is captured by this limitation. First, even though pre-determined features can be designed or introduced in an algorithm before it undergoes the process of self-learning rules, it does not mean that the resulting AI system can immediately be classified as being based on pre-determined rules. Technical details regarding how the decision-making process (self-learned rules) would be necessary to evaluate the outcome interpretability and for a final classification.

Second, overcoming the opacity of machine-learning systems is equally difficult because implementing legal claims of transparency in designing these systems is still an ongoing task.[113] Opacity concerns have driven legislators to adopt specific legal requirements to be applicable where automated decision-making is used.[114] From data protection law to public law, legal scholars have explored how transparency can be achieved for AI systems. The solutions to achieve transparency have ranged from reviewing the choice of AI systems (in the public sector) to the duty to give justifications for algorithmically-supported decisions.[115] In the field of computing and information systems, ensuring more

[111]Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236, 19 September 2018.

[112]C. Derave et al., 'The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System', 13(3) *European Journal of Risk Regulation* (2022) p. 389.

[113]A. Bibal et al., 'Legal Requirements on Explainability in Machine Learning', 29 *Artificial Intelligence and Law* (2021) p. 149.

[114]The most common example in this context is the right to meaningful intervention and explanation found in the EU's GDPR.

[115]*See*, for example, S. Wacther et al., 'Why a Right to an Explanation of Automated Decision-making Does Not Exist in the General Data Protection Regulation', 7 *International Data Privacy Law* (2017) p. 76; M. Almada, 'Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems' (2019) Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law, https://doi.org/10.1145/3322640.3326699, visited

transparency to algorithms has been equally sought because of the ethical and trust issues surrounding the opaque AI models.[116] However, the opacity question is framed as part of achieving interpretable AI models that, in essence, require 'the extraction of relevant knowledge from a machine-learning model concerning relationships either contained in data or learned by the model'.[117] The aim is to give the human audience insights into why certain decisions or predictions were made using different methods, from visualisation to mathematical equations.[118] In a way, interpretable AI models are developed to represent the mathematical model used in the system, which may not necessarily translate into legal requirements purported to achieve transparency.

The applicability of legal requirements of transparency to interpretable AI models remains important in the background. Still, a particular question arises from the *Ligue des droits humains* decision. Where would the European Court of Justice's findings on opacity be situated in this debate? If technological limitations for achieving the transparency of machine-learning algorithms are overcome, would this be sufficient for the Court to permit their use? A deeper reading of the European Court of Justice's findings can help us to anticipate its potential stance on the transparency that the public authorities claim the machine-learning algorithms have.

The European Court of Justice did not limit the opacity question to the technical means by which the transparency of machine-learning systems could be achieved. Instead, it attached weight to the responsibility and accountability of public bodies for the automated decision-making process. Crucially, as mentioned above, in condemning machine-learning systems, the Luxembourg Court directly connected the right to an effective remedy under Article 47 of the Charter.[119] It continued to refer to this right when it set out one of the conditions where the automated use of PNR data (not based on machine-learning models) is allowed. Here, the Court referred to two cases that relate to the enjoyment of the Article 47 right in two different contexts: one in the context of visa refusal for reasons of public order (*RNNS and KA*[120]); and the other in the context of non-admission of

21 June 2023; T. Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box', in T. Wischmeyer and T. Rademacher (eds.), *Regulating Artificial Intelligence* (Springer 2020) p. 75.

[116]T. Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences', 267 *Artificial Intelligence* (2019) p. 1.

[117]W.J. Murdoch et al., 'Definitions, Methods and Applications in Interpretable Machine Learning' (2019) 116(44) *Proceedings of the National Academy of Sciences*, https://doi.org/10.1073/pnas.1900654116, visited 21 June 2023.

[118]Ibid.

[119]*Ligue des droits humains*, *supra* n. 1, para. 195.

[120]ECJ 24 November 2020, Joined Cases C-225/19 and C-226/19, *RNNS (C-225/19), KA (C-226/19)* v *Minister van Buitenlandse Zaken*, ECLI:EU:C:2020:951.

an EU citizen to another member state for reasons of public security (*ZZ*).[121] Based on these precedents, the Court recognised a duty to explain the model and the final decision to the individual, as the subject of the decision, and to the oversight bodies.

First, data subjects should be able to 'to understand how [pre-determined assessment criteria and programs applying those criteria] work, so that that person can decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress', albeit without necessarily becoming aware of those criteria and programs.[122] The precedent that the European Court of Justice used, *RNNS and KA*, suggests that the duty is not limited to the general working of the system and comprises the duty to explain how the system reached a *particular* decision about the person.[123] Second, authorities using an automated decision-making system to arrive at a decision must disclose its basis to courts and the other oversight bodies. When the person concerned contests the decision, the competent court must examine the grounds and evidence based on that decision and 'the pre-determined assessment criteria and the operation of the programs applying those criteria', except in state security cases.[124] Finally, the Court mentions the power of data protection and national supervisory authorities to monitor the processing of PNR data by the national Passenger Information Units and recognises that they need to access the pre-determined criteria.[125]

According to the European Court of Justice's findings on the proportionate automated PNR processing data, just as the Court condemned the use of machine-learning models because of the problems with guaranteeing the Charter right to an effective remedy, neither did it provide a blank cheque for the systems that use pre-determined models (such as those the Court found to be implemented by the EU PNR Directive). While, in principle, an interpretable algorithm can be generated, it is reasonable to assume that – given the diversity (and therefore complexity) of the data collected through PNR – this will not, in general, be true for an automated system used to detect unknown patterns and behaviours for border security purposes. Most importantly, by its nature, the automated system is continuously fed with new data so that the algorithm upon which it is based (and consequently the decision rules) are always updated to reach better performances. Moreover, the close link to the right to remedies in considering both algorithmic models suggests that the Court would focus on enjoying this right despite the transparency claims based on abstract mathematical

[121]ECJ 4 June 2013, Case C-300/11, *ZZ* v *Secretary of State for the Home Department*, ECLI:EU:C:2013:363.

[122]*Ligue des droits humains*, *supra* n. 1, para. 210.

[123]*RNNS and KA*, *supra* n. 120, para. 43.

[124]*Ligue des droits humains*, *supra* n. 1, para. 211.

[125]Ibid., para. 212.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

models. The more detrimental the self-learning systems are to data subjects' enjoyment of effective remedies, the less acceptable they would be under EU law. Yet, there can be difficulties with claiming this right effectively where automated systems are used for security interests which have provided the very reason why public authorities refrain from disclosing information.

Finally, the Court's observations on the AI technologies (both machine-learning and rule-based models) will have a domino effect on the other EU databases that implement these technologies. For example, the legality of the European Travel Information and Authorisation System has captured particular attention for its direct reference to the automated processing of the information obtained by the arriving visa-exempt passengers against the risk indicators.[126] The attempts by Derave, Genicot and Hetmanska to obtain details about those risk indicators revealed that Frontex, which was the only EU agent who replied to their information request, had denied that this system should be considered an AI system.[127] Whether it can be classified as a machine-learning system or a system that uses pre-determined rules is outside the scope of this case note.[128] Either way, its compatibility with the Charter must be assessed based on the European Court of Justice's limitations for machine-learning systems and further requirements for non-machine-learning systems, depending on the final qualification of the automated system it uses. For example, Zandstra and Brouwer considered the extent to which there is a meaningful 'human-in-the loop' when a hit resulting from the automated processing is processed manually as per the European Travel Information and Authorisation System Regulation (Articles 20(5) and 21(2)).[129] Moreover, this (qualified or non-qualified) limitation on machine-learning systems might contradict how the EU envisions regulating AI under the proposed AI Act.[130] Although the Act concerns the AI systems to be placed in the EU internal market and the obligations of producers and users of the AI systems, there is an overlap with the Charter obligations, as using these systems would trigger fundamental rights protections. The Act identifies four risk categories for

[126]ETIAS Regulation, Art. 33.

[127]Derave et al., *supra* n. 112, p. 18-19.

[128]Note here that, based on the publicly available reports on the European Travel Information and Authorisation System, Derave et al considered it to be an AI-based system that uses machine-learning techniques: ibid., p. 19-23.

[129]T. Zandstra and E. Brouwer, 'Fundamental Rights at the Digital Border – ETIAS, the Right to Data Protection, and the CJEU's PNR judgment', *Verfassungsblog*, 24 June 2022, https://verfassungsblog.de/digital-border/, visited 21 June 2023. *See also* A. Musco Eklund, 'Frontex and Algorithmic Discretion – (Part I)', *Verfassungsblog*, 10 September 2022, https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/, visited 21 June 2023.

[130]Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, COM/2021/206 final [AI Act].

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

implementing AI systems, from unacceptable to minimal risks. The second in the risk category is high-risk AI, whereby the producers of AI systems that fall within this category must perform a conformity assessment before placing them in the internal market.[131] The Act first lists AI systems used in migration, asylum and border control management under the high-risk category,[132] only to later exclude the large-scale EU immigration and border control databases (including the European Travel Information and Authorisation System) from this category.[133] The *Ligue des droits humains* decision increases the pressure to amend the proposal.[134]

In search of an effective review body

The requirement for an 'effective review', as the European Court of Justice calls it, is evident throughout the decision as the Court considered the oversight provisions of the EU PNR Directive.[135] The decisions the Court considered to be subjected to review are: (i) the member states' decisions to extend PNR processing to all or selected intra-EU flights where there is a genuine and present or foreseeable terrorist threat;[136] and (ii) decisions of competent national authorities (where the judiciary is not the designated authorisation body) to access the retained PNR data for the fight against terrorism and serious crimes irrespective of the fact that the access request is made before or after depersonalisation.[137]

[131]AI Act, Title III.

[132]AI Act, Annex III.

[133]AI Act, Art. 83 and Annex IX.

[134]EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* (EDPS 18 June 2021), https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, visited 21 June 2023; 'Uses of AI in Migration and Border Control: A Fundamental Rights Approach to the Artificial Intelligence Act', *EDRi,* November 2021, https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf, visited 21 June 2023.

[135]The PNR Directive circumscribes an ongoing oversight to be carried out by national data protection officers (Art. 6(7)), an ex-post oversight by the designated national supervisory authority (Art. 15), and an oversight of access authorisation after de-personalisation of the data (Art. 12) in addition to the judicial oversight that can take place in connection with the data subjects' data protection and redress rights as recognised under Art. 13. The first two types of oversight became relevant in considering the mandate of the competent authorities to provide access to the officers and the supervisory authorities for their role in verifying the lawfulness of PNR processing.

[136]*Ligue des droits humains*, *supra* n. 1, para. 172.

[137]Ibid., paras. 221-222. No review mandate was required for the decisions to extend PNR processing to intra-EU flights based on threats relating to the serious crime except for the one-off reporting duty entrusted to the Commission. *See* EU PNR Directive, Art. 13.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

There is a stark difference in the stages at which the review can take place for these decisions. While reviewing decisions to extend PNR processing to intra-EU flights on terrorism grounds takes place *ex-post*, the review of access requests must be *a priori*. This is because the EU PNR Directive already mandated a priori review mechanisms for granting access to the retained PNR data.[138] The European Court of Justice also required such an *a priori* review in its Opinion 1/15, the findings of which were based on the precedent of communications data retention.[139] The legal dispute, however, was not over the stage at which the review could take place, but about the qualities that the review body must have under EU law.

The common thread to both review mechanisms is their 'independence'. This independence requirement is central to a fundamental-rights-compliant review body. The member states must observe this requirement when making necessary amendments to national laws in light of the European Court of Justice's decision. For the Court, the independence requirement means that the oversight body is a *third party* to the authority that delivered the decision to enable it to review the request free from *any external* influence.[140] This means that the reviewing body must be institutionally and operationally detached from the authority it oversees. The review body must be mandated to deliver legally binding decisions,[141] and the powers entrusted to it must allow it to 'reconcile the various interests and rights at issue'.[142] Based on the precedent on data retention, on which the Court relied heavily in certain parts of the decision, it can also be suggested that these powers encompass the authority to review the necessity of the measures.[143] A reading as such means that the review body has powers beyond assessing whether the decision is conducted in accordance with the law. Its powers comprise reviewing the case for the operations, including their necessity.

Further requirements for independence can be found in the European Court of Human Right's case law on secret surveillance, which could provide the source of inspiration for the minimum threshold for independence required from the administrative bodies that undertake revisions of access to PNR data or introduce

[138]EU PNR Directive, Art. 12.

[139]Opinion 1/15, *supra* n. 34, para. 202; *Digital Rights Ireland*, para. 62; EJC 21 December 2016, Case C-203/15 *Tele2 Sverige AB* v *Post –och telestyrelsen and Secretary of State for the Home Department* v *Tom Watson and Others* ECLI:EU:C:2016:970, para. 120; ECJ 5 April 2022, Case C-140/20, *GD* v *Commissioner of An Garda Síochána and Others*, ECLI: EU:C:2022:258, para. 110.

[140]*Ligue des droits humains*, *supra* n. 1, para. 226.

[141]ECJ 16 July 2020, Case C-311/18, *Data Protection Commissioner* v *Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559, para. 196; *La Quadrature du Net*, *supra* n. 68, paras. 168 and 192.

[142]*Ligue des droits humains*, *supra* n. 1, para. 225.

[143]*GD*, *supra* n. 139, para. 110.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

PNR processing for intra-EU-flights on terrorism grounds. For example, the European Court of Human Rights shared similar views to the European Court of Justice on the powers and tasks assigned to the bodies, especially on whether they had the power to render legally binding decisions.[144] As the European Court of Human Rights has been asked to consider the independent status of non-judicial and quasi-judicial bodies, it has developed certain criteria for the relevant body to maintain that status: the manner of appointment ; the terms of office ; and the impact of their dual responsibilities.[145]

Overall, designating a review body to oversee the PNR data access and intra-EU flight data processing (albeit only in the context of responding to terrorist threats) can be an uphill battle for the member states. For example, locating a division within the Passenger Information Unit to review data access requests would not satisfy the independence requirements. Neither would designating data protection officers as the *a priori* body, because the EU PNR Directive already entrusts them with *ex-post* powers to review those requests made by national administrative bodies. Tasking data protection officers with a double review duty would jeopardise the effectiveness of the review, as it would be asked to assess its own activities. The independence requirements considered in this section can guide in designating the relevant review bodies.

Conclusion

The *Ligue des droits humains* decision is a foreword to the ongoing legal disputes on the legality of PNR processing and the potential political tensions that will erupt along the way. The European Court of Justice salvaged the EU PNR Directive by providing a Charter-compliant interpretation of its text. The decision's immediate effect is that the member states must amend their national laws in compliance with the Court's observations. The next hurdle will be to ensure a harmonised application of what the European Court of Justice deemed to be a Charter-compliant Directive. This case review focused on three legal issues. The first legal issue is the European Court of Justice's different proportionality analysis for the PNR processing for extra-EU flights and intra-EU flights. For the latter, the Court reiterated its findings in Opinion 1/15 by declaring indiscriminate data transfer proportionate to protecting the Charter rights to privacy and data protection due to a reading of 'border security' as the justificatory ground. However, it adopted a stringent Charter framework for PNR processing

[144] *Leander* v *Sweden* (1987) 9 EHRR 433, paras. 82-83; ECtHR 6 June 2006, No. 62332/00, *Segerstedt-Wiberg and Others* v *Sweden*, para. 118.

[145] ECtHR 18 May 2010, No. 26839/05, *Kennedy* v *the UK*, paras. 166-167; ECtHR 25 May 2021, No. 35252/08, *Centrüm för Rättvisa* v *Sweden*, para. 346.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press

for intra-EU flights. It also raised questions on how the member states can consistently implement this framework in the existing PNR systems. The other pending preliminary requests contain similar questions on the extent to which PNR processing for these flights guarantees the Charter rights to privacy and data protection, and additional questions on the compatibility of the processing with the freedom of movement. The European Court of Justice's opinion on these matters will shape the course of the dialogue that the Council has started among the member states on consistently implementing the Court's initial findings in *Ligue des droits humains*. The second legal issue is the judicial framing of the automated PNR processing, which allowed the European Court of Justice to consider a constitutional framework for machine-learning and non-machine-learning systems. In this context, it provided a fundamental rights anchor for both systems: the right to an effective remedy. Finally, the Court requires a review body to oversee the extension of PNR processing to intra-EU flights, which will be another contentious point in redesigning PNR systems.[146] The independence of that review body will be paramount for a Charter-compliant PNR system. The European Court of Justice's case law on data retention and the European Court of Human Rights' case law on secret surveillance can provide essential insights into the independence qualities that must be observed in designating that review body.

Elif Mendos Kuşkonmaz is Lecturer in Law, University of Essex, United Kingdom.

Acknowledgements. I thank the editors and anonymous reviewers for their helpful comments and suggestions. All errors remain my own.

[146]The Council suggested setting up an EU-wide review body, but not all member states gave clear support to this suggestion. France, for example, argued for the revision to remain national. *See* Council of the EU, *Improving Compliance – Comments from Member States*, *supra* n. 99, p. 42.

https://doi.org/10.1017/S1574019623000111 Published online by Cambridge University Press