LUISS

Department of Political Sciences
Degree Program in International Relations

Chair of Security Law and Constitutional Protection

The Price of Security in Air Travel. The PNR Jurisprudence of the Court of Justice of the European Union

Prof. Davide Paris
SUPERVISOR

Prof. Domenico Pauciulo
CO-SUPERVISOR

ID. 650222

Alessia
Urciuoli

CANDIDATE

Academic year 2022/23

INDEX

INTRODUCTION

Meet Paul O'Connor. Paul is a thirty-five-year-old man from Ireland, passionate about travelling and who has always dreamt of exploring the natural landscapes of Canada. One day, the opportunity finally came, and he eagerly booked a flight to Vancouver, excited to visit the beauty of Canada. As Paul filled out the online booking form, he didn't think much of the personal information he entered: his name, contact details, travel dates, meal preferences and payment information. It was a routine part of booking a ticket, after all.

However, while Paul's journey lasted a total of 14 hours, he didn't realize that his information was about to embark on a journey of its own. Paul's Passenger Name Record (PNR) data was on its way to becoming part of a much bigger story. A story that would explore the challenges and questions surrounding data privacy in a digital age.

This is a story not just about one traveller but about the complexities of our interconnected world, where personal information flows freely but must also be safeguarded, where security and privacy dance a delicate tango.

Since the first decades of the twenty-first century, governments tried to respond to gaps both in knowledge and in capacity with regard to emerging security threats, by prioritizing areas such as counter-terrorism and serious transnational crime, focusing on the technological side of security.[1] While high-tech tools improve the ability for early warning and prevention, the legitimate question that arises is whether such technologies are suitable and efficient, and also if their interference with fundamental rights is proportionate.

In the aftermath of the deadliest terrorist attack on American soil on 11 September 2001, a strong emphasis was put on enhancing airport security and different security measures were adopted to prevent similar attacks from ever happening again.[2] Nowadays we have become accustomed to the prohibition from carrying sharp objects like scissors

[1] Kolliarakis, Georgios. "In quest of reflexivity. Towards an anticipatory governance regime for security." In: M. Friedewald, et al. edits. Surveillance, privacy and security. Citizens' perspectives. Abingdon:Routledge, 2017: 233-254,. p.236

[2] Gerace, Diane. "A Look at How Airport Security Has Evolved Post 9-11." June 11, 2021. Last accessed 08/09/2023 at https://www.phl.org/newsroom/911-security-impact.

and knives, to the limits on flying with liquids or to enduring endless queues to go through security checks before boarding an intercontinental flight.

However, while people believe that standing in long, endless queues at the airport is an attack on their personal freedom, much more patience is shown towards invasions of privacy, indeed people distribute their data easily.[3] Also, most of the time, the "simple" transfer of air passenger data to security services goes widely unnoticed by the public.[4] Most passengers, including those who travel often, are unaware of the potential use of their data by law enforcement agencies. However, the processing and storage of such data presents a significant threat to the protection of the fundamental rights of citizens, particularly the right to privacy and the right to protection of personal data.

It can be affirmed that the transfer of personal data from the European Union to third countries constitutes a minefield, because of the different approaches and standards of data protection that each State has.[5] This topic becomes even more thorny when one considers the fact that the European Union has a very high standard of data protection. The political conflict that arises over data sharing is nowhere more evident and delicate than in the realm of air travel, where a variety of actors (such as commercial airlines, border authorities, law enforcement agencies, and security agencies) have interests in the creation and sharing of such data.[6] Thus, the examination of international agreements on the transfer of Passenger Name Record (PNR) data turns out to be particularly interesting in evaluating how they affect the right to privacy and data protection of individuals.

But what is Passenger Name Record (PNR) data? It is unverified information submitted by the passenger while booking a ticket, including name, address and email, phone numbers, terms of payment, booking dates, seat number and dietary choices. Originally this information was used for commercial purposes, but soon states started to realize that the processing of such data could also be used as a tool to proactively prevent terrorist offences and serious transnational crime. Indeed, when all of this information is

[3] Hobbing, Peter, "Tracing Terrorists: The EU-Canada Agreement" in PNR Matters CEPS Special Report/September 2008. p.1
[4] *Ibidem*
[5] Fahey, Elaine, Elspeth Guild, and Elif Kuskonmaz. "The Novelty of EU Passenger Name Records (PNR) in EU Trade Agreements: On Shifting Uses of Data Governance in Light of the EU-UK Trade and Cooperation Agreement PNR Provisions." European Papers, July 24, 2023. p. 274 accessed at https://www.europeanpapers.eu/en/e-journal/novelty-eu-passenger-name-records-eu-trade-agreements.
[6] *Ibidem*

combined, it may paint a complete picture of a traveller, including information on their socioeconomic level, religious affiliation, state of health, and interpersonal ties.

The European Union signed three bilateral agreements with the United States, Canada and Australia to transfer PNR data of passengers to prevent and effectively combat the terrorist threat. For the purposes of this dissertation, only the Agreement between the EU and Canada on the transfer and processing of PNR will be analysed, due to a variety of reasons.

First of all, it is the most recent of the three agreements, since it was signed in 2014[7]. As a result, it is most likely to better give a representation of the EU's approach on how to balance security and privacy in the context of exchanging PNR data. Second, this specific Agreement faced a legal dispute initiated by the European Parliament, which contended that it did not sufficiently protect the privacy of EU citizens. Third, on 26 July 2017 in Opinion 1/15, the Court of Justice of the EU (CJEU) delivered an important ruling, finding that the agreement could not be finalized in its current form.[8] On this occasion, the Court of Justice of the EU had the opportunity to evaluate the compatibility of an international agreement with the rights outlined in the Charter of Fundamental Rights of the EU for the first time. Additionally, the existence of these PNR agreements with third countries combined with the terrorist attacks in Paris in 2015 and the Brussels bombings in 2016 led to the adoption of the EU PNR Directive.[9] Its validity and compliance with the Charter of Fundamental Rights of the EU were subject to evaluation by the Court of Justice of the European Union in 2022 in case C-817/19, or *Ligue des droits humains*.[10]

Given all of this, through the examination of two rulings of the CJEU in *Opinion 1/15* and *Ligue des droits humains*, this research aims to investigate whether the CJEU has been able to uphold the right to privacy and the right to protection of personal data of air passengers while ensuring national security. Indeed, the European Commission affirmed that "in a society where individuals will generate ever-increasing amounts of

[7] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).*
[8] CJEU. Opinion 1/15 delivered on 26 July 2017, ECLI:EU:C:2016:656.
[9] 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
[10] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. 2022

data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules."[11]

Thus, the research question this thesis aims to deal with can be essentially summarized as follows: Could the Court of Justice of the European Union effectively prioritize the rights and interests of individuals, in accordance with European values, fundamental rights, and rules, while considering national security interests?

In order to provide an answer to this question, this work is divided into three chapters.

The first introductory chapter lays down the foundations of this study and for this reason, consists of two sections. The first section demonstrates that data protection is not a game without rules and that the European Union has created a comprehensive and robust framework of data protection regulations to safeguard data subjects' rights. The second section, instead, pertains to the domain of air transportation. First of all, the differences between Passenger Name Record (PNR) and Advance Passenger Information (API) are clarified. Then, the reasons why the EU has entered negotiations and has concluded agreements on the transfer of PNR data to third countries are explained. In particular, not only the circumstances that led to the adoption of those agreements in the first place but also the events that caused their renegotiation are outlined. Furthermore, in this section, the reasons why the European Parliament decided to challenge only the EU-Canada PNR Agreement and not the other two concluded with the United States and Australia are explained. Last but not least, the path towards the adoption of the highly controversial EU PNR Directive, which created a harmonized PNR scheme at the European level, is described. Then, to avoid confusion, the difference between the EU PNR Directive and the bilateral PNR Agreements negotiated by the EU is also made clear.

The core of the second chapter is Opinion 1/15 of the Court of Justice of the European Union. The analysis starts with a description of the process that led to the contested 2014 PNR Agreement between the European Union and Canada. Then, the

[11] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. A European Strategy for data. COM/2020/66 final. 2020

chapter goes into the details of the EU-Canada PNR Agreement, whose main provisions are explained through the Court's reasoning in Opinion 1/15. Indeed, the most important aspects of the Agreement, such as the collection and transfer of sensitive data pertaining to passengers, the automated processing of data and the purposes for which it may be used, as well as the crucial question of the proportionality of the measures and safeguards for data subjects, are analysed. Finally, the various significant implications of this judgment of the Court are discussed.

The third and last chapter explores the aftermath of Opinion 1/15: case C-917/19 or *Ligue des droits humains.* This judgment of the Court of Justice of the European Union was long awaited by many Member States because the Court had the opportunity to assess the validity of the EU PNR Directive. Given the fact that the said Directive is quite similar to the EU-Canada PNR Agreement, which was declared incompatible with the fundamental rights recognized by the EU, many believed that for the same reason the Court of Justice would have invalidated the EU PNR Directive. However, this was not the case. This chapter analyses the most significant statements of the Court in this judgement in order to investigate the reasons behind this unexpected departure from previous judgment and understand the complex dynamics between security, privacy, and data protection in our data-driven era.

In light of the above, an attempt will be made to answer the following question: Did the Court's judgment in *Ligue des droits humains* signify a turning point where national security interests weighed more heavily in the balance with data protection?

CHAPTER I
The EU's regulatory framework on data protection and PNR data

Introduction

Technological advancements and the development of the Internet have brought about both new opportunities and challenges for the protection of personal data. Indeed, thanks to technological improvements both private companies and governmental agencies today have widespread access to data. Additionally, individuals are growing more open to sharing their personal information publicly. These developments have had impacts on the economy and social interactions by enabling the exchange of information within the European Union as well as with third countries and international organizations.[12]

The European Union has recognized the significant shift in the market over the past few years: from a data-driven economy, where data was the most valuable source, to a true "data economy", where data is the very object of production, transactions, and investments.[13] This growing economic significance of data collection and processing has raised concerns over the appropriate protection of fundamental rights in the digital age.[14] In other words, the opportunities offered by the new information and communication technologies (ICT), in terms of data collection and exploitation, have made it more difficult to strike a balance between the need for protection and the free flow of data and personal information.

Within the air transportation industry, the topic of passenger data, commonly known as Passenger Name Records (PNR data) presents complexities, that primarily revolve around how this information is transferred, processed and used as a security tool aimed at combating terrorism activities.[15] The issue first came to light in 2001 following the events of 11 September, when the US government addressed one of the areas where

[12] Recital 6 GDPR
[13] Cerrina Feroini Ginevra. "Luci e ombre della Data Strategy europea" - Intervento di Ginevra Cerrina Feroni, Vicepresidente del Garante per la protezione dei dati personali. *AgendaDigitale*, 13 maggio 2022. Last Accessed 20/07/2023 at https://www.garanteprivacy.it/home/docweb/-/docweb display/docweb/9769786
[14] Nesterova, Irena. "The Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security." *How International Law Works in Times of Crisis*, 2019, 109–26. p. 110
[15] Wilson, Kerianne. "Gone with the Wind?: The Inherent Conflict between API/PNR and Privacy Rights in an Increasingly Security-Conscious World." *Air and Space Law* 41, no. Issue 3, 2016: 229–264. p.229-230

counterterrorism measures had been found to lack information: air travel.[16] Thus, it enacted a law requiring all airlines operating flights to the US to disclose passengers' data to US Customs and Border Control. Anyone who travels by air must provide certain information when making a reservation, including their first and last names, contact information (such as an address and phone number), the date of their trip and their itinerary, as well as information about their luggage, payment method, and fellow passengers. Collecting and analysing these data can help authorities to identify dangerous passengers and take appropriate measures in order to prevent, detect, investigate and prosecute terrorism and other serious crimes.[17] For this reason, other third countries started to request the transfer of PNR data from the European Union.

The European Union, in order to meet these requests and to foster global collaboration in combating terrorism and serious transnational offenses, entered into agreements on the processing and transfer of PNR data originating from the EU with the United States, Canada, and Australia in 2004, 2006, and 2008 respectively. After the adoption of the Lisbon Treaty, these agreements were subject to renegotiation. While the EU PNR Agreements with the US and Australia were renegotiated and entered into force in 2012 with the consent of the European Parliament, this was not the case for the EU-Canada PNR Agreement.

To better gain a comprehensive understanding of the EU-Canada PNR Agreement case study, the first chapter of this dissertation is divided into two sections.

The first section explores the historical development of the right to data protection from its genesis to its recognition as a fundamental right. Indeed, it was not until the 1970s, when technology started advancing and digital platforms became widely used that the necessity to safeguard the personal data of individuals became apparent. The fact that individuals' data became increasingly exposed to abuse, vulnerable to data breaches and illegal access prompted the emergence of the right to protection of personal data.

Various European countries responded by enacting laws to address this issue, which paved the way for global discussions on privacy and data protection. As a result, during the 1980s efforts were made to harmonize legislation on data protection. The Organization for Economic Cooperation and Development (OECD) issued *Guidelines* on

[16] Kuşkonmaz, Elif Mendos. "The Grand Gala of PNR Litigations: Case C-817/19,Ligue Des Droits Humains v Conseil Des Ministers." *European Constitutional Law Review* 19, no. 2, 2023: 294–319. p. 297

[17] Villani, Susanna. "Some further reflections on the Directive (EU) 2016/681 on PNR data in the light of the CJEU Opinion 1/15 of 26 July 2017". *Revista de Derecho Político*, 1(101), 2018: 899- 928, p. 902

privacy protection and cross-border movement of data[18] while the Council of Europe introduced *Convention 108*[19] as a treaty specifically designed to prevent potential abuse in data processing.

In the 2000s two key legal instruments within the European Union (EU) played roles in shaping data protection legislation: the Charter of Fundamental Rights of the European Union[20] (CFR), which recognized with Article 8 a separate right to data protection, and the Lisbon Treaty[21], which has elevated this right to fundamental right.

Subsequently, this first section provides an overview of data protection laws and highlights changes that have occurred over time. The journey of evolution began when the Data Protection Directive[22] (DPD) was introduced in 1995. Its purpose was to bring consistency to data protection laws across EU member states and establish a framework for handling and safeguarding data. However, as technology advanced, the shortcomings of the Directive appeared evident. In this renewed context new challenges emerged that called for an updated approach to data protection. In response to these changes in 2016 the General Data Protection Regulation[23] (GDPR) was enacted. The GDPR can be seen as a revision of the 1995 Directive, introducing responsibilities and reinforcing the rights and guarantees of individuals.

The second section of this chapter clarifies two terms that will frequently appear throughout this dissertation: Passenger Name Record (PNR) data and Advance Passenger Information (API) data. While PNR data is information on passengers created after the purchase of a ticket, API data is information about passengers gathered by airlines at check-in and extracted from the machine-readable part of the passport.

The EU started to engage in negotiations with third countries regarding the sharing of PNR data in the wake of the 11 September 2001 terrorist attacks, in order to quickly

[18] OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* 1980.
[19] Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 1981
[20] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02.
[21] European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 13 December 2007, 2007/C 306/01
[22] Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJL 281, 23 November 1995.
[23] 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) (Text with EEA relevance). OJ L 119. 4.5.2016.

comply with the demands of recently passed US laws. Indeed, European airlines were under urgent pressure to adhere to these strict regulations.

These terrorist attacks forced a review of aviation security on a worldwide scale and called for expanded data sharing to strengthen counterterrorism operations. As part of their attempts to strengthen security measures, also Canada and Australia started to show interest in obtaining access to PNR data. The European Union saw the significance of developing structured agreements in light of this shifting environment in order to allow the transfer of PNR data while maintaining a balance between preserving individual privacy and fulfilling security requirements.

Lastly, this chapter traces the journey towards the adoption of the EU PNR scheme, that is the PNR Directive[24], which faced obstacles and controversies since the initial dialogues in 2003 and was only approved in 2016. The objective of this Directive is to enhance security for flights by facilitating the collection and analysis of PNR data, which is crucial for preventing detecting, investigating and prosecuting offences and serious crimes.

The adoption and implementation of this Directive exemplify the EU's dedication to striking a balance between security needs on the one hand while addressing concerns about data protection and privacy on the other.

[24] 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. 4.5.2016.

Section 1 – The European Data Protection Regime: An Overview

1.1. The genesis of the right to data protection

After the end of World War II, various international instruments such as the 1948 Universal Declaration of Human Rights (UDHR)[25] and the 1950 European Convention on Human Rights (ECHR)[26] along with most European constitutions acknowledged the importance of safeguarding individuals' privacy, family life, home and correspondence. However, it wasn't until the 1970s[27] that any legal system recognized the need to comprehensively safeguard information or data pertaining to people (referred to as 'data subjects) in order to protect their rights and interests.

The 1970s marked an era characterized by the use of automated processing systems and the accumulation of vast amounts of personal data. As society grappled with the implications brought by these advancements it became evident that legal safeguards for data were necessary. [28]

In particular, advancements in data processing and the introduction of computers enabled administrations and large organizations to establish expansive databases. This facilitated the collection, processing and interlinking of data on a larger scale. Recognizing the risks that came with this trend, the Council of Europe took steps to establish a framework consisting of principles and norms aimed at preventing the unjust collection and processing of personal data.[29]

In 1970, the German state of Hessen took the lead in Europe by enacting the first law explicitly addressing the issue of the protection of personal data. This important milestone was followed by Sweden's initiative in 1973 to introduce its national data protection laws, with Germany following suit in 1977 and France in 1978. These

---

[25] United Nations General Assembly. *The Universal Declaration of Human Rights (UDHR)*. New York, 1948. Article 12: **"**No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[26] Council of Europe. *European Convention on Human Rights (ECHR).* 1953. Article 8(1): "Everyone has the right to respect for his private and family life, his home and his correspondence."

[27]European Parliament. *Understanding EU Data Protection Policy*. p. 2. Accessed June 16, 2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf.

[28] Erdos, David. "The Development of European Data Protection Law and Regulation." *European Data Protection Regulation, Journalism, and Traditional Publishers*, 2019, 35–54. p.36

[29] Council of Europe. "Convention 108 and Protocols - Background." Accessed June 16, 2023. https://www.coe.int/en/web/data-protection/convention108/background.
To initiate progress in this direction, in 1973 and 1974 through the Council of Europe adopted Resolutions (73) 22 and (74) 29. These resolutions laid out fundamental principles aimed at safeguarding personal data stored in automated databases, both within the private sector and the public sector.

legislative measures were prompted by different factors: Germany's laws emerged in response to surveillance measures imposed by the state, while France and Sweden's actions reflected a strong culture of privacy.[30] These early developments in European countries laid the foundations for broader discussions and initiatives regarding data protection.

During the 1980s efforts were made to harmonize the growing number of data protection laws.[31] This was achieved through the adoption of *Guidelines*[32] by the Organisation for Economic Cooperation and Development (OECD) in 1980 and the establishment of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[33] in 1981 by the Council of Europe. The latter, known as *Convention 108*, was a significant development as it became the first legally binding international instrument aimed at protecting individuals from potential abuses arising from data processing.[34] This Convention has been ratified by all 47 Council of Europe members, except for Turkey.

1.2. The Data Protection Directive (DPD) – Directive 95/46/EC

For many years the main tool for the protection of personal data in the EU was the Data Protection Directive (DPD) or Directive 95/46/EC, which originated from Convention No. 108[35] of the Council of Europe.

However, while the Council of Europe made significant progress in placing 'data protection' on the agenda and outlining the key components of a legal framework, it faced challenges in ensuring consistent implementation across its member states. Some member states were slow in adopting Convention 108, and those that did implement it had varying outcomes, including placing restrictions on data transfers to other member states.[36]

---

[30] European Parliament. *Understanding EU Data Protection Policy*. p.2-3. Accessed June 16, 2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf.
[31] *Ibidem*
[32] OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* 1980.
[33] Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 1981
[34] Evans, A. C. "European Data Protection Law." *The American Journal of Comparative Law* 29, no. 4 (1981): 571-582. p.578
[35] Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 1981
[36] Hustinx, Peter. "EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation." *Oxford Scholarship Online*, 2017. p.131

This lack of uniformity and consistency raised concerns for the European Commission as it could impede the growth of the market in areas where handling personal data was increasingly crucial such as the free movement of people and services.[37] As a result in 1995 the Commission introduced Directive 95/46, the Data Protection Directive (DPD) to address this matter. During that time, the European Union, with its focus on the unified market, prioritized data protection measures to prevent the violation of individuals' rights by market actors and government agencies operating as service providers.[38]

Member States were required, under this Directive, to safeguard the fundamental rights and freedoms of individuals, specifically their right to privacy when it comes to the handling of their data. Moreover, Member States were not allowed to limit or prohibit the unrestricted movement of personal data between Member States.[39] Both obligations are closely connected and aim to ensure a consistent and robust level of protection across all Member States, promoting a fair development of the internal market.[40]

As far as the scope of material application is concerned, according to Article 3, the Directive was *"applicable to the processing of personal data, whether fully or partially automated, as well as to the processing of personal data that is not automated but is part of or intended to be part of a filing system."*[41] However, two exceptions existed: firstly, processing that falls beyond the boundaries of Community (now Union) law, particularly when it pertains to public security, defence, state security, or criminal law enforcement. Secondly, processing is performed by an individual within the context of purely personal or household activities.[42] The Court invoked the exception for data processing related to public security and criminal law enforcement in a significant case concerning the transfer of airline passenger data to the US for border protection after the terrorist attacks on September 11, 2001.[43] According to the CJEU, processing data for

[37] Kranenborg, Herke. "Access to documents and data protection in the European Union: On the public nature of personal data". 2008., 45, *Common Market Law Review*, Issue 4, pp. 1079-1114. p.1084
[38] Bignami, Francesca. "Privacy and Law Enforcement in the European Union: The Data Retention Directive." *Chicago Journal of International Law*, Article 13, Volume 8, no. 1. 2011: 233–55. p.234
[39] Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJL 281, 23 November 1995. Art. 1.
[40] Hustinx, Peter. op. cit. p. 131
[41] Directive (EU) 95/46/EC Art. 3(1).
[42] Ibid. Art.3(2).
[43] CJEU, Joined Cases C-317/04 and C-318/04, 2006, at 56-59 and 67-69.

such purposes is “outside the scope of the protection afforded by Directive 95/46/EC according to its Article 3 paragraph 2.”[44]

The Directive's territorial scope covered the processing of personal data that occurred within an EU Member State in connection with the activities of a controller[45]'s establishment, regardless of the location where the data processing took place.[46] This criterion also determined the applicability of national law within the EU: if the controller was not established in the EU, the relevant law was determined by the Member State where the processing means were located. Moreover, the Directive applied the principle that data can only be transferred to third countries, if those ensure an *adequate level of protection*.[47] This principle applied to the transfer of PNR data to third countries and aimed to prevent any circumvention of EU data protection guarantees. The CJEU in the Schrems[48] case has clarified the term “adequate level of protection”:

> *“The term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.”*[49]
>
> .

Furthermore, Member States were given the authority to establish specific conditions for lawful personal data processing.[50] This granted them too much discretion over the transposition of the Directive. [51]

Chapter II of the Directive established in Article 7 six criteria that outline the conditions for ensuring the legitimacy of data processing, which was only possible:

1) if the data subject *unambiguously consented*, or

2) if processing is *necessary* for the performance of a contract to which the data subject is party,

---

[44] Ibid.
[45] Art.2(d) of the Directive defines the ‘controller' as an individual or organization, whether it be a person, public authority, agency, or any other entity, that independently or jointly with others decides the objectives and methods of processing personal data.
[46] Directive (EU) 95/46/EC. Art.4.
[47] Ibid. Art. 25
[48] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015
[49] Ibid. at 73
[50] Directive (EU) 95/46/EC. Art. 5.
[51] Hustinx, Peter. op. cit. p. 132

3) for compliance with a legal obligation, for the performance of a government task, to protect the vital interests of the data subject, or to protect the legitimate interests of the controller, except where such interests are overridden by the interests of the data subject.[52]

Moreover, there was the prohibition of processing personal sensitive data, such as data *"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life"*[53] with two exceptions: either obtaining explicit consent from the data subject or meeting specific conditions, such as those related to the use of health data in healthcare settings. Member States had the option to grant derogations under national provisions that offer *"suitable safeguards."*[54]

As another guarantee, Member States had the obligation to ensure that the data controller or their representative provided the data subject, from whom their personal data is being collected, with the following information:

a) The identity of the data controller and their representative.

b) The purposes for which the data will be processed.

c) Additional information *"as necessary to ensure fair processing based on the specific circumstances of data collection."*[55]

Moreover, it was crucial for Member States to guarantee that each individual had the right to obtain confirmation, without undue delay or excessive cost, on whether their data was being processed, access to the processed data and its source, understanding of the logic behind automated decisions, and, where necessary, rectification, erasure, or blocking of non-compliant data.[56] In relevant cases third parties should also be notified unless it is impossible or requires a disproportionate amount of effort.[57]

The Directive also provided for the establishment of independent supervisory authorities responsible for overseeing the implementation of the provisions established by the Member States in accordance with the Directive.[58]

[52] Directive (EU) 95/46/EC Art. 7.
[53] Ibid. Art.8 (1)
[54] Ibid. Art. 8 (2b)
[55] Ibid. Artt. 10-11
[56] Ibid. Art. 12
[57] *Ibidem*
[58] Ibid. Art.28

1.3. The right to data protection in the Charter of Fundamental Rights of the EU

In December 2000, the Charter of Fundamental Rights of the European Union (CFR) was solemnly proclaimed in Nice by the European Parliament, the Council, and the European Commission. Chapter II of the Charter, titled "Freedoms", contains two Articles relevant for the protection of personal data: Article 7 and Article 8.

Article 7, which guarantees the right for private and family life, establishes that *"Everyone has the right to respect for his or her private and family life, home and communications"*, echoing Article 8 of the ECHR[59], which enshrines a right to respect for private life.

Article 8 of the CFR, instead, introduced "a constitutional recognition of the right to data privacy in the EU legal order"[60], asserting that:

"1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."

Hence, when considered in light of the ECHR, Article 8 of the CFR represents an "innovation"[61], because the ECHR does not enshrine an *additional* right on the protection of personal data.

In a broader sense, by separating the right to the protection of personal data from the right to respect for private and family life, the home, and communications, the Nice Charter differs from both the ECHR and other international human rights instruments.[62]

However, it must be clear that these two articles are not absolute[63] and need to be read in conjunction with the Charter's Article 52, on the 'Scope of guaranteed rights', and in particular with its first paragraph, which establishes that:

---

[59] Council of Europe. *European Convention on Human Rights (ECHR).* 1953. Article 8(1): "Everyone has the right to respect for his private and family life, his home and his correspondence."
[60] Tzanou, Maria. "Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right." *International Data Privacy Law* 3, no. 2 (2013): 88–99. p.93
[61] Fuster, Gloria González. *Emergence of personal data protection as a fundamental right of the EU*. Cham: Springer, 2014. p.199.
[62] Kranenborg, Herke. "Article 8 – Protection of Personal Data." *The EU Charter of Fundamental Rights*, 2022, 231–290.
[63] Fuster, Gloria González. *Emergence of personal data protection as a fundamental right of the EU*. Cham: Springer, 2014. p.201

"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

The words of Article 52(1) recall to some degree the content of the ECHR[64], indeed both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR) apply the same jurisprudential framework of (1) a basis in law, (2) legitimate purposes, and (3) proportionality to check whether an interference with the right to privacy and protection of personal data can be accepted or not.[65]

The entry into force of the Lisbon Treaty in December 2009 had a profound impact on the development of data protection law within the European Union.[66] First of all, the Charter became legally binding not only for EU institutions and bodies but also for the Member States of the European Union: under Article 6(1) of Treaty on the EU (TEU), "*The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights […] which shall have the same legal value as the Treaties."*

In the second place, the Lisbon Treaty introduced another key provision that solidifies the significance of data privacy rights within the EU's constitutional framework. Indeed, according to Article 16 of the Treaty on the Functioning of the European Union (TFEU), *"Everyone has the right to the protection of personal data concerning them."* The second paragraph of the same provision grants the European Parliament jointly with the Council, the power to *"lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."* As a matter of fact, the EU's institutional structure underwent a significant transformation with the implementation of the Lisbon Treaty. The Maastricht Treaty's 'pillar' structure was abolished, and the role of the European Parliament also changed, from advisory to co-

[64] Ibid, p. 201.
[65] Bignami, Francesca, and Giorgio Resta. "Transatlantic Privacy and Regulation: Conflict and Cooperation." *Law and Contemporary Problems* 78, no. 4 (2015): 231–266. p.233
[66] Hustinx, Peter. "EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation." *Oxford Scholarship Online*, 2017. p.141

decision-making with the Council on new legislation proposed by the Commission.[67] The Court of Justice gained full judicial authority, and the Commission's role as the guardian of the Treaties was reinforced for enforcing EU laws. Consequently, data protection legislation in the former third pillar, previously adopted by the Council alone, had to be replaced with rules approved through co-decision by the Parliament and Council, aligning with Article 16(2) of the Treaty on the Functioning of the European Union.

1.4. The General Data Protection Regulation (GDPR)- Regulation 2016/679

In 2012, the European Commission put forward the proposal for a new legislation replacing Directive 95/46 for different reasons. Firstly, there was the need to modernize and update the regulatory framework to accommodate technological advancements and evolving data protection challenges.[68] The existing Directive was enacted back in 1995, and with the rapid development of digital technologies, there was the need to have a more comprehensive and updated legal framework. Additionally, the Commission aimed to address discrepancies and variations in data protection regulations among Member States. Indeed, a Directive is "a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals."[69] As a result, enforcement of Directive 95/46 varied greatly across EU Member States.[70]

The European Union recognized the necessity to harmonize data protection laws to ensure a consistent level of protection for individuals' data across Member States. The Commission intended to build a more uniform and harmonized approach to data

[67] European Parliament "Personal Data Protection: Fact Sheets on the European Union". Accessed June 20, 2023. Available at https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection. pp.1-2

[68] European Commission. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM(2012) 11, 25 January 2012.

[69] European Union. "Types of Legislation". Accessed June 20, 2023. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.

[70] Directive (EU) 95/46/EC. Recital 9 of the Preamble reads "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC."

protection inside the EU by implementing new legislation in the form of a regulation. Indeed, regulations are legally binding acts that have direct implications for all Member States. They are uniformly applied throughout the EU, which means they are directly enforceable in each Member State, just like any local law. This makes them valuable when a consistent legal framework is desired across all territories of the Member States.[71] The transformation[72] of Directive 95/46 into Regulation 2016/679 involved a shift from harmonizing national regulations to achieving true uniformity of law in the European Union.[73]

Regulation (EU) 2016/679 consists of 173 recitals and 99 articles, compared to the 72 recitals and 34 articles of the 1995 Directive. The extensive nature of the text serves as a significant indicator of the European institutions' intention to introduce stricter regulations, reducing the leeway for operators in the field of personal data processing. Given the considerable volume of the legislation, only the most innovative aspects will be analysed.

The GDPR entered into force on 24 May 2016, repealing Directive 95/46/EC, and applies since 25 May 2018 to all types of organizations, irrespective of their location, that engage with the personal data of EU citizens.

The main objective of the GDPR, as stated in Article 1, is to protect the fundamental rights and freedoms of individuals and ensure the free flow of personal data within the European Union while promoting a high level of data protection.

In order to reach these objectives, the European legislator expanded the material and territorial scope of application. Indeed, the Regulation applies *"to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*"[74] and it applies to both organizations established within the EU and organizations outside the EU that deal with data of EU individuals or monitor their behaviour.[75] Thus, the main goal is to ensure that organizations, regardless of where they are located, follow the regulations and protect the data of individuals within the EU.

---

[71] Lenaerts, Koen, and Marlies Desomer. "Towards a Hierarchy of Legal Acts in the European Union? Simplification of Legal Instruments and Procedures." *European Law Journal* 11, no. 6, 2005.: 744–65. p.747

[72] For more on the Transformation of Directives into Regulations see Křepelka, Filip. "Transformations of Directives into Regulations: Towards a More Uniform Administrative Law?". *European Public Law* 27 (Issue 4), 2021: 781–806.

[73] Ibidem

[74] European Union. Regulation (EU) 2016/679. Art. 2

[75] Ibid. Art. 3.

This expansion of territorial scope signals the European Union's intention to establish its data protection legal framework as a robust model that extends beyond its own borders. According to Buttarelli, this demonstrates the EU's dedication to promoting strong data protection standards globally, emphasizing the importance of safeguarding individuals' rights regardless of territorial boundaries. [76] However, it is important to note that the Regulation does not apply to the processing of personal data in any case concerning public security, defence and State security that is to say for law enforcement purposes.[77] Thus, it does not apply to the PNR Agreements concluded by the EU with the US, Canada and Australia.

Then, Article 4, paragraph 1 contains a broad definition of 'personal data', demonstrating the growing importance of the right to the protection of personal data. Accordingly, 'personal data' means *"any information relating to an identified or identifiable natural person ('data subject')*;…".

At first, this definition may seem practically identical to the one contained in the former DPD, but it is possible to note that the European legislator has taken steps to adapt the concept of identifiability in response to technological advancements, providing a practical example of how individuals can be identified: *"..an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*[78]

With the emergence of new technologies, personal data related to electronic communications and geolocation have become crucial in determining an individual's identity. Recognizing this gap in the regulatory framework, the GDPR "supplements the DPD's list of potential 'identifiers' with 'location data' and 'online identifier' and adds a 'genetic' dimension to the 'identity' of a person."[79] Thus, any information that identifies a natural person is included in the category of 'personal data'. This is also confirmed by Recital 26 of the Preamble, which clarifies how the principles of data protection outlined

[76] Buttarelli, Giovanni. "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard." *International Data Privacy Law* 6, no. 2, 2016. pp. 77–78.
[77] European Union. Regulation (EU) 2016/679. Art.2(2)(d)
[78] Ibid. Art. 4
[79] Tosoni, Luca and Lee A. Bygrave. "Article 4(1). Personal data." In *The EU General Data Protection Regulation (GDPR): A Commentary the EU General Data Protection Regulation (GDPR): A Commentary*. 2020. p.108

in the Regulation do not apply to anonymous information that does not relate to an identified or identifiable individual, or to data that has been sufficiently anonymized to the point where the data subject cannot be identified.[80]

An interesting feature of the GDPR is Chapter II, Article 5, where the European legislator has identified 7 principles relating to the processing of personal data:

1. *Lawfulness, fairness, and transparency*: Personal data must be processed lawfully and in a fair manner, while ensuring transparency towards the data subject;
2. *Purpose limitation:* Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. *Data minimization*: The collection and storage of personal data should be limited to what is necessary for the intended purposes.
4. *Accuracy:* Personal data must be accurate, and reasonable steps should be taken to ensure that inaccurate or outdated data is rectified or erased.
5. *Storage limitation*: Personal data should be kept in a form that allows identification for no longer than necessary for the purposes for which it was processed.
6. *Integrity and confidentiality*: Personal data should be processed securely, protecting against unauthorized access, loss, or damage.
7. *Accountability*: Data controllers are responsible for complying with the principles of the GDPR and must be able to demonstrate their compliance.

The last principle represents an element of novelty in comparison to the DPD: now the controller must be able to demonstrate that the processing complies with these legal rules.[81] This risk-based framework for data protection lies at the heart of GDPR emphasizing that data controllers should consider potential risks to individuals' data and implement appropriate safeguards. This approach emphasizes the responsibility of data controllers, obliging data controllers to assess and mitigate risks associated with their data processing activities.[82] It intends to create trust between data subjects, controllers, and

[80]European Union. Regulation (EU) 2016/679. Recital 26.

[81] De Terwangne Cécile. "Article 5. Principles relating to processing of personal data" In *The EU General Data Protection Regulation (GDPR): A Commentary the EU General Data Protection Regulation (GDPR): A Commentary*. 2020. p.318

[82] Karjalainen, Tuulia. "All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm." *European Data Protection Law Review* 8, no. 1 (2022): 19–30. p.23

processors by stressing responsibility, openness, and the deployment of suitable technological and organizational safeguards.

Another notable aspect of the new risk-based approach is the introduction of a Data Protection Officer (DPO) as a crucial component of data protection governance. The DPO is a dedicated expert within an organization who is responsible for ensuring compliance with data protection laws and regulations.[83] The DPO plays a crucial role in ensuring that personal data is processed lawfully, transparently, and in accordance with the rights individuals have under the GDPR.

Furthermore, Regulation 2016/679 provides a framework that covers various aspects concerning data subjects. In addition to the requirement of obtaining valid consent for data processing activities outlined in Article 7, the GDPR provides robust protections for data subjects by granting them several rights.[84] These rights include but are not limited to:

1. the right to be informed about the collection and use of their personal data (Articles 13 and 14)
2. the right to access their data (Article 15)
3. the right to rectify inaccurate information (Article 16)
4. the right to request erasure or restriction of processing, also known as "the right to be forgotten" (Article 17)
5. the right to data portability (Article 20) [85]
6. the right to object to processing (Article 21)
7. safeguards against automated decision-making (Article 22).

These rights empower individuals to exercise control over their personal data and ensure transparency and accountability from organizations handling their information.

As far as transfers of personal data to a third country or an international organization, the Regulation has confirmed the existing approach based on Directive 95/46, stipulating that such transfers are prohibited, in principle, unless specific safeguards, listed in hierarchical order by the Regulation, are in place:[86]

[83] European Union. Regulation (EU) 2016/679. Art.39
[84] *Ivi.* Chapter III. Rights of the data subject. Articles 12-22
[85] Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another data controller when the processing is based on consent or a contract.
[86] European Union. Regulation (EU) 2016/679. Art. 46

1) Adequacy decision: pursuant to Article 45, the European Commission has to evaluate whether a third nation, territory, a specialized sector within a third country, or international organization ensures an adequate level of data protection. The adequacy decision of the European Commission is based on an examination of the third country's data protection laws, regulations, and practices and the consideration of "the specific circumstances surrounding a certain data transfer operation, such as the nature of data, the purpose and duration of the processing, and the rules in force in the non-EU State."[87] If an adequacy decision is made by the Commission personal data can be transferred without requiring any authorization.

2) Appropriate Safeguards: in the absence of an adequacy decision, the transfer may still be permitted if appropriate safeguards are in place to protect the personal data. These safeguards can include:

a. Standard Contractual Clauses (SCCs): the transfer is governed by specific clauses approved by the European Commission that provide adequate protection to the personal data being transferred.[88]

b. Binding Corporate Rules (BCRs): multinational companies can establish their own internal rules regarding data transfers, which are legally binding and ensure an adequate level of protection.[89]

c. Approved Codes of Conduct or Certification Mechanisms: transfers can be permitted if the data controller or processor adheres to an approved code of conduct or certification mechanism that provides adequate safeguards for the data.[90]

3) Derogations: in certain limited circumstances, derogations may apply, allowing data transfers without the need for an adequacy decision or specific safeguards. These derogations include situations where the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers, or when such transfer is necessary for an important reason of public interest, for the

[87] Lazzerini, Nicole, and Elena Carpanelli. "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum after Opinion 1/15 of the CJEU." *Air and Space Law* 42 (Issue 4/5), 2017: 377–402. p. 381
[88] European Union. Regulation (EU) 2016/679. Art. 46(2)(d)
[89] Ibid. Art. 47
[90] Ibid. Art. 46(2)(e)

establishment, exercise, or defence of legal claims, or to protect the vital interests of the data subject.[91]

Then, Article 51, the first Article of Chapter VI on independent supervisory authorities signals the beginning of the GDPR's second, more procedural section, in which these bodies play a crucial role.[92] It is important to note that, in contrast to the DPD's broad discretion granted to Member States, the GDPR under Article 51 lays out explicit regulations on the creation, responsibilities, and powers of independent supervisory authorities: the Data Protection Authorities (DPAs).[93] Should a personal data breach occur, according to Article 33 of the GDPR, the controller must promptly inform the relevant DPA under Article 55 within 72 hours of becoming aware of it, provided that such a breach poses a risk to individuals' rights and freedoms. However, if it is unlikely that the breach will have such an impact, notification is not mandatory. In situations where it is not possible to meet this 72-hour deadline for notification, the controller must provide an explanation for any delay along with their notification.

Moreover, Article 55 of the GDPR sets out the tasks of the supervisory authorities, which include promoting and monitoring the application of the GDPR, providing guidance and information to data subjects and organizations, handling complaints, and conducting investigations.

According to Article 58 of GDPR, supervisory authorities have a broad range of corrective powers at their disposal, such as the power to give orders to the controller or processor, to issue warnings or reprimands, to impose a limitation or ban on processing, and to impose an administrative fine for noncompliance.

Finally, it is important to underline that the EU data protection landscape is composed not only of the General Data Protection Regulation (GDPR), which is a *lex generalis,* but also of sectoral, more specific laws, such as *Directive (EU) 2016/680*, designated as the Data Protection Law Enforcement Directive (LED)[94] and *Directive*

[91] Ibid. Art. 49
[92] Hijmans Hielke, "Article 51 Supervisory authority". In *The EU General Data Protection Regulation (GDPR): A Commentary the EU General Data Protection Regulation (GDPR): A Commentary*. 2020. p. 867
[93] *Ibidem*.
[94] European Union. Directive (EU) 2016/680 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**.** OJ L 119, 4.5.2016

2002/58/EC, referred to as ePrivacy Directive (ePD)[95] that complement Regulation 2016/679.[96]

The LED came into effect on May 5, 2016, and EU Member States were required to incorporate its provisions into their national legislations by May 6, 2018. The purpose of this Directive is to ensure that individuals' right to data protection is respected when their personal information is used by law enforcement authorities *"for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."*[97] It specifically ensures that the personal data of crime victims, witnesses, and suspects are adequately safeguarded, and it facilitates international collaboration in combating crime and terrorism.

The ePrivacy Directive, instead, is a legislation of the European Union that governs privacy and data protection in electronic communications. It covers services such, as email, instant messaging, phone calls and other forms of communication. It lays down rules for the processing of personal data while transmitting and storing it over electronic networks. It also includes requirements to safeguard citizens' privacy such as obtaining consent for the use of cookies and the processing of traffic data.

Currently, the EU is developing an ePrivacy Regulation to complement the GDPR. The ePrivacy Regulation proposal intends to strengthen privacy protection in electronic communications, for example, by introducing new provisions on consent for the use of cookies and other tracking technologies, as well as stricter rules on the protection of electronic communications metadata.[98]

Section 2 - Passenger data in air travel as a security tool

2.1. The difference between API and PNR data

Recent acts of violence in various regions serve as stark reminders that terrorism continues to pose a significant concern for the international community. With its global

[95] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002

[96] Hudobnik, Matthias M. "Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?" *ERA Forum* 21, no. 3, 2020: 485–500. p.485

[97] European Union. Directive (EU) 2016/680. Art.1.

[98] European Commssion, Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017), 10 January, 2017

nature and cross-border implications, terrorism demands a coordinated response that encompasses various aspects of security. In response to this threat, several states deemed it necessary to implement new measures, and the utilization of PNR data for counter-terrorism purposes is precisely one of these measures. Indeed, advancements in technology have revolutionized the ability to transmit extensive quantities of personal data belonging to individuals.

In the post-9/11 landscape, aviation security immediately expanded: pre-flight security measures, such as the screening process before check-in and the restriction on carrying liquids onboard, have been reinforced by additional covert safeguards. These include collaboration between airlines and security authorities and the implementation of no-fly lists. Indeed, an inspection of a traveller and their travel documents is now just a minor component of border control processes for travellers arriving by air.

Most of the border control procedure is based on secure electronic data given by the traveller when they purchase a ticket or board an airplane. In any case, these measures must be in place before the traveller arrives in the destination country. This enables border agents to perform risk-based checks on both individuals and the objects they are carrying. Nonetheless, it is crucial to strike a balance between strengthening security measures and safeguarding individual rights, including privacy concerns, such as the protection of personal data.

The transmission of passenger-related data from airlines to border control authorities may be divided into two categories: Advance Passenger Information (API) and Passenger Name Record (PNR).

Advance Passenger Information (API) data is generated during the check-in process, and it involves "the capture of a traveller's biographic data and their flight details by the aircraft operator prior to departure and the transmission of that information by electronic means to the Border Control Agency in the departing and (or) destination country."[99] In other words, API data refers to the biographic details extracted from the machine-readable section of a passport. This information encompasses[100]:

a) the person's full name

b) place of birth

c) nationality

d) the number and type of travel document used

[99] WCO/IATA/ICAO "Guidelines on Advance Passenger Information (API)", 2022, p.4
[100] Council Directive 2004/82/EC, Art.3(2).

Additionally, it includes various itinerary specifics such as:

e) the border crossing point of entry into the territory of the Member States

f) code of transport

g) departure and arrival time of transportation

h) total number of passengers carried on that transport

i) the initial point of embarkation.

The use of advance passenger information (API) data serves as an efficient mechanism for conducting pre-arrival checks on air travellers.[101] This helps to speed up border checks for legitimate travellers while allocating more time and resource towards the identification of individuals who require additional scrutiny. As a result, API facilitates a risk-based, data-driven approach to border security.[102]

The significance of API data has been consistently emphasized, with repeated calls for its increased utilization by international organizations such as the United Nations (UN).[103] Additionally, the commitment of participating states in the Organization for Security and Co-operation in Europe (OSCE) to establish API systems further underscores the importance attributed to this data. Moreover, the International Civil Aviation Organization (ICAO) has mandated the establishment of national API systems as a standard since February 2018, making it obligatory for all countries that are Contracting States to the Chicago Convention.[104]

The regulation and transfer of API data within the European Union (EU) are guided by Council Directive 2004/82/EC, commonly known as the API Directive. This Directive imposes an obligation on air carriers to share passenger data with the destination Member State before the departure of the aircraft for inbound flights originating from a non-EU country.[105] The purpose of this requirement is to strengthen border controls and deter illegal immigration.[106] Moreover, Member States are authorized to utilize API data

---

[101] *Ivi*, p.27

[102] European Commission. "Border and Law Enforcement - Advance Passenger Information (API) Revised Rules." Migration and Home Affairs. Accessed June 30, 2023. https://home-affairs.ec.europa.eu/whats-new/border-and-law-enforcement-advance-passengerinformation-api-revised-rules_en

[103] UN Counter-Terrorism Committee Executive Directorate in a 2015 report called for the expansion of the use of advance passenger information (API) as a means to address the issue of foreign terrorist fighters. See more https://news.un.org/en/story/2015/06/501412 Accessed 25 June 2023.

[104] European Commission. *Supra* note 102. *Ibidem*.

[105] Council Directive 2004/82/EC, Art.3.

[106] Council Directive 2004/82/EC, Art.1.

for law enforcement purposes, including the fight against organized crime and terrorism, when certain conditions are fulfilled.[107]

It must also be noted that more and more countries are using interactive Advance Passenger Information (iAPI), a type of API that "interacts with the Border Control Agencies in real-time, allowing for an immediate response to be provided to a check-in agent with a boarding Directive".[108] This enhances the oversight capabilities of Border Control Agencies and airline operators, enabling them to identify individuals who are known or suspected to be a potential threat before they board a flight.

Passenger Name Record (PNR) data is "unverified information provided by passengers and collected by and held in the carriers' reservation and departure control systems for their own commercial purposes. It contains several different types of information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent at which the flight was booked, means of payment used, seat number and baggage information."[109] In other words, PNR is a database containing a series of commercial information[110] specifically related to:

a) Data that allows the identification of the passenger, accompanying individuals, and those who requested the reservation on their behalf, the agency or employee who made the reservation and/or issued the ticket.

b) Data concerning the itinerary for which the ticket was issued, as well as all other segments that constitute the complete route of a journey composed of multiple stops, hence involving multiple tickets.

c) Data concerning the means of payment, the passenger's credit card number, special conditions granted to specific categories (frequent flyers, members of special categories), email addresses, as well as physical home and work addresses, private and/or professional telephone numbers provided at the time of booking, the names of emergency contacts.

d) Data relating to a specific service connected to the person's health conditions, and dietary preferences.

[107] Council Directive 2004/82/EC, Art.6.
[108] WCO/IATA/ICAO "Guidelines on Advance Passenger Information (API)", 2022, p.5
[109] 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. 2 February 2011. p.3
[110] Annex I of the PNR directive contains the full list of PNR data (19 elements).

e) Specific remarks made by airline personnel.

f) If applicable, details about car rental and hotel room reservations.

However, it must be clear that PNR data are information voluntarily submitted by passengers when booking a ticket for a flight and only some of these elements are mandatory[111]. In particular:

- Name: the passenger's title (e.g., Mr., Mrs.), first name and surname are recorded.
- Itinerary: details about the flight, such as the airline name, departure date, cabin class, and arrival and departure cities or airports.
- Contact information: the passenger's phone number and email address (or those of the travel agent who made the booking on the passenger's behalf.)
- Ticketing information: the status and conditions of the flight ticket, including ticket number, fare details, payment status, and any restrictions associated with the ticket. Depending on how the booking was made, the flight ticket may not be issued immediately.
- Reference information: a reference to identify the person or entity responsible for creating the PNR and any subsequent modifications made to the booking.

These mandatory elements can be arranged in any order and can be subject to changes even after the initial reservation.[112] However, if any of these essential elements are missing, it becomes impossible to complete a booking, generate a PNR, and acquire a record locator for the booking.

Airlines have two options when it comes to sharing PNR data with authorities: they can either allow competent authorities to access the PNR information (the "pull" method) or they can send them the information electronically (the "push" method).[113] By receiving this information, border and security services can screen passengers for links to illegal activity, particularly terrorism and serious crime. The use and transfer of PNR data in the EU are regulated by the 2016 PNR Directive which will be further analysed in section 2.3.

[111] AltexSoft.*What Is PNR: Passenger Name Record Explained in Details.* 2021. Last accessed 20/07/2023 at https://www.altexsoft.com/blog/pnr-explained/.
[112] Ibidem
[113] Hobbing, Peter, "Tracing Terrorists: The EU-Canada Agreement" in PNR Matters CEPS Special Report/September 2008. p.11

Based on what has been described, it is evident that API and PNR data serve two different purposes. Indeed, while API data can assist law enforcement agencies in finding suspects and wanted individuals, its primary function is to confirm the identity of individuals travelling across borders. It provides essential information such as passport details, visa status, and flight itineraries, allowing authorities to verify the authenticity of travel documents and ensure that travellers match the information provided. By focusing on identity verification, API data plays a role in confirming the legitimacy of travellers and expediting border checks for *bona fide* passengers.[114] Furthermore, the information provided by API does not allow law enforcement agencies to evaluate passengers, thereby failing to assist in the identification of previously unrecognized criminals or terrorists.

Conversely, PNR data encompasses a broader array of unstructured details concerning a person's travel arrangements, enabling insights into aspects that may not be immediately apparent, such as travel habits, trends, religion, and behavioural patterns.[115] The collection and analysis of this information can lead to inferences on sensitive issues, such as the religion of certain individuals or their health conditions. [116]

As a matter of fact, the key distinction between API and PNR data lies in the source of information.[117] API data heavily relies on the passport information provided directly by the passenger, offering national officers more objective and enduring data for individual identification. On the other hand, PNR data relies on the information voluntarily submitted by the passenger to the reservation system.[118] It provides national officers with insights into the individual's background and potential connections with other individuals who may be of interest in ongoing investigations.

By combining and analysing API and PNR data, authorities can gain a comprehensive overview of an individual's information when entering or departing a

[114] European Commission. "Border and Law Enforcement - Advance Passenger Information (API) Revised Rules." Migration and Home Affairs. Accessed June 30, 2023. https://home-affairs.ec.europa.eu/whats-new/border-and-law-enforcement-advance-passengerinformation-api-revised-rules_en
[115] WCO/IATA/ICAO "Guidelines on Advance Passenger Information (API)", 2022, p.30
[116] Vagelis Papakonstantinou, and Paul De Hert. 2009. "The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic." *Common Market Law Review* 46 (Issue 3): 885–919. p.887
[117] Brouwer, Evelien. "Towards a European PNR System ? Questions on the Added Value and the Protection of Fundamental Rights: Think Tank: European Parliament." Think Tank. European Parliament, 2009. p.2
[118] Vagelis Papakonstantinou. *op. cit.* pp. 886-887

country. This consolidated data enables authorities to make accurate decisions regarding passenger admissibility and assess potential risks.

Thus, it is possible to affirm that PNR data complements API data along with additional information like visa applications and biometrics, creating a complete profile of the traveller's identity and travel arrangements, all of which are crucial for border enforcement purposes.[119] This comprehensive analysis involves comparing API and PNR data with relevant databases and applying targeting rules based on investigations and intelligence that highlight how terrorists and criminals exploit travel.[120] The ultimate objective is to identify travellers who may require additional scrutiny.

2.2. The EU bilateral agreements with third countries

As an inevitable consequence of the terrorist attacks on 11 September 2001, security at airports has been extremely heightened. The turning point was the adoption of the US Aviation and Transportation Security Act[121] (ATSA) on 19 November 2001. This act imposed an obligation on all airlines passing through the US to allow access to passenger-related data to the US Customs and Border Protection Bureau in order to proactively assess the potential threat each passenger may pose and thus ensure the identification of terrorists or individuals responsible for serious crimes.[122] Airlines that failed to adhere to ATSA regulations could face penalties in the form of fines or could be denied entry into the United States.[123] In other words, if the airline ITA Airways, had refused to provide the US Customs and Border Protection Bureau with the PNR data of a passenger who purchased a ticket from Rome Fiumicino to New York, in compliance with the provisions of Directive 95/46, the airline could have been subjected to a heavy fine or even denied the right to land in the United States.

Hence, European airlines had two options: either comply with Directive 95/46 or grant the US authorities access to the personal data of their transatlantic passengers.[124]

---

[119] WCO/IATA/ICAO "Guidelines on Advance Passenger Information (API)", 2022, p.30
[120] *Ibidem*
[121] US Aviation and Transportation Security Act 2001
[122] US Aviation and Transportation Security Act 2001, Sec. 115.
[123] VanWasshnova, Matthew R.. "Data Protection Conflicts between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange." *Case Western Reserve Journal of International Law* 39 (3), 2008: 827-865. p.833
[124] Louks, Douglas. "(Fly) Anywhere but Here: Approaching EU-US Dialogue Concerning PNR in the Era of Lisbon." *Indiana International & Comparative Law Review* 23, no. 3 (2013): 479–522. p.480

Caught between a rock and a hard place, the European Union found itself facing a difficult dilemma. To avoid financial losses, the EU airlines chose the latter option.

This is the reason why, following the enactment of the ATSA, negotiations commenced between the EU and the United States to establish conditions for an agreement addressing the transmission of the required passenger information. Eventually, despite the challenging circumstances, the EU and the United States managed to reach an agreement, which was signed on 28 May 2004.[125]

Shortly after the PNR Agreement came into effect, the European Parliament, that objected to the PNR Agreement at nearly every point of the process[126], initiated legal action against the Council and Commission of the EU, arguing that the agreement directly violated the privacy and data protection rights guaranteed by Directive 95/46/EC.[127] Indeed, as it was explained earlier, the Directive applied the principle that data can only be transferred to third countries, if those ensure an *adequate level of protection*,[128] and according to the EP this was not the case.

In 2006, the Court of Justice of the European Union (CJEU) invalidated the 2004 PNR Agreement due to a lack of legal basis.[129] Thus, it was more a procedural ruling than a substantive one.[130]

Indeed, on this occasion the CJEU had the opportunity to deliberate on issues about the protection of personal data, but it "eschewed this as the main focus in their decision related to a consideration as to whether the Directive's scope in processing personal data fell outside Community law."[131] As Kuhelj noted, "the CJEU did not take an explicit position on whether the PNR Agreement disproportionately encroached on the rights of EU citizens, but instead took an easier course and annulled the Council Decision and Commission Decision on formal grounds."[132]

---

[125] Council Decision 2004/496/CE of 17 May 2004 on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security, Bureau of Customs and Border Protection, OJ 2004 L 183/84.
[126] Louks, Douglas. "(Fly) Anywhere but Here: Approaching EU-US Dialogue Concerning PNR in the Era of Lisbon." *Indiana International & Comparative Law Review* 23, no. 3 (2013): 479–522. p.481
[127]CJEU. European Parliament v Council of the European Union and Commission of the European Community, Joined Cases C-317/04 and C-318/04, 2006, ECR I-4721.
[128] European Union. Directive 95/46/EC. Art. 25
[129] European Parliament v Council of the European Union and Commission of the European Community, Joined Cases C-317/04 and C-318/04, 2006, ECR I-4721.
[130] Louks, Douglas. "(Fly) Anywhere but Here: Approaching EU-US Dialogue Concerning PNR in the Era of Lisbon." *Indiana International & Comparative Law Review* 23, no. 3 (2013): 479–522. p.481
[131] Lowe, David. The European Union's Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?. *International Criminal Law Review*. 17, 2017: 78-106. p. 83
[132] Alenka Kuhelj. The Twilight Zone of Privacy for Passengers on International Flights Between the EU & USA, 16 *U.C. DAVIS J. INT'L L. & POL'Y,* 2010: *383*-408, p.400

In response, the EU Commission changed the agreement to establish a proper legal basis while keeping the actual data transfer aspects unchanged.[133] In terms of rights protection there was only one improvement: instead of directly accessing PNR data, the US authorities were required to request its transmission from the carriers (a shift from the 'pull' to the 'push' system).[134] Subsequently, a second PNR agreement with the US was signed on 23 July 2007.[135] Because it was not founded on the first pillar[136], the European Parliament did not have the necessary power to challenge the validity of the 2007 PNR Agreement before the CJEU.[137]

The initial intention behind the 2007 PNR Agreement was for it to be valid until 2014, at the latest. However, the adoption of the Lisbon Treaty in 2009 made four significant amendments to the EU Treaties, that affected heavily the PNR debate.[138]

First, it declared the European Union's Charter of Fundamental Rights (CFR) has the same legal value as the Treaties.[139]

Secondly, the EU acceded to the ECHR under the Lisbon Treaty, placing its institutions and all Member States within the jurisdiction of the European Court of Human Rights (ECtHR).[140]

Third, the Treaty of Lisbon eliminated the previous pillar system by giving the European Parliament significantly more political and legislative authority.

Finally, the Lisbon Treaty changed the legislative process, giving the European Parliament more authority. The consultation procedure of legislative enactment, which

---

[133] Wilson, Kerianne. "Gone with the Wind?: The Inherent Conflict between API/PNR and Privacy Rights in an Increasingly Security-Conscious World." *Air and Space Law* 41, no. Issue 3, 2016: 229–264. p.253
[134] Vedaschi, Arianna. "Privacy and Data Protection versus National Security in Transnational Flights: The EU–Canada PNR Agreement." *International Data Privacy Law* 8, no. 2, 2018: 124–139. p.127
[135] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the EU, of an Agreement between the EU and the US on the processing and transfer of PNR data by air carriers to the US Department of Homeland Security.
[136] Louks, Douglas. "(Fly) Anywhere but Here: Approaching EU-US Dialogue Concerning PNR in the Era of Lisbon." *Indiana International & Comparative Law Review* 23, no. 3 (2013): 479–522. p. 481
Prior to the current status of the EU Treaties, the European Union once had a three-pillar structure that represented the various competencies allocated to the various institutions of the European Communities (Union). The EP had only the power to challenge legislation enacted in the first pillar. When the Commission switched the legal basis of the US-EU PNR agreement from the first pillar, which was covered by Directive 95/46, to another pillar, the EP could not challenge it anymore. For a more detailed explanation of the three-pillar structure see https://www.europarl.europa.eu/ftu/pdf/en/FTU_1.1.3.pdf
[137] Louks, Douglas. "(Fly) Anywhere but Here: Approaching EU-US Dialogue Concerning PNR in the Era of Lisbon." *Indiana International & Comparative Law Review* 23, no. 3 (2013): 479–522. p.481
[138] *Ibidem*
[139] European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 13 December 2007, 2007/C 306/01. Art. 6(1)
[140] Ivi. Art. 6(2)-6(3)

resulted in very limited involvement by the European Parliament, was replaced with the co-decision procedure between the Council and the European Parliament.

Thus, the Lisbon Treaty introduced a new legal framework that mandated the European Parliament's approval along with a Council Decision for international agreements to take effect. As a result, the European Parliament withheld its consent to the 2007 agreement as it believed that passengers did not enjoy sufficient guarantees for the protection of their rights,[141] and urged the European Commission to come up "with a coherent approach to the use of PNR."[142] In other words, the European Parliament urged the Commission to produce a single model for EU PNR Agreements with third countries.[143]

To this end, in September 2010, the Commission published a Communication setting out a global EU approach for the transfer of PNR data to third countries, including a "set of general criteria which were to be fulfilled by bilateral PNR agreements, including, in particular, several data protection principles and safeguards"[144] which should guide the EU in negotiating PNR Agreements with third countries.[145]

This was accompanied by three recommendations which asked the Council to authorise the negotiation of PNR Agreements with Australia, Canada and the United States of America.

Finally, a third PNR agreement between the EU and the US was signed and has been in force since 1 July 2012.[146] The European Parliament approved the 2012 Agreement by a vote of 409 to 226, with 33 abstentions. One might wonder why the Parliament approved the Agreement despite strong opposition from its members. As Juan

---

[141] Vedaschi, Arianna. "Privacy and Data Protection versus National Security in Transnational Flights: The EU–Canada PNR Agreement." *International Data Privacy Law* 8, no. 2, 2018: 124–139. p.127

[142] European Parliament. "Timeline of the EU-US PNR Agreements". News: European Parliament. 26-03-2012. Last accessed September 7, 2023 at https://www.europarl.europa.eu/news/en/press-room/20120326BKG41893/transfer-of-air-passengers-data-to-the-us-what-s-at-stake/7/timeline-of-the-eu-us-pnr-agreements.

[143] House of Commons - Documents considered by the Committee on 4 September 2013 - European Scrutiny Committee. Last accessed September 5, 2023. At https://publications.parliament.uk/pa/cm201314/cmselect/cmeuleg/83-xiii/8327.htm

[144] 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). 24 July 2020. p.2

[145] The Commission planned to modernize and simplify its approach regarding PNR agreements by considering current realities and developments since 2010. To achieve this goal, after a decade, it released a Roadmap on July 24, 2020, to outline the policy goals and significant legal and operational challenges that a revised strategy should address in the future.

[146] Agreement between the United States of America and the European Union on the use and transfer of PNRs to the US Department of Homeland Security, OJ 2012 L 215/13

Santos Vara observes this is due, on the one hand, to the fact that the US threatened to halt visa-free travel for EU citizens to the US in the event that the EP voted against the PNR deal.[147]

On the other hand, the author believes that the reason for the shift in the Parliament's stance is because it felt heard and included in the negotiating process by the key players.[148] In conclusion, the European Parliament, according to the author, is more interested in asserting its new position in the negotiation and conclusion of international treaties in the area of police and judicial cooperation in criminal matters than in influencing the substantive content of the transatlantic agreement. [149]

This view is confirmed by the 2011 PNR Agreement with Australia.

The first EU-Australia PNR Agreement was signed by the Council on 30 June 2008. However, the EP in its Recommendation[150] of 2008, stated its negative assessment of the EU-Australia PNR Agreement. In its critical evaluation the EP "observed that the procedure followed by the Council completely lacked democratic legitimacy since the European Parliament had not even been informed on the adoption of the mandate, the conduct of the negotiations or the conclusion of the Agreement."[151]

Then, with the entry into force of the Lisbon Treaty, the existing agreement had to be reviewed. Thus, in 2010 a new round of negotiations started, and it lasted almost two years. On 22 September 2011, the Council, with Decision 2012/380/EU98[152] authorized the signing of the new PNR Agreement on behalf of the EU, which was successfully approved by the European Parliament on 27 October 2011.[153] The new EU-Australia PNR Agreement entered into force on 1 June 2012 and is still valid.

---

[147] Santos, Juan. "The Role of the European Parliament in the Conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon." SSRN, April 25, 2014. p.28-29
[148] *Ibidem*
[149] *Ibidem*
[150] European Parliament Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, OJEU C 81E, 15.3.2011, p. 70.
[151] Francesco, Rossi dal Pozzo. *EU legal framework for Safeguarding Air Passenger Rights*. Cham: Springer, 2016. p.115
[152] Council Decision 2012/381/EU of 13 Dec. 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record data by air carriers to the Australian Customs and Border Protection Service, OJ 2012 L 186/3.
[153] Francesco, Rossi dal Pozzo. *EU legal framework for Safeguarding Air Passenger Rights*. Cham: Springer, 2016. p.115

To summarize, the EU found it necessary to establish bilateral PNR Agreements with the United States as an urgent response to comply with new US PNR regulations. This measure was taken when European airlines faced immediate pressure to adhere to these rules. In the meantime, other third countries requested access to PNR data. Currently, the European Union has negotiated PNR bilateral agreements with the United States, Australia and Canada.

Among the mentioned bilateral agreements, the one between the European Union and Canada is particularly relevant for this thesis and will be examined in detail in the next chapter.

First of all, it is the most recent of the three accords, since it was signed in 2014. As a result, it is most likely to better give a representation of the EU's thinking on how to balance security and privacy in the context of exchanging PNR data.

Second, this specific Agreement faced a legal dispute initiated by the European Parliament, which contended that it did not sufficiently protect the privacy of EU citizens.

Indeed, with Opinion 1/15 of July 2017, the Court of Justice of the EU evaluated for the first time the compatibility of an international agreement with the fundamental rights enshrined in the EU Charter of Fundamental Rights.

By declaring this Agreement incompatible with the Charter, the CJEU demonstrated its strong commitment to safeguarding privacy and upholding data protection standards.

Furthermore, the Opinion of the Court holds far-reaching implications, raising questions about the compatibility of existing PNR Agreements with the US and Australia and also impacting the international relations of the Union and the future of the EU PNR framework, which includes the regional scheme introduced by Directive 2016/681/EU[154]. Thus, analysing the EU-Canada PNR agreement is the starting point for studying the CJEU's approach to the delicate balance between privacy and security.

2.3. The PNR Directive

> "The talks with third countries on the transfer of PNR data should be complemented and to the extent possible preceded by the development of an EU policy on the use

[154] European Union. *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, 4.5.2016.*

> of PNR and/or travellers' data more generally within the Union. Such a policy will have to strike a balance between the different interests involved, in particular between legitimate security concerns and the protection of fundamental rights, including privacy."[155]

As it is possible to see from this 2003 statement of the Commission, discussions about the establishment of a legal framework to share passenger data had started early on within the EU. This statement also shows that the development of the EU PNR Directive was not only driven by norm convergence, but it addressed previously existing interests and convictions.[156] Notwithstanding that, its delayed adoption suggests it was a contentious and debated issue.

The first European Commission proposal for an EU PNR Directive failed to be adopted before the entry into force of the Lisbon Treaty, which made necessary a substantial review to obtain the support of the European Parliament.[157] In 2010, the European Council called upon the Commission to propose a Union measure on PNR data for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences and serious crimes, based on a thorough impact assessment.[158]

In 2011 a new proposal was presented, but it was rejected in 2013 by 30 votes to 25 by members of the LIBE Committee, the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament which raised concerns about the necessity and proportionality of the proposed EU scheme, as well as the duration for which data would be retained. Additionally, considering the European Court of Justice's decision to invalidate the data retention Directive[159], the European Parliament emphasized the importance of evaluating the Court's ruling before moving forward with any new measures.

---

[155] Commission of the European Communities. Communication from the Commission to the Council and the Parliament on the Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach. COM(2003). 16 December 2003, p.8

[156] Obendiek, Anke Sophia. "Passenger Data in Air Travel Establishing Data as a Security 'Tool.'" Essay. In *Data Governance: Value Orders and Jurisdictional Conflicts*. Oxford, United Kingdom: Oxford University Press, 2023. p. 121

[157] Brouwer, Evelien. op. cit. p.9

[158] European Council. The Stockholm Programme An open and secure Europe serving and protecting citizens (2010/C 115/01) (OJ C 115, 4.5.2010), 2010, p.12.

[159] CJEU. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Karntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, 2014, ECR I-238

It is only after the two tragic terrorist attacks in Paris in 2015, in a fearful and mutated political climate, that the European Parliament committed to finalizing an EU PNR Directive by the end of 2015 and also encouraged the Council to make progress on the Data Protection package[160], aiming for parallel discussions on both issues.[161]

However, despite the sense of widespread insecurity and urgency, it was not until 14 April 2016, after further terrorist attacks took place, specifically in Brussels, that the text of the Directive was approved by plenary with 461 votes in favour, 179 against, and 9 abstentions.[162] It was then passed in the first reading on 21 April and signed by the presidents of the European Parliament and Council on 27 April 2016, with the data protection package. According to some, the EU managed to "both strengthen and weaken its privacy on the same day."[163]

One year later, specifically on December 21, 2017, the United Nations Security Council, on a unanimous basis adopted Resolution 2396 to combat international terrorism[164]. This resolution, operating under Chapter VII of the UN Charter, requires countries to develop the capacity to collect, process, and analyse PNR data. The main objective is to prevent, detect, and investigate terrorist offences, as well as track related travel activities. The resolution shows the "efforts to broaden PNR analysis and sharing globally"[165], encouraging the sharing of PNR data with other countries for enhanced security measures. As a result, the EU PNR regime encompasses a global dimension that goes beyond the European Union and includes cooperation with third countries.[166] This is especially true in the context of counterterrorism efforts. Indeed, as it was described earlier, the EU negotiated and concluded bilateral agreements with third countries such as the United States, Australia, and Canada on the transfer of PNR data.

---

[160] The data protection reform package consists of two draft laws: a general regulation covering the bulk of personal data processing in the EU (the GDPR) and a directive on processing data to prevent, investigate, detect or prosecute criminal offences or enforce criminal penalties (the LED)

[161] European Parliament resolution of 11 February 2015 on anti-terrorism measures (2015/2530(RSP). Paragraph 13.

[162] European Parliament. "EU Passenger Name Record (PNR) Directive: An Overview: News: European Parliament.". June 1, 2016. https://www.europarl.europa.eu/news/en/press-room/20150123BKG12902/eu-passenger-name-record-pnr-directive-an-overview.

[163] Krahulcova, Estelle Massé, Lucie. 2016. "The Stormy Seas of Privacy in Europe." Access Now. April 14, 2016. https://www.accessnow.org/stormy-seas-privacy-europe/. Accessed 3 July 2023.

[164] UN Security Council. Resolution 2396. 21 December 2017, paragraph 12

[165] Propp, Kenneth. "Avoiding the next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data." *Atlantic Council.* July 1, 2021.

[166] Olsen, Henrik Palmer, and Cornelius Wiesener. "Beyond Data Protection Concerns – the European Passenger Name Record System." *Law, Innovation and Technology* 13, no. 2, 2021: 398–421., p. 401

Hence, looking at the EU PNR regime, it might be helpful to clarify the distinction between the EU PNR Directive and the EU PNR Agreements made with third countries. The latter refers to agreements that have been negotiated between the European Union and individual third countries to establish the terms and conditions for exchanging PNR data of EU passengers between the authorities of the EU and the authorities of the respective third country, with the aim of strengthening security cooperation and combat terrorism and cross border crime.

It is precisely the existence of these PNR agreements with countries that has led to the creation of the EU PNR Directive because EU authorities did not automatically have access to PNR data shared with those third countries.[167] In other words, based on the EU-US PNR Agreement, Air France (a European airline) collects and processes the PNR data of passengers who have purchased a ticket to fly from Paris to Los Angeles. Then, Air France transfers the PNR data to the United States Department of Homeland Security (the US competent authority) with the aim of identifying potential threats to US security. In the opposite situation of a US airline operating a flight from Los Angeles to Paris, based on the EU-US PNR Agreement, the PNR data of passengers on that flight to France would not be transferred to the French competent authority, which in this case is the National Travel Data Agency (ANDV). Since the adoption of the EU PNR Directive, the National Travel Data Agency in France would receive the PNR data of passengers of extra EU flights, because the Directive requires airlines that operate flights outside of the European Union to send the information gathered during the booking and check-in procedures to a Passenger Information Unit (PIU), a competent unit of the EU country from which the flight departs or that of its destination.[168]

The primary objective of the PNR Directive is to bolster the security framework for international flights by facilitating the collection and exchange of PNR data between airlines and member state authorities.[169] By analysing these data, competent authorities can identify potential threats and take necessary measures to prevent, detect, and investigate terrorist offences and serious crimes. According to the Directive, serious crimes are offences "punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State."[170]

[167] Orrù, Elisa. 'The European PNR Directive as an Instance of Pre-emptive, Risk-based Algorithmic Security and Its Implications for the Regulatory Framework'. 1 Jan. 2022 : 131 – 146. p.133
[168] European Union. Directive (EU) 2016/681. Art. 1
[169] European Union. Directive (EU) 2016/681. Art.1.
[170] *Ivi.* Art. 3(9)

They include for example, participation in a criminal organisation, trafficking in human beings, sexual exploitation of children and child pornography, and illicit trafficking in narcotic drugs and psychotropic substances.[171]

To begin with, it must be noted that the Directive requires only the collection of PNR data of passengers of extra-EU flights (flights from third countries to the European Union or from the European Union to third countries).[172] However, there is also a provision that allows for the potential expansion of this regime to cover flights within the EU.[173] With the exception of Ireland and Slovenia, the overwhelming majority of EU member states have chosen to use this opportunity.[174] Hence, airlines are required to transfer passenger name record (PNR) data for flights to and from the EU to a dedicated newly established authority in each Member State, known as the Passenger Information Unit (PIU).[175] The PIUs are responsible for the collection, retention, and processing of PNR data, as well as for transferring them to the relevant authorities and exchanging them with the PIUs of other Member States and, when necessary, with Europol.[176]

Then, the Directive outlines the specific purposes for which PNR data can be processed. The PIUs will only process PNR data for the following purposes[177]:

(a) to assess passengers before their scheduled arrival or departure from the Member State. This assessment aims to identify individuals who may require further examination by competent authorities or Europol if there is suspicion of their involvement in a terrorist offence or serious crime.

(b) to respond to duly reasoned requests from competent authorities on a case-by-case basis. This involves providing and processing PNR data in specific instances for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences or serious crimes. The results of this processing are shared with the competent authorities or Europol, as needed.

(c) to update existing criteria or create new criteria for risk assessments.

---

[171] The complete list of 26 offences is contained in Annex II of the Directive (EU) 2016/681
[172] European Union. Directive (EU) 2016/681. Art. 1
[173] *Ivi.* Art.2.
[174] See Updated list of Member States who have decided the application of the PNR Directive to intra-EU flights as referred to in Article 2 of Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC1026(01)&rid=1 Accessed 2 July 2023
[175] European Union. Directive (EU) 2016/681. Art. 4(1)
[176] *Ivi.* Art.4.(2)
[177] *Ivi.* Art.6(2)

When comparing PNR data with predetermined criteria and databases, any positive results must be individually reviewed by non-automated means to determine if the competent authority needs to take action according to national laws.[178] The fundamental principle behind this requirement is to ensure that decisions that could have a negative legal impact on an individual or significantly affect them are not solely made based on the automated processing of PNR data without human involvement.

Art.9. of the Directive prohibits the "pull" method, by specifying that Member States are not permitted to directly access airline companies' databases[179]. Instead, the airlines themselves are responsible for sending the Passenger Name Record (PNR) data to the respective Passenger Information Unit (PIU) of the concerned Member State (the "push" method). In cases where it is necessary and pertinent, a Member State must provide PNR data on an identified individual to the competent authorities of another Member State. Moreover, the transfer of PNR data to non-EU countries is subject to specific conditions, that must be met before any transfer takes place.[180]

An interesting aspect concerns the several data protection safeguards that have been put in place to ensure the privacy and security of passenger data. These safeguards have been designed to comply with EU data protection regulations and uphold fundamental rights. Article 13 paragraph 4 of the Directive explicitly prohibits the processing of sensitive data, such as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation.

Furthermore, the Directive establishes five years as the maximum retention period,[181] but already after six months from the data transfer, all PNR data should undergo depersonalization by masking specific identifying elements that directly relate to the passenger (e.g. name, address and contact information, payment information, frequent flyer information, etc).[182] Upon expiration of the six months, data can be re-personalized

[178] *Ivi.* Art.6(5)
[179] *Ivi.* Art.9
[180] *Ivi.* Art.11
[181] *Ivi.* Art.12(1).
[182] *Ivi.* Art.12(2)

only if strictly necessary for fighting crime and if it has been approved by a judicial authority or a similar body.[183]

In addition to this, it must be noted that each PIU is required to designate a data protection officer who is responsible for supervising the processing of PNR data and ensuring the implementation of appropriate safeguards[184] and independent national supervisory authorities must oversee the processing activities of PIUs. These national supervisory authorities, as outlined in Article 15, are responsible for monitoring compliance with data protection rules, handling complaints, and conducting investigations to ensure the lawful and responsible processing of PNR data.

Under Article 18, Member States were required to enact legislation, regulations, and administrative measures needed to adhere to the PNR Directive by 25 May 2018 and promptly notify the Commission once these provisions have been implemented.[185] However, after the deadline for the transposition, few member states were able to transpose it. It is important to consider that prior to the Directive's implementation, the majority of Member States lacked an existing framework for the collection and processing of PNR data. Recognizing the challenges in terms of resources, time, and technical complexities involved in developing PNR systems that align with the Directive, the Commission adopted an Implementation Plan on November 28, 2016.[186] This plan acknowledged the difficulties and offered guidance to Member States, outlining the essential steps and measures required to establish a functional PNR system.[187]

Throughout the entire implementation process, the Commission has supported Member States by organizing regular meetings, facilitating the exchange of best practices and peer-to-peer assistance, and providing financial aid.[188]

Notwithstanding that, the report of 7 June 2018 stated that only 14 member states communicated to the Commission the measures they adopted to transpose the

[183] *Ibidem*.
[184] *Ivi.* Art. 5
[185] *Ivi.* Art. 18
[186]European Commission. Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. SWD(2016). 28 November, 2016.
[187] *Ivi*. p.3
[188] 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). 24 July 2020. p.3

Directive.[189] The Commission "has not hesitated to make use of its competencies as the guardian of the treaties to ensure that Member States comply with their obligation to transpose the Directive"[190] and in July 2018 responded to non-compliance with the Directive by initiating infringement proceedings.

Letters of formal notice were sent to fourteen Member States that had failed to communicate their complete transposition of the Directive.[191] However, in ten of these cases, the infringement proceedings were closed after the Member States later notified the Commission of their successful implementation of the Directive. By the end of the review period on 25 May 2020, 24 out of 26 Member States had officially informed the Commission that they had completed the process of transposing the Directive into their national legislation. However, Spain, which had not communicated any transposition measures, was brought before the Court of Justice on 2 July 2020 due to its failure to implement the Directive.[192] This unequivocally demonstrates the Commission's conviction that the use of PNR data is indispensable in the EU's approach to combat and counteract serious criminal activities and acts of terrorism.

Based on the information provided by the Member States, the Commission was supposed to conduct a comprehensive review of all aspects of this Directive by May 25, 2020, and then present a report to both the European Parliament and the Council.[193] However, the report was presented two months later, in July 2020.

The Commission's evaluation of the initial two years of implementing the Directive indicates an overall positive assessment. The review concludes that the Directive is effectively contributing to its primary objective of establishing efficient PNR systems in the Member States to combat terrorism and serious crime.[194] The Commission assessed that Member States had effectively incorporated data protection standards during

---

[189] See communication from the Commission to the European Parliament, the European Council and the Council. Fifteenth Progress Report towards an effective and genuine Security Union.COM(2018).13 June 2018. p.10
Those states are: Belgium, Croatia, Estonia, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Slovakia and the United Kingdom.
[190] 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). 24 July 2020. p.8
[191] *Ivi,* p.9
[192] *Ibidem.*
[193] European Union. Directive (EU) 2016/681. Art. 19.
[194] 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). 24 July 2020. p.11-12.

the transposition of the Directive and believed that "no amendments to the PNR Directive should be proposed at this stage."[195] Instead, the focus should be on ensuring the correct implementation of the Directive, especially considering practical issues that have emerged.[196]

[195] *Ibidem*
[196] *Ibidem*

Conclusion

Since the 1970s, there has been a growing focus on privacy, with the European Union being at the forefront of this development. As it has been shown, the EU is the first entity to explicitly recognize a right to the protection of personal data as an independent and distinct right, separate from the right to privacy.[197] In recent decades, the issue of privacy has gained significant importance in the global context, especially with the rapid advancements in technology and the widespread use of digital platforms. As individuals' personal data became more vulnerable to misuse, data breaches, and unauthorized access, the need to establish comprehensive data protection measures became evident. The European Union, recognizing the fundamental nature of privacy and its essential role in safeguarding human rights and individual liberties, took proactive steps to address these concerns.

The chapter has shown that cornerstone of the EU's approach to privacy is the General Data Protection Regulation (GDPR), which was adopted in 2016 and came into effect in 2018. The GDPR represents a groundbreaking legal framework that enshrines the rights of individuals to control their personal data and ensures that organizations handle this data responsibly and transparently. It establishes strict guidelines for the collection, processing, and storage of personal data, and imposes substantial fines on entities that fail to comply with its provisions. Moreover, one of the most important aspects of the EU's commitment to privacy and data protection is that it goes beyond its borders. Indeed, it applies to both organizations established within the EU and organizations outside the EU that deal with data of EU individuals or monitor their behaviour.[198] This is done to ensure that organizations, regardless of where they are located, follow the regulations and protect the data of individuals within the EU. Moreover, this extension of territorial scope shows the European Union's intention to develop its data protection legislative framework as a strong model that transcends national boundaries.[199] The EU's pioneering efforts in data protection have also influenced global privacy discussions and inspired other jurisdictions to develop their own privacy regulations. Many countries have sought to align their data protection laws

[197] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02. Art. 8
[198] European Union. Regulation (EU) 2016/679. Art. 3.
[199] Buttarelli, Giovanni. "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard." *International Data Privacy Law* 6, no. 2, 2016. pp. 77–78.

with the GDPR's principles to ensure consistency in the treatment of personal data across borders.

Another point that it is worth noting and that emerged from the second section of this chapter is that while on the one hand the European Union took a step forward in protecting citizens' data by implementing the GDPR, on the other hand it almost simultaneously adopted the much-debated EU PNR Directive. Scholars have criticized the EU's commitment to harmonising PNR legislations through the EU PNR Directive from the very beginning, due to the excessive interference it creates with the rights to privacy and data protection contained in the EU fundamental rights framework.[200] Collecting and processing air passenger information is part of the EU Security Union Strategy[201], but the transfer of PNR to other countries is a complex matter, this is demonstrated by the long and tortuous path that required more than 13 years in order for the PNR Directive to be adopted.

In conclusion, by gaining a comprehensive understanding of the European data protection landscape, of the need to enter into bilateral agreements with third countries, the PNR Directive and the context surrounding the use of passenger data as a security instrument, this chapter set the foundations for the subsequent analysis, shedding light on the historical, legislative, and conceptual aspects relevant to analyse the EU-Canada PNR Agreement and its implications. The following chapters will delve deeper into the specific details of this case study, examining its legal aspects concerning privacy and security.

[200] Kuşkonmaz, Elif Mendos. "The Grand Gala of PNR Litigations: Case C-817/19,Ligue Des Droits Humains v Conseil Des Ministers." *European Constitutional Law Review* 19, no. 2, 2023: 294–319. p. 299

[201] European Union. Communication from the Commission on the EU Security Union Strategy. Brussels, 24.7.2020. COM(2020) 605 final

CHAPTER II
The CJEU's Opinion 1/15 on the EU-Canada PNR Agreement: balancing privacy and security in cross-border passenger data sharing

Introduction

In a hyper-connect world, where increasingly sophisticated technologies are being used by state authorities to monitor the personal data and lives of individuals in the name of the need to combat terrorism and transnational crime, the fragile balance between public security and citizens' privacy has been the focus of legal, political, and ethical debates. This delicate balance is never more evident than in international data-sharing agreements aimed at improving security while protecting fundamental rights.

On 26 July 2017, the Grand Chamber of the CJEU delivered a leading legal precedent: by conducting a deep analysis of the EU-Canada PNR Agreement, it assessed for the first time the compliance of an international agreement with the rights enshrined in the European Union's Charter of Fundamental Rights. As some scholars have affirmed, "having the CJEU finally look at PNR schemes is a matter of great interest for all EU travellers, and not only them. Especially at a time like this, when it feels like surveillance is served to the people by states all over the world – from liberal democracies to authoritarian states, as an acceptable social norm."[1]

Given the importance of Opinion 1/15, this chapter goes into the CJEU's multidimensional evaluation, examining the delicate interplay between data privacy, security imperatives, and the pursuit of a sound coexistence of individual liberty and public safety. To begin with, the history of the adoption of the Agreement will be traced. Indeed, following the 11 September attacks, after the US imposed an obligation on all airlines passing through the US to allow access to passenger-related data to the US in order to actively fight the terrorist threat, Canada followed suit.

The first agreement on the sharing of PNR data between the EU and Canada was concluded in 2006 and it allowed the Canada Border Service Agency to access passenger data from airlines flying to or from Canada. After this agreement expired, a new one was

[1] Zanfir, Gabriela. "Analysis of the AG Opinion in the 'PNR Canada' Case: Unlocking an 'Unprecedented and Delicate' Matter." *pdpEcho,* November 3, 2016. Available at https://pdpecho.com/2016/09/12/analysis-of-the-ag-opinion-in-the-pnr-canada-case-unlocking-an-unprecedented-and-delicate-matter/ (last accessed 29/07/2023).

negotiated in 2014, but its adoption required the European Parliament's approval. Before granting consent, the Parliament sought the Court of Justice's opinion on the Agreement's compliance with key EU laws, specifically Article 16 of the Treaty on the Function of the European Union (TFEU) and Articles 7, 8, and 52(1) of the Charter of Fundamental Rights of the European Union (CFREU).

The chapter will shed light on how the Court has weighed the need to preserve public security against the right to privacy, providing a critical analysis of the choices made by the Court and the implications these may have for the future of passenger data in international relations.

The most significant aspects analysed by the Court will be closely scrutinised: from the appropriateness of the collection and transfer of passengers' sensitive data to the automated processing of data and the purposes for which it may be used, to the crucial question of the proportionality of the measures and safeguards for data subjects.

1. The EU-Canada PNR Agreement: a chronology

The Agreement between the European Union and Canada on the transfer of PNR data has a long history. In the direct aftermath of the 11 September terrorist attacks, there were concerns that the hijackers had entered the United States through Canada. For this reason, there was a pressing need for the Canadian government to swiftly address the emerging threat and allegations of inadequate border security.[2] At the same time Canada, like other nations, was required to adhere to United Nations Security Council resolution 1373 (2001) which called for the criminalization of international terrorism.

As a result, the Anti-terrorism Act (ATA)[3] was passed in 2001 by the Canadian government. Since 2002, air carriers have been required to provide the Canada Border Services Agency (CBSA) with Advance Passenger Information (API) and, beginning in 2003, with Passenger Name Record (PNR) data relating to all passengers travelling to or departing Canada.[4] The requirements for the transfer of personal data within the PNR of air passengers to the CBSA are established based on Section 107.1 of the Customs Act[5] and Paragraph 148(d) of the Immigration and Refugee Protection Act.[6]

On 6 September 2005, the Commission, by decision 2006/253/EC, considered that the CBSA was able to "ensure an adequate level of protection for PNR data transferred from the Community concerning flights bound for Canada."[7]

In light of this adequacy decision, under Art.25 of the EU Data Protection Directive, the Council of the European Union in 2006 was able to approve the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data.[8] In other words, the 2006 EU-Canada PNR Agreement was adopted without the European Parliament's consent, as it was based on the Commission adequacy decision.

---

[2] Graziani, Chiara & Vedaschi, Arianna. "National Security and Counter-Terrorism in Canada: Past, Present and Future.". *DPCE Online*. 2019. p. 754

[3] Government of Canada. *Anti-Terrorism Act*. SC 2001. C.41

[4] Government of Canada, Canada Border Services Agency. *Memorandum D2-5-11 - Guidelines for commercial air carriers for the processing of prescribed traveller information,* December 20, 2021.

[5] Government of Canada. *Customs Act R.S.C.* 1985. C.1 (2nd Supp.)

[6] Government of Canada. *Immigration and Refugee Protection Act*. S.C. 2001. C. 27

[7] European Commission. *Commission Decision of 6 September 2005 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the Canada Border Services Agency*. OJ 2005, 29.3.2006. L 91/49. Art.1.

[8] Council of the European Union. *Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record Data*. OJ L 86, 24.3.2006, p. 19–19

However, when the adequacy decision expired in 2009, just before the Treaty of Lisbon entered into force,[9] the agreement ceased to have effect.

The Lisbon Treaty was a turning point because, as it was described in the first chapter, it enhanced the European Parliament's role in the conclusion of agreements in the area of police and judicial cooperation in criminal matters. As a result, the procedure for the negotiation of PNR agreements was transformed.[10] Pursuant to Art. 218, para. 6, let. a), sub-let. v) TFEU, the European Parliament's approval became necessary to conclude PNR agreements.

On May 5, 2010, the European Parliament adopted a resolution[11] to initiate negotiations for PNR data Agreements with the United States, Australia, and Canada. The key objective was establishing a coherent approach for the use of PNR data in law enforcement and security, identifying a unified set of principles that would serve as the basis for the negotiation of Agreements with third countries.

The Communication issued by the Commission on 21 September 2010, regarding the global strategy for sharing PNR data with third nations declares that the European Union "has an obligation to itself and to third countries to cooperate with them in the fight against [terrorist threats and serious transnational crime]."[12] As a result, Agreements were signed and concluded with the United States and Australia, and after receiving the Parliament's approval, officially took effect in 2012.

Subsequently, on 19 July 2013, the European Commission adopted the Proposal for a Council decision on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data[13], containing the text of the proposed Agreement between Canada and the European Union. The proposal was sent to the European Data Protection Supervisor (EDPS) on 23 July 2013.

---

[9] Kuner, Christopher. "International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15 (EU-Canada PNR) of the Court of Justice of the EU." *Common Market Law Review* 55, no. Issue 3. 2018: 857–82. p. 861

[10] Santos, Juan. "The Role of the European Parliament in the Conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon." SSRN, April 25, 2014. p.9

[11] European Parliament. *Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) Agreements with the United States, Australia and Canada (2011/C 81 E/12).*

[12] European Commission. *Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries.* Brussels, 21.9.2010 COM(2010) 492 final.

[13] European Commission. *Proposal for a Council decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data.* Brussels, 18.7.2013 COM(2013) 529 final

The EDPS, Peter Hustinx, reviewed and provided his opinion on the proposals for the conclusion and the signature of the Agreement between Canada and the European Union on 30 September, 2013[14]. He raised several concerns regarding the necessity and proportionality of PNR schemes and bulk transfers of PNR data to third countries and questioned the choice of the substantive legal basis. Additionally, the EDPS made various observations and recommendations concerning different provisions of the envisioned Agreement.

Nonetheless, on 5 December 2013, the Council decided to proceed with the signature of the planned Agreement without amending it based on the EDPS's feedback. Thus, the Agreement was officially signed on 25 June, 2014[15], and by letter of 7 July, 2014, the Council sought the Parliament's approval for its decision.

On 25 November 2014, the European Parliament (EP) adopted a resolution[16] seeking an Opinion from the CJEU under Article 218(11) TFEU, which grants the EP the power to request the opinion of the Court on the compatibility of an international Agreement with the Charter of Fundamental Rights and the EU Treaties, before approving it. The European Parliament made use of its recently acquired powers from the Lisbon Treaty to engage the CJEU for the first time in a process of *ex-ante* review of the draft EU-Canada Agreement.[17]

The EP has continuously worked to ensure that PNR agreements adhere to the proportionality principle and the legislative framework for EU data protection.[18] However, the turning points which convinced the EP to refer to the CJEU were:

1) the CJEU decision Directive in *Digital Rights Ireland*[19], invalidating the Data Retention which allowed for unlimited data collection and storage

[14] EDPS. *Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data.* 30/09/2013, Brussels.
[15] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).*
[16] European Parliament. *Resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the EU on the transfer and processing of PNR data.* (2014/2966(RSP)).
[17] Zalnieriute, Monika. "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement." *The Modern Law Review* 81, no. 6. 2018: 1046–63. p.1051
[18] *Ibidem*
[19] CJEU. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Karntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, 2014, ECR I-238

2) the European Data Protection Supervisor's critical opinion[20], which questioned the appropriateness of PNR schemes and the selection of the legal basis, proposing the inclusion of Article 16 TFEU (personal data protection).

2. CJEU's Opinion 1/15

On July 26, 2017, the Court of Justice, with a Grand Chamber comprising 15 judges, issued a significant opinion regarding the EU-Canada Agreement on PNR data, by determining that the current version of the PNR Agreement could not receive approval due to several of its clauses being inconsistent with the fundamental rights recognized by the European Union.

This decision is consistent with the Court's previous case law. According to Olivia Tambou, with Opinion 1/15, the CJEU has acted for the fourth time as a "constitutional Court in order to defend the fundamental rights against states' surveillance measures."[21] Indeed, before delivering Opinion 1/15, the CJEU handed three landmark rulings which "left little doubt that the Agreement could not emerge unscathed."[22]

First, In *Digital Rights*[23] of 8 April 2014, the CJEU annulled the Data Retention Directive (the DRD) because it provided for the indiscriminate bulk collection and storage of data.

Second, In October 2015 the Court delivered its judgment in *Schrems*[24], invalidating the EU-US Safe Harbor scheme, the Agreement that had allowed for the transfer of personal data between the EU and certified US companies. The Court ruled that the Safe Harbor framework did not offer adequate protection for European citizens' personal data, mainly due to concerns about US surveillance practices. It is in this instance that the Court of Justice clarified what "an adequate level of protection" under Art. 25 of the Data Protection Directive means. The concept of "essential equivalence"

---

[20] EDPS. *Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data.* 30/09/2013, Brussels.
[21] Tambou, Olivia. "Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights." *European Foreign Affairs Review* 23, no. Issue 2. 2018: 187–202. p.190
[22] Mendez, Mario. "Opinion 1/15: The Court of Justice Meets PNR Data (Again!)". *European Papers*, *Vol. 2, No 3, 2017: 803-818*. p. 806.
[23] CJEU. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Karntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, 2014, ECR I-238
[24] CJEU. C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015.

refers to a level of data protection in a third country that may not be identical to EU legislation but must offer comparable safeguards. In other words, the EU's core data protection laws must be identified, and compliance with them should be a prerequisite for processing data outside EU jurisdiction.[25] For example, while the supervisory bodies in the EU and third countries may have differences in their structure, they must function independently as required by the Charter. Furthermore, the *Schrems* case emphasized that the Commission should not have excessive discretion when making adequacy decisions and outlined specific criteria to be considered. The General Data Protection Regulation (GDPR), which replaced the Data Protection Directive on May 25, 2018, also includes these criteria.

Third, another important ruling was delivered in December 2016 in *Tele2 Sverige*[26] where the principles established in *Digital Rights* and *Schrems* were strongly reaffirmed.

Opinion 1/15 represents the first time that the Court of Justice of the EU tackled the issue of PNR data transfer and processing.

The following paragraphs will examine the answers of the CJEU to the two main questions posed by the European Parliament, notably:

1) Is the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to the protection of personal data?

2) Do [point (d) of the second subparagraph of Article 82(1) and Article 87(2)(a)] TFEU constitute the appropriate legal basis for the act of the Council concluding the envisaged Agreement or must this act be based on Article 16 TFEU?'

3. The legal basis

Following the unfolding of the Court of Justice's reasoning, the question of the appropriate legal basis of the Agreement will be addressed first.

[25] Vedaschi, Arianna. "Privacy and Data Protection versus National Security in Transnational Flights: The EU–Canada PNR Agreement." *International Data Privacy Law* 8, no. 2, 2018: 124–139. p.130
[26] CJEU. Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Case C-203/15, 2016.

First of all, the Court explains how the choice of the substantive legal basis for an act holds constitutional significance, as it can be subject to judicial review and profoundly impacts the extent of EU powers concerning a particular matter.[27]

Article 5 of the Treaty on European Union (TEU) requires the Union to derive any action from the powers provided for in the Treaties. Thus, the European Union, having only conferred powers, "must link the acts which it adopts to provisions of the FEU Treaty which actually empower it to adopt such acts."[28]

Choosing an incorrect legal basis could render the agreement invalid, and so vitiate the European Union's consent to be bound by the agreement it has signed.[29]

Furthermore, it has to be underlined that the choice of a legal basis has also implications on the procedure required for adopting the act, for example concerning the involvement of the European Parliament and the required majority in the Council.

According to the well-established case law of the Court, when determining the legal basis for a European Union act, including one aimed at concluding an international agreement, as in this case, objective factors that are open to judicial scrutiny must be taken into account.[30] These factors include the purpose and substance of the act at issue.

In Opinion 1/15, there are essentially three legal bases under consideration: Articles 82(1)(d), 87(1)(a), and 16(2) of the Treaty on the Functioning of the European Union (TFEU).

First, point (d) of the second subparagraph of Article 82(1) TFEU, provides for the possibility for the Parliament and the Council to adopt measures to "facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions."[31]

Second, Article 87(2)(a) TFEU states that, for the purposes of prevention, detection and investigation of criminal offences, the Union shall "establish police cooperation involving all the Member States' competent authorities"[32], and the

[27] Nardone, Valentina. "The Passenger Name Record Case: Profiling Privacy and Data Protection Issues in Light of CJEU's Opinion 1/15." *Use and Misuse of New Technologies*, 2019, 135–50. p. 138
[28] CJEU. Opinion 1/15 delivered on 26 July 2017, ECLI:EU:C:2016:656. para 71
[29] Advocate General Paolo Mengozzi. Opinion 1/15 delivered on 8 September 2016, ECLI:EU:C:2016:656, para 40.
[30] CJEU. Opinion 1/15 delivered on 26 July 2017, ECLI:EU:C:2016:656. para 76
[31] European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01. Art.82(1)(d)
[32] Ivi. Art.87(2)(a)

Parliament and the Council may establish measures concerning "the collection, storage, processing, analysis and exchange of relevant information."[33]

Third, Article 16(2) TFEU provides that the European Parliament and the Council, "shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."[34]

The draft EU-Canada PNR Agreement was based on Articles 82(1)(d) and 87(2)(a) TFEU. As it was shown above, both these articles fall under the scope of the Area of Freedom, Security and Justice (AFSJ), since they pertain to measures aimed at facilitating judicial cooperation among Member States in relation to criminal matters (Article 82(1)(d) and the collection of information to foster police cooperation (Article 87(2)(a)).

However, the European Parliament argued that, although the envisaged agreement has the aim of ensuring the security and safety of the public and to prescribe the means by which PNR data will be protected, its principal aim is the protection of personal data.[35] Thus, according to the EP, the two legal bases chosen failed to properly take into account the data protection dimension and the Agreement should have been based on Art.16(2) TFEU.[36]

The Court, following its previous jurisprudence, conducted a thorough analysis of the Agreement's purpose to identify its legal basis, employing a teleological reasoning framework.[37] Accepting the positions of both Advocate General Mengozzi[38] and the EDPS[39], the CJEU found that the legal bases chosen were not correct, since the

---

[33] *Ibidem*
[34] European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01. Art.16(2)
[35] CJEU. Opinion 1/15 delivered on 26 July 2017, ECLI:EU:C:2016:656. para 31
[36] Ivi. para 32
[37] Graziani, Chiara. "PNR EU-Canada, La Corte Di Giustizia Blocca l'accordo: Tra Difesa Dei Diritti Umani e Implicazioni Istituzionali." *DPCE Online*. 2018: 959-966. p. 962
[38] The Court followed the analysis of Advocate General Paolo Mengozzi delivered on 8 September 2016. *Supra* note 29.
[39] EDPS. *Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data.* 30/09/2013, Brussels.

Agreement was serving two different objectives or components that are "inextricably linked"[40]:

1) the objective of protecting the security and safety of the public
2) the objective of prescribing how PNR data is to be protected.

The Court of Justice concluded that the Council's decision regarding the conclusion of the envisaged Agreement should rely on both Article 16(2) and Article 87(2)(a) of the TFEU in order to represent properly the two objectives.

Article 82(1)(d), instead, had to be excluded because, as the Court noted, there are no provisions of the Agreement envisaging a facilitation of judicial cooperation and the Canadian authority in charge of the use of PNR data is not a judicial authority, nor equivalent to it.

4. Compatibility with the Charter of Fundamental Rights and the TFEU

The European Parliament asked the Court of Justice of the EU to assess the compatibility of the EU-Canada PNR Agreement with:

1) Article 16 TFEU, which enshrines the right to the protection of personal data;
2) Article 7 CFR, which enshrines the right to respect for private and family life;
3)Article 8 CFR, which enshrines the right to the protection of personal data;
4) Article 52(1) CFR, which provides for the requirements to be respected in order to limit the rights and freedoms recognised by the Charter.

The first aspect that can be noted is that while the European Parliament mentioned both Article 16 TFEU and Article 8 CFR, given that they both provide for the right to the protection of personal data, the Court opted to assess the Agreement only under Article 8 CFR.

The reason for this decision was that Article 8 CFR is considered a *lex specialis*, as it provides more specific conditions, particularly in paragraph 2, regarding the processing of such data.[41] It must be underlined that this is an important step: by using the Charter as a separate standard, the Court of Justice enhanced its value and its

[40] CJEU. Opinion 1/15. *supra* note 30. para 94
[41] CJEU. *Ivi*. para 120

importance, not just in a formal sense – as granted by the Lisbon Treaty, which put it on equal legal footing with the Treaties – but also in a meaningful and practical way. [42]

Another aspect that can be noted is how, at the beginning of its reasoning the Court analysed Art. 7 and Art. 8 of the Charter separately but, as the analysis progressed, the distinction between the two articles became less and less pronounced, confirming the prevailing trend established by its previous case law concerning data protection.[43]

The approach followed by the Court of Justice is the classic one employed in cases involving limitations of fundamental rights: first, the existence of an interference by the measures under examination with the rights in question is determined; secondly, the appropriateness of the means to achieve the legitimate and general interest objective is scrutinized; finally, a decision is made on whether the adopted measures are limited to what is strictly necessary to achieve the declared purpose (so-called strict proportionality scrutiny).

The Grand Chamber acknowledged interferences with the rights enshrined in Art. 7 and Art. 8 of the Charter, as PNR data transferred may "reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers[44]." However, with a more pronounced emphasis than in *Digital Rights Ireland* and *Tele2 Sverige,* the Court emphasized the importance of considering that Articles 7 and 8 are not absolute rights and that "must be considered in relation to their function in the society."[45]

Thus, the Court focused on the justifiability of such interference, evaluating it based on the framework set forth in Articles 8(2), 8(3) and 52(1) of the Charter. In accordance with this latter provision, three aspects need to be considered, the interference must:

(1) be provided for by the law and respect the essence of the right;

(2) pursue an objective of general interest recognized by the EU or the need to protect the rights and freedom of others;

---

[42] Graziani, Chiara. "PNR EU-Canada, La Corte Di Giustizia Blocca l'accordo: Tra Difesa Dei Diritti Umani e Implicazioni Istituzionali." *DPCE Online*. 2018: 959-966. p. 962

[43] Fuster, Gloria González. *Emergence of personal data protection as a fundamental right of the EU*. Cham: Springer, 2014. p. 259

[44] CJEU. Opinion 1/15. *supra* note 30. para 128

[45] CJEU. *Ivi.* para 136

(3) be proportionate and strictly necessary in respect of their aim.

First of all, under Article 8(2) personal data should only be processed based on the consent of the individuals concerned or other legitimate bases established by law. The Court noted that the processing of PNR data under the proposed Agreement served a different purpose than the initial data collection by airlines, and therefore could not be considered as being based on passengers' consent. Thus, the CJEU had to determine whether the Agreement itself could be deemed as a legitimate legal basis within the context of Article 8(2) CFR.

The Court dismissed the European Parliament's argument that the Agreement is not a "law" and explained that when international agreements cover areas subject to the ordinary legislative processes (Article 294 TFEU), Parliament's approval (Article 218(6)(a)(v) TFEU) is required, making them equivalent to legislative acts: they are the external counterparts of internal legislative acts.[46] Thus, it concluded that the transfer of PNR data to Canada is based on "some other basis" laid down by law. [47]

In paragraph 149 of the Opinion, the Court clarified that the interferences with Art. 7 and Art. 8 of the Charter are justified by an objective legitimate interest of the European Union, notably that of ensuring public security through the transfer and processing of PNR data for combating terrorist offences and serious transnational crime, highlighting how "the protection of public security also contributes to the protection of the rights and freedoms of others."[48] Thus, while the core of the decision seems to favour fundamental rights, the underlying principles of the balancing act conducted by the CJEU reveal a strong sense of realism.

As far as the essence of the right to respect for private life is concerned the Court stated that while PNR data may reveal specific information about a person's private life "the nature of that information is limited to certain aspects of that private life"[49], in particular air travel between Canada and the European Union. Similarly, the essence of the right to the protection of personal data, enshrined in Article 8 of the Charter, is respected in the envisaged Agreement because of the limitations on the purposes for processing PNR data by Canada (stated in Article 3) and the establishment of rules to

[46] *Ivi*. para 146
[47] *Ivi*. para 147
[48] *Ivi*. para 149
[49] *Ivi.* para 150

ensure data security, confidentiality, integrity, and protection against unlawful access and processing (mentioned in Article 9). It can be noted that the inclusion of security obligations as a crucial aspect of the right to personal data protection was influenced by the reinforced security responsibilities imposed on data controllers and processors with the General Data Protection Regulation (GDPR) and the LED Directive, set to be implemented from May 2018 onwards.[50]

Given these measures, the Court concluded that the interferences that the envisaged Agreement introduced are justifiable in pursuit of a general interest objective of the European Union and do not adversely affect the essence of the fundamental rights protected by Articles 7 and 8 of the Charter. However, other scholars are hesitant on this matter. Maria Tzanou, for example, states that:

> The blanket collection of the PNR data of every passenger, irrespective of whether he is considered to be under suspicion, its retention for long periods and its processing in order to develop terrorist profiles, without granting adequate procedural rights to the individuals concerned to challenge it, affects cumulatively the essence of several different fair information principles and, might, therefore, be considered to touch upon the essence of the fundamental right to data protection.[51]

Another aspect that has been criticised by some authors is the evaluation of the Court on the appropriateness of the data processing in relation to the objective of ensuring public security.

The Grand Chamber highlighted how the use of PNR data has proven effective in facilitating security and border control checks. It has also led to successful outcomes in terms of arrests related to security threats, enabling "the arrest of 178 persons from among the 28 million travellers who flew between the European Union and Canada in the period from April 2014 to March 2015."[52] Therefore, the transfer and processing of PNR data to Canada were deemed appropriate for achieving the objective of enhancing public security and safety, as sought by the envisaged Agreement.

---

[50] Tambou, Olivia. "Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights." *European Foreign Affairs Review* 23, no. Issue 2. 2018: 187–202. p. 195

[51] Tzanou, Maria. *The fundamental right to data protection: Normative Value in the context of counter-terrorism surveillance*. Oxford: Hart, 2019. p. 173

[52] CJEU. Opinion 1/15. *Supra* note 30. Para 152

However, the Luxemburg Court solely relied on statistical analysis provided by the Commission. It could be contended that these elements are not persuasive enough regarding the effectiveness of the large-scale transfers of PNR data. As some scholars have observed, it would have been preferable to have increased transparency and conducted a comprehensive impact assessment on this issue.[53]

5. Proportionality of the EU-Canada PNR Agreement

The Grand Chamber faced a particularly challenging task in evaluating compliance with the principle of proportionality, which involves assessing the necessity of interferences resulting from the Agreement. Indeed, as Advocate General Mengozzi clarified, the principle of proportionality "requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives." [54]

This complexity arose due to the multitude of factors that needed consideration. Throughout a detailed evaluation of the Agreement, the Court applied the test of strict necessity (test of proportionality *stricto sensu*) at length. While certain provisions of the Agreement were deemed to meet this stringent test, being considered "clear and precise"[55] and falling within the limits of strict necessity, there were notable exceptions.

For the purposes of this analysis, the most criticized provisions of the Agreement analyzed by the CJEU will be discussed in the following order:

1) the PNR data to be transferred;

2) the automated processing of personal data and the purposes for which PNR data may be processed;

3) the competent authority responsible for processing the data and the air passenger concerned;

4) the retention and use of PNR data;

5) the disclosure of PNR data;

6) the rights of and the guarantees for data subjects.

[53] Tambou, Olivia. *Supra* note 50. p.196
[54] Advocate General Paolo Mengozzi. *Supra* note 29. para 196
[55] CJEU. Opinion 1/15. *Supra* note 30. paragraphs 154, 158, 178 and 190

5.1. The PNR data to be transferred

One primary concern was the lack of precision and clarity in defining the categories of transferable data, which encompassed a wide range of personal information, often described in vague terms. The Court found imprecise three of the nineteen data headings outlined in the Annex of the proposed Agreement. These imprecisions arise from vague phrasing, such as "all available contact information," in heading 7 that "does not specify sufficiently the scope of the data to be transferred"[56], or the use of the word "etc" in heading 5. More generally, the concerns revolved around the unclear nature and extent of the information being sent to the competent Canadian authority.

The lack of clarity in the Annex to the Agreement, as observed by the Advocate General, is a serious concern that makes it difficult for airlines and Canada to comply with the Agreement and may potentially lead to the exploitation of personal data.[57] Indeed, even if Article 4(3) of the Agreement[58] clearly states that Canada is required to delete any data transferred to it, if it is not listed in the Annex to the Agreement, the lack of clarity of the headings in the Annex makes it difficult for airlines and Canada to know which data can be transferred to Canada and which data must be deleted.

Secondly, the CJEU emphasized that the proposed Agreement might involve the transfer and processing of sensitive data, which have been defined by Article 2(e) of the draft Agreement as any information that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership", or concerning "a person's health or sex life." [59]

Differently from the 2006 EU-Canada PNR Agreement which excluded sensitive data, the 2014 Agreement does not. Under the draft Agreement, the Canadian Competent Authority is required to mask sensitive data using automated systems. However, the Agreement also allows for sensitive data to be processed on a case-by-case basis in exceptional circumstances, such as when an individual's life is in peril or there is a risk of serious injury."[60] In its opinion, Advocate General Mengozzi highlighted how under

[56] *Ivi*. Para 158
[57] Advocate General Paolo Mengozzi. *Supra* note 29. para 219
[58] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).* Art. 4(3)
[59] *Ivi.* Art 2(e)
[60] *Ivi.* Art 8(3)

the EU-Canada PNR Agreement, sensitive data of a Union citizen who has taken a flight to Canada can be retained for up to five years by any Canadian public authority in accordance with Article 16(5) of the Agreement envisaged. During that period, this data can be unmasked and examined for any purpose, even if it is unrelated to the Agreement's goal, such as processes involving contract law or family law.[61] As a result, the aforementioned provision fails to strike a fair balance between the Agreement's purposes and the protection of individual privacy. Indeed, the Parliament argued that the data retention term was excessive, and that the data could potentially be used for purposes other than public security. Furthermore, the risk of sensitive data being held for five years and subsequently exploited for unrelated reasons, according to Advocate General Mengozzi, is an important problem, which could lead to the misuse of personal data and the loss of privacy rights.

In the Court's view transferring sensitive data to Canada would necessitate a precise and robust justification, one that goes beyond the mere protection of public security against terrorism and serious transnational crime. However, in this particular instance, such a justification is deemed to be lacking.

It is interesting to note how the Court's stance on the transfer of sensitive data to Canada presents an intriguing ambiguity. While it may seem that the Court has absolutely prohibited the transfer of sensitive data, this is actually not the case. These can be transferred if there is a solid justification.

Indeed, on the one hand, the Court criticized the transfer of such data when the purpose is to combat terrorism and serious transnational crime, as it could infringe upon the rights guaranteed in Articles 7 and 8 of the Charter, read in conjunction with Article 21[62]. This indicates the Court's vigilance in safeguarding individual privacy and fundamental rights.

On the other hand, the Court also recognized that under certain circumstances and with precise and solid justifications, such transfers may be permissible. Thus, arguing that the prohibition of transferring sensitive data is not an absolute and rigid one. This nuance leaves room for considering exceptional cases where sensitive data could be transferred,

[61] Advocate General Paolo Mengozzi. *Supra* note 29. para 224

[62] European Union. *Charter of Fundamental Rights*. Art. 21 states that: "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

if there are strong and legitimate reasons beyond the scope of public security against terrorism and transnational crime.

Furthermore, another aspect has to be underlined: the Court implicitly recognized that relying on individuals' sensitive data, such as religion or race, could lead public authorities to unfairly target specific groups (e.g., Muslims) with harsher counter-terrorism measures, resulting in discrimination and violation of Article 21 of the Charter of Fundamental Rights of the EU[63]. While the Court's stance might seem to impose an absolute ban on profiling, there are other non-sensitive data, like travel destinations or food preferences, that could still lead to discriminatory profiling.[64] These points were not thoroughly addressed by the Court, and more clarity on them would have been beneficial.

5.2. The automated processing of personal data and the purposes for which PNR data may be processed

For what concerns the automated data analysis procedures, where pre-established models and criteria seem to exhibit a notable margin of error, the Court, agreeing with the Advocate General's observations, stressed that "databases with which data is cross-checked must be reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime."[65] Moreover, in situations where a suspicious individual is flagged during the analysis, it is essential that before implementing any security measure, a further individual evaluation by non-automated tools takes place.[66] In this passage, the Court entered rather technical considerations, demonstrating the meticulous nature and depth of the analysis.

Then, the Court thoroughly evaluated the clarity and precision of the purposes for which PNR data may be processed by the Canadian Competent Authority.

Article 3(1) of the Agreement explicitly allows for processing PNR data exclusively to prevent, detect, investigate, or prosecute terrorist offences or serious transnational crimes.[67] In Article 3(2), the expression "terrorist offences" is clearly

---

[63] European Union. *Charter of Fundamental Rights*. Art. 21 "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

[64] Vedaschi, Arianna. "The European Court of Justice on the EU-Canada Passenger Name Record Agreement." *European Constitutional Law Review* 14, no. 2, 2018: 410–29. p.422

[65] CJEU. Opinion 1/15. *Supra* note 30. Para 172

[66] *Ivi.* Para 173

[67] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).* Art 3(1)

defined, encompassing specific activities and identifying individuals, groups, and organizations that could be considered as "terrorist entities."[68] Similarly, "serious transnational crime" is distinctly outlined in the first subparagraph of Article 3(3), specifying the severity of the offences as punishable under Canadian law by at least four years of prison or a more severe penalty. Additionally, the nature of these offences is deemed sufficiently precise, as they are based on definitions established by Canadian law.[69] The second subparagraph of Article 3(3) further clarifies the various situations in which a crime is deemed to be of a transnational nature. Consequently, the Court acknowledged that provisions in Article 3(1) to (3) of the envisaged Agreement are found to contain explicit and well-defined regulations limited to what is strictly necessary, ensuring clarity and adherence to the required criteria for processing PNR data.[70]

However, the Grand Chamber criticized the lack of clarity in the provisions of Article 3(5) allowing PNR data processing by Canada on a case-by-case basis for purposes like overseeing or holding the public administration accountable and complying with subpoenas, warrants, or court orders.[71] From the Court's perspective, such vague wordings allow for the processing of data for purposes that are not strictly necessary to achieve the objectives of the Agreement. Indeed, this provision was declared incompatible with Articles 7 and 8 and Article 52(1) of the Charter, because it allowed the processing of PNR data to be extended beyond what is strictly necessary, independently of the stated purposes of the Agreement.[72]

5.3. The competent authority responsible for processing the data and the air passenger concerned

According to the CJEU, the proposed Agreement adequately and unambiguously defined the relevant Canadian authorities and the air passengers to whom it applies.

The Canadian competent authority is responsible for receiving and processing passenger name record data and it is deemed to guarantee an adequate level of protection for PNR data under EU law. Even if the identity of the Canadian competent authority is not indicated in the Agreement, Canada is required to notify the EU of its identity before

[68] *Ivi*. Art.3(2)
[69] *Ivi*. Art. 3(3)
[70] Ivi. Para 178
[71] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE)*. Art 3(5)
[72] Advocate General Paolo Mengozzi. *Supra* note 29. Para 237

the Agreement enters into force. This, according to the Court of Justice of the EU, ensures that the EU is aware of the authority that will be responsible for processing PNR data.

The Agreement also does not specify the identities of the other government authorities in Canada to whom PNR data may be disclosed. However, it does specify that these authorities must have functions directly related to the scope of Article 3 of the Agreement, such as border control and law enforcement. Additionally, the disclosure of PNR data to these authorities must be necessary for the purposes stated in Article 3, and the authorities must afford protection equivalent to the safeguards described in the Agreement. In the Court's view, this ensures that PNR data will only be disclosed to authorities that have a legitimate need for it, and that the data will be protected in accordance with EU law.[73]

For what concerns the air passengers, the Court acknowledged that Article 13 of the Chicago Convention, which is applicable to both the EU and Canada, mandates the verification of PNR data for all air passengers travelling between the two regions. The envisaged Agreement thus aligns with this requirement, ensuring that the verification process encompasses all applicable air travellers and is clearly delineated in the Agreement.

5.4. The retention and use of PNR data

The provisions of the Agreement regarding data retention stipulate that the retention period cannot exceed five years, and a portion of the data must be masked after a short period of 30 days, without any distinction among the affected passengers. [74] Furthermore, two years after Canada receives the PNR data, it must be further depersonalized.[75]

The Court distinguished between three different situations: (1) the transfer and storage of PNR data for the purpose of entering Canada; (2) the further use and storage of that data during the stay of the passengers concerned in Canada, (3) and after their departure.

While the transfer and storage of PNR data of passengers for entering Canada may be deemed appropriate for the legitimate purposes of the Agreement and does not exceed

[73] CJEU. Opinion 1/15. *Supra* note 30. Para 184
[74] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE)*. Art 16(1)(2)
[75] *Ivi*. Art 16(3)

the limits of necessity, the same cannot be said for the use of such data during their stay in Canada and after their departure. Indeed, after air passengers have been allowed to enter Canada, following verification of their PNR data, "the use of that data during their stay in Canada must be based on new circumstances justifying that use"[76] and must be "subject to a prior review carried out either by a court or by an independent administrative body.[77]"

More serious issues, on the other hand, are associated with the use of data after the passengers' departure from Canada. Only passengers considered to be a potential threat in terms of terrorism and serious transnational crimes may have their PNR data retained after their stay in Canada. In such cases, the five-year retention period outlined in the proposed Agreement does not go beyond the limits of what is deemed strictly necessary. Nonetheless, the utilization of this PNR data must be justified and subjected to a prior assessment by either a court or an administrative body. In other words, the CJEU has ruled that the Canadian government cannot use PNR data for general surveillance or law enforcement purposes. It can only use the data if it has grounds to believe that a passenger poses a threat to public safety and even then, the use of the data must be subject to independent oversight.

For what concerns the retention of data, the Court and the Advocate General held different views. The latter took the position that a five-year retention period was excessive but could be mitigated through data masking. In contrast, the Court deemed such a period to be justified without specific elaboration. The Advocate General's stance is commendable for its explicit and clear expression, unlike the Court's approach, which lacked detailed consideration of the retention duration, potentially causing uncertainty about the criteria used to decide on the retention period.[78]

5.5. The disclosure of PNR data

The Canadian authority responsible for processing PNR data can communicate it to other Canadian authorities, authorities of third countries, or, in specific circumstances, to individuals. In none of these cases has this been deemed limited to what is strictly necessary.

---

[76] CJEU. Opinion 1/15. *Supra* note 30. Para 200
[77] *Ivi*. Para 202
[78] Vedaschi, Arianna. "The European Court of Justice on the EU-Canada Passenger Name Record Agreement." *European Constitutional Law Review* 14, no. 2, 2018: 410–29. p. 425

First of all, Articles 18 and 19 of the 2014 EU-Canada PNR Agreement regulate two types of data disclosure: internal disclosure to other government authorities and external disclosure to third countries.[79] These two types of data disclosure are possible only if certain conditions are met and four of them are identical for both types of disclosure:

1) if the government authorities have functions that are directly related to the scope of the purpose limitation of the Agreement;
2) on a case-by-case basis;
3) under the particular circumstances the disclosure is necessary for the purposes stated in the purpose limitation;
4) only the minimum amount of PNR data necessary is disclosed;

For internal disclosure, there are two additional guarantees since government authorities to whom the PNR data is disclosed must offer "protection equivalent to the safeguards described in the Agreement"[80] and cannot "disclose the PNR data to another entity unless the disclosure is authorized by the Canadian Competent Authority respecting the conditions laid down in this paragraph."[81] These safeguards are missing for external disclosure. Indeed, the Grand Chamber raised concerns about the discretionary power granted to the Canadian authorities regarding the disclosure of PNR data to governments of third countries. Specifically, Article 19 of the Agreement gave Canadian authorities the discretionary power to evaluate the level of protection provided by third countries, ensuring that they offered the same level of protection as the Union.

In Opinion 1/15, the Court has taken a significant step in regulating data transfers from Canada to third countries, aligning its decision with the standards established in the *Schrems* case. Indeed, the Grand Chamber emphasized that such data transfers should only be permissible if the third countries offer a level of protection for fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.

To meet this crucial requirement, data transfers to third countries are allowed only under 2 circumstances:

[79] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).* Artt. 18-19
[80] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).* Art 18(e)
[81] *Ibidem*

1) if there exists an Agreement between the European Union and those countries, which must be equivalent to the one in place with Canada
2) if the European Commission has issued a specific decision approving the level of protection offered by the third country.

If these two circumstances are not met, disclosure to authorities in third countries would constitute an outright circumvention of the guarantees laid down in EU law, in clear breach of Article 25 of Directive 95/46/EC.[82]

Secondly, the CJEU criticized the disclosure of PNR data to individuals – which could be considered the most problematic issue – in terms of precision and clarity, because the proposed Agreement lacked explicit limitations on the type of information that could be shared, the recipients of such information, and the specific purposes for which it could be used. Furthermore, the Court noted that there was no requirement that the disclosure "be linked to combating terrorism and serious transnational crime or that the disclosure be conditional on the authorisation of a judicial authority or an independent administrative body".[83]

5.6. The rights of and the guarantees for data subjects

Finally, the Court identified additional deficiencies in the Agreement's ability to uphold the guarantees for data subjects outlined in Articles 7 and 8 of the Charter. To ensure compliance with these provisions, it was deemed necessary to individually notify passengers about the transfer of their personal data to Canada and its use as soon as the information was "no longer liable of jeopardizing the investigations being carried out by the government authorities." [84]Although the envisaged Agreement between the EU and Canada gave air passengers the right to access and correct their PNR data[85], it did not require that they be notified of the transfer of their data to Canada or how it will be used.

It is important that air passengers have the right to know how their data is being used, and to have the opportunity to challenge the use of their data if they believe it is being used in a way that is harmful to them.

[82] CJEU. Opinion 1/15. *Supra* note 30. Para 214
[83] CJEU. *Ivi*. Para 217
[84] *Ibidem*. Para 220
[85] Council of the European Union. *Agreement between Canada and the European Union on the transfer and processing of PNR, 2013/ 0250(NLE).* Artt. 12-13

The Court of Justice has set a high standard, stressing that data retention systems must include an individual notification system. The CJEU also ruled that access to data should generally depend on prior review by a judicial or independent administrative authority.[86] This means that law enforcement agencies cannot simply access data without first getting approval from a judge or other independent body.

This issue of individual notification, which is a strong *ex-post* guarantee, represents a novelty, since it had not been extensively addressed in previous cases like *Digital Rights*, nor is it governed by the EU PNR Directive.

Furthermore, with regard to the supervisory activities of an independent authority, the Court found elements of incompatibility with the rights protected by the Charter of Nice. As clarified by the Advocate General, Article 10 of the Agreement seems to allow for data protection oversight to be carried out by authorities that are not entirely independent but are subject to external influences and directions. This circumstance, according to the CJEU, is in conflict with Article 8 paragraph 3 of the Charter of Fundamental Rights[87], as the competent Canadian authority must perform its functions with complete independence, without its decisions being in any way influenced by external powers. This concern was also raised by the EDPS, which in its opinion noted how "the limitations of judicial review and the fact that administrative redress can be provided in some cases by an internal authority which is not independent."[88]

6. Implications

Opinion 1/15 is important not only because it supplements previous CJEU case law on EU data protection (such as the rulings in *Schrems, Digital Rights Ireland, Tele 2 Sverige/Watson*) but also – for the first time – the Court of Justice of the EU sets out the conditions under which international agreements may be used to legalise cross-border data transfers.[89] Therefore, it can be considered as a "crucial standard-setter" in the field of transnational data exchange for law enforcement purposes. [90]

[86] CJEU. Opinion 1/15. *Supra* note 30. Para 202
[87] *Ivi*. Para 231
[88] EDPS. *Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data.* 30/09/2013, Brussels. p.2
[89] Csonka, Peter, Adam Juszczak, and Elisa Sason. "The Establishment of the European Public Prosecutor's Office : The Road from Vision to Reality." *eucrim - The European Criminal Law Associations' Forum*, 2017. p.115
[90] *Ibidem*

The first evident implication of this decision of the Luxemburg Court is that the Agreement in its existing form could not be ratified by the EU, thus preventing its enactment. The Court made it clear that it is imperative for the Commission and Council to make substantial revisions in order to align with the criteria outlined in the CJEU's viewpoint. Consequently, in June 2018 the EU initiated negotiations[91] with Canada to modify the Agreement. However, five years later, these discussions are still in progress. Indeed, Opinion 1/15 provided the European Commission with an extraordinarily prescriptive and complex roadmap for renegotiating its draft PNR agreement with Canada. Furthermore, unlike the US Supreme Court, the Court of Justice of the EU "does not defer to its executive branch negotiators to broadly define the content of international agreements"[92]. Thus, the EU Commission lacks negotiation discretion.

Secondly, the Court established that any EU instrument which governs how personal data collected by private operators for commercial purposes may be further used for security and law enforcement purposes must be adopted on Article 16(2) TFEU (on data protection) in conjunction with Article 87(2) TFEU (on police cooperation among the Member States in criminal matters).[93] Thus, any Council resolutions regarding the revised Agreement must be adopted on the dual legal bases highlighted by the Grand Chamber, because security and data protection are two equal components of the Agreement and each requires its own legal basis.

Indeed, Opinion 1/15 has departed from the CJEU's earlier 2006 PNR ruling[94], which occurred before the adoption of the Lisbon Treaty and considered the relevant EU-US PNR Agreement to be related to public security rather than a data protection instrument.[95] In that occasion, the Court had clearly stated that "the transfer of PNR data […] constitutes processing operations concerning public security and the activities of the

[91] European Commission. *Commission recommendation for a Council decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime*. COM(2017) 605 final, 18 October 2017

[92] Propp, Kenneth. "Avoiding the next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data." *Atlantic Council.* July 1, 2021. p. 10

[93] Docksey, Christopher. "Opinion 1/15: Privacy and security, finding the balance". *Maastricht Journal of European and Comparative Law* 24, no. 6 2017: 768–73. p.770

[94] CJEU, Joined Cases C-317/04 and C-318/04, 2006

[95] Zalnieriute, Monika. "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement." *The Modern Law Review* 81, no. 6. 2018: 1046–63. p.1059

State in areas of criminal law"[96], without even mentioning the data protection dimension of this process.

Now, alongside Article 87(2) of the Treaty on the Functioning of the European Union (TFEU), the Court stressed the importance of data protection as a joint legal basis for PNR Agreements. This shift is significant as it illustrates the influence of the Lisbon Treaty, which consolidated the former First and Third Pillars of the Maastricht Treaty.[97] It also means that negotiations and adoption of such dual-goal data-sharing instruments will now involve both DG Home and DG Justice of the European Commission.[98] This reflects the greater importance given to data protection in the negotiation, adoption, and supervision of such Agreements, with an independent data privacy commissioner overseeing them after adoption, as provided for by both Article 16(2) TFEU and Article 8(3) of the Charter.[99] However, it must also be clear that theoretically, this applies not only to international PNR agreements but also to EU legal instruments that establish data protection regimes, such as the Europol Regulation and the EU PNR Directive, neither of which has currently Article 16(2) TFEU as one of the legal bases.[100]

Thirdly, another important implication of the findings of the Court in Opinion 1/15, is that it cast doubt on the compatibility of the existing EU PNR Agreements with the US and Australia. These Agreements are similar to the EU-Canada Agreement, in that they allow for the transfer of PNR data to these countries for the purposes of preventing and combating terrorism and serious crime. Thus, the Court's findings suggested that these Agreements might also be incompatible with the Charter of Fundamental Rights and thus in need of renegotiation. This was also confirmed by the European Commission, which in its latest report declared that the 2012 EU-US PNR Agreement is "not fully in line" with Opinion 1/15 of the CJEU.[101] Nonetheless, the US government has shown reluctance to engage in discussions about revisiting the 2012 Agreement, and up until

[96] CJEU, Joined Cases C-317/04 and C-318/04, 2006, para 56
[97] Docksey, Christopher. *Supra* note 93. p.770
[98] Zalnieriute, Monika. "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement." *The Modern Law Review* 81, no. 6. 2018: 1046–63. p.1059
[99] *Ibidem.*
[100] The EU PNR Directive is based on Article 82(1) and Article 87(2)(a) TFEU and the Europol Regulation on Article 88 TFEU.
[101] European Commission. *Report from the Commission to the European Parliament and the Council on the Joint Evaluation of the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security,* January 12, 2021, COM (2021) 18.

now, the European Commission has not emphasized this issue. Instead, the Commission has directed its efforts towards the ongoing re-evaluation of a PNR Agreement with Canada and an internal reconsideration of its overall strategy regarding the global sharing of PNR data.[102]

This unwillingness to focus on the renegotiation of the EU-US PNR Agreement - which has never stopped being in force - may be due to the fact that the EU is too economically interdependent with the US to seriously consider the suspension of data transfer, as this would lead to political consequences.[103] As some scholars have observed, the "CJEU may now have accepted that threats to suspend data transfers to the US as leverage to renegotiate for increasing data protection standards have not so far been politically effective."[104]

Fourthly, the impact of Opinion 1/15 on future negotiations has to be considered. On the one hand, the ruling has restricted the EU's flexibility in conducting international negotiations across significant domains concerning the movement of personal data.[105] These areas encompass international trade, data exchange with third nations, and post-Brexit arrangements. On the other hand, the Court's definitive stance on certain matters can undoubtedly be advantageous in future negotiations.[106] For example, third states will have to legislate to fill gaps under national law to ensure an adequate level of protection, which has to be "essentially equivalent" to that of the EU. For instance, in the present case, Article 10(1) of the draft Agreement outlines that the safeguards for data protection in processing PNR data will be subject to supervision by an "independent public authority" or by an "authority established through administrative means, demonstrating impartial functioning and a proven history of autonomy." The Court did not accept this latter alternative form of supervision, stating that it was not adequate to ensure the strict

[102] Propp, Kenneth. "Why Sharing Passenger Data Doesn't Fly for the EU's Top Court." *Atlantic Council,* July 7, 2022. Last accessed 05/08/2023 at https://www.atlanticcouncil.org/blogs/new-atlanticist/why-sharing-passenger-data-doesnt-fly-for-the-eus-top-court/.
[103] Weiss, Martin, and Kristin Archick. "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*. 2016. p.8
[104] Zalnieriute, Monika. "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement." *The Modern Law Review* 81, no. 6. 2018: 1046–63. p.1061
[105] Kuner, Christopher. *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15, VerfBlog*. 2017
[106] Docksey, Christopher. "Opinion 1/15: Privacy and security, finding the balance". *Maastricht Journal of European and Comparative Law* 24, no. 6 2017: 768–73. p.771

standard of independent supervision required under Article 8(3) of the Charter.[107] Thus, Opinion 1/15 provides valuable support for European negotiators in future agreements. The EU is founded on the values of democracy and the rule of law, and EU negotiators have the opportunity to insist that specific concessions demanded by third countries might not align with the Court's or Parliament's standards.

Furthermore, while carefully examining the EU-Canada Passenger Name Record Agreement, Opinion 1/15 has affirmed, strengthened, enhanced, and provided greater clarity to the principles previously articulated by the Court regarding the collection, retention, and use of personal information. These principles were elucidated in at least three prior rulings: *Digital Rights, Schrems, and Tele2,* and the CJEU clarified that they extend to Passenger Name Record data as well, thus "building a comprehensive framework for EU data protection, which will be highly beneficial to the perception of the EU as a rule of law-based institution".[108]

[107] CJEU. Opinion 1/15, para. 228-231.
[108] Vedaschi, Arianna. "The European Court of Justice on the EU-Canada Passenger Name Record Agreement." *European Constitutional Law Review* 14, no. 2, 2018: 410–29. p. 428

Conclusion

For the first time, the Court of Justice of the EU has ruled on the compatibility of an international agreement with the rights enshrined in the Charter of Fundamental Rights. This is an important step, as it reinforces the constitutional[109] value of the Charter and establishes that it is the only parameter for deciding whether challenged acts (including international Agreements) violate EU law.[110] For example, when the Court had to assess the compatibility of the Agreement with the right to the protection of personal data, it chose to evaluate the Agreement under Article 8 of the Charter instead of Article 16 TFEU, thus using the Charter as a distinct criterion and enhancing its value. Indeed, for some scholars, Opinion 1/15 is "an example of the growing influence of the Charter on the external policy of the EU."[111]

The Court has also found that international agreements are substantively equivalent to EU legislation, meaning that they must meet the same high standards of protection for fundamental rights.[112] The issue of whether international agreements may be used to determine adequacy, has been finally resolved by the CJEU.[113] Indeed, the European Parliament had claimed that the proposed Agreement could not be justified by reference to it as "law," which is the essential precondition for interfering with a fundamental right. However, the Court determined, in accordance with the Advocate General, that such an agreement may be seen as being the equal, externally, of what a legislative act is internally.

Furthermore, the Grand Chamber carefully examined the wording of the Agreement and made some critical observations. It went beyond making general statements and provided specific examples of words and phrases that should be replaced in the redrafted Agreement. This level of involvement is significant because it reflects the Court's view that mass surveillance must be subject to strict regulations, even in the face of the terrorist threat. The Court is willing to take on a more active role in protecting

[109] Vedaschi, Arianna, and Lubello, Valerio. "Data Retention and Its Implications for the Fundamental Right to Privacy." *Tilburg Law Review* 20, no. 1 2015: 14–34. p.17
[110] Vedaschi, Arianna. "The European Court of Justice on the EU-Canada Passenger Name Record Agreement." *European Constitutional Law Review* 14, no. 2, 2018: 410–29. p. 426
[111] Tambou, Olivia. "Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights." *European Foreign Affairs Review* 23, no. Issue 2. 2018: 187–202. p. 189
[112] CJEU. Opinion 1/15. Para 67
[113] Docksey, Christopher. "Opinion 1/15: Privacy and security, finding the balance". *Maastricht Journal of European and Comparative Law* 24, no. 6 2017: 768–73. p.771

individual rights, even if it means exceeding its traditional duties, assuming a "quasi-legislative and political responsibility."[114]

As Arianna Vedaschi has observed in the balance between privacy and security "the Court took a firm stance towards the protection of fundamental rights, avoiding, at the same time, the pitfall of a utopian approach".[115] Indeed, while the Court of Justice has acknowledged the utility of widespread and indiscriminate surveillance of travellers as a valuable counterterrorism measure, it has also tempered this security-focused approach with caution. By departing from the Advocate General's position, the Court "has pulled back a bit from the prohibition against general and indiscriminate retention of data and has found that interference with the fundamental rights to privacy and data protection may be justified."[116] Nonetheless, the Court demonstrated an understanding of the significant threats that mass surveillance poses to fundamental rights, especially when there is a lack of well-defined and specific guidelines for how such actions are carried out.[117] The CJEU indeed clarified that to avoid abuses, the legislation should set down "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards."[118]

While this decision of the Luxemburg Court is seen as a victory for privacy-advocates, some scholars contend that the CJEU could have gone further in challenging the very rationale of PNR schemes in their entirety.

However, the next chapter of this dissertation will focus on another important implication that has not been discussed yet: the implication for the EU PNR Directive. Through the analysis of a recent case brought before the Court of Justice of the EU in 2022 (case C-817/19), which assesses the EU PNR Directive's validity, it will be possible to see the impact of Opinion 1/15 on the Court's evaluation of the Directive and it will be also possible to explore how the Luxemburg Court's perspectives have evolved since the its pivotal decision on the EU-Canada PNR Agreement.

How will the balance between privacy and security be influenced by this new recent ruling of the CJEU?

---

[114] Vedaschi, Arianna. "The European Court of Justice on the EU-Canada Passenger Name Record Agreement." *European Constitutional Law Review* 14, no. 2, 2018: 410–29. p. 428
[115] Vedaschi, Arianna. *Ivi*. p.429
[116] Villani, Susanna. "Some further reflections on the Directive (EU) 2016/681 on PNR data in the light of the CJEU Opinion 1/15 of 26 July 2017". *Revista de Derecho Político*, 1(101), 2018: 899- 928, p. 922
[117] *Ibidem*
[118] CJEU. Opinion 1/15. para. 141

CHAPTER III
Implications for the PNR Directive: *Case C-817/19*

Introduction

Among the profound, far-reaching implications of the judgment delivered by the Court of Justice of the European Union in Opinion 1/15, it is impossible not to mention case C-817/19 (also known as *Ligue des droits humains*).

The conclusion reached by the CJEU in Opinion 1/15 for many served as a resounding alarm bell for the validity of the PNR Directive. Indeed, the Court's decision that the Agreement could not be concluded in its current form, because of its incompatibility with the fundamental rights enshrined in the Charter, raised questions about the validity of the PNR Directive, which shares several provisions with the agreement.

Furthermore, as some scholars have observed, *Ligue des droits humains* can be considered "the direct successor case to the 2017 Opinion 1/15."[1] As a matter of fact, this judgment represents the second time that the CJEU has appraised the conformity of a PNR system with the EU Charter of Fundamental Rights.

This case, which is considered "one of the principal dilemmas of contemporary liberal democratic consolidation"[2] is particularly useful for this dissertation also because it offers a lens through which it is possible to comprehend how the Court of Justice answers a rather complex question:

> "what balance should be struck between the individual and society in this data age in which digital technologies enabled huge amounts of personal data to be collected, retained, processed and analysed for predictive purposes?"[3]

The Court of Justice of the European Union, through its case law, has taken a firm stance in favour of the fundamental rights to privacy and the protection of personal data, which are guaranteed by Articles 7 and 8 of the Charter and has

[11] Beauregard-Lacroix, Raphaël. "Ligue Des Droits Humains (C-817/19): A Display of Consistency by a Steadfast and Pragmatic Court." *European Law Review* 48, no. 2. 2023: 220–31. p.220
[2] Opinion of Advocate General Pitruzzella delivered on 27 January 2022, Ligue des droits humains, C-817/19. Para 2
[3] *Ibidem*

invalidated various legislation for infringing on those rights. The judgment of the Court in Opinion 1/15 confirmed this direction.

However, with its ruling in *Ligue des droits humains* on 21 June 2022, the CJEU broke from this pattern. Despite acknowledging the undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter posed by the PNR Directive, the CJEU declared it valid.

This chapter will delve into the rationale behind this unexpected departure, shedding light on the reasoning that underpinned this significant decision.

1. Background of the case

On 21 June 2022, the Court of Justice of the European Union, sitting as Grand Chamber, handed down its judgment in the preliminary ruling procedure C-817/19, *Ligue des Droits Humains v. Council of Ministers*[4], assessing the validity of the PNR Directive.

Adopted in 2016, the PNR Directive mandates air carriers to transfer the PNR data of all passengers of extra-EU flights to a designated national authority that each Member State is required to establish (the Passenger Information Unit) to prevent, detect, investigate and prosecute terrorist offences and serious crime.

Although the obligation to transfer PNR data to the designated national authorities only applies to flights outside the EU, the PNR Directive gives Member States the possibility of extending this requirement to flights within the EU. Almost all Member States availed of this option, except for Ireland and Slovenia.

Furthermore, the PNR Directive governs how PNR data is processed and how Member States can exchange it.

Under this regulatory framework, as part of the pre-screening of passengers, PNR data transferred to the Passenger Information Units are subject to automated processing against pre-existing databases and pre-determined criteria in order to identify those who might need further examination. The Directive also includes a list of the PNR data to be transferred to the Passenger Information Units in Annex I and a list of serious crimes offences in Annex II. Data are stored for five years with a stricter access regime for the first six months after the receipt of the data and they can be shared with competent authorities on a case-by-case basis under specific circumstances.

On 24 July 2017, the *Ligue des droits humains* (LDH), a non-profit human rights organization, filed an action with the Belgian Constitutional Court (*Cour constitutionnelle*), seeking the total or partial annulment of Law of 25 December 2016, which transposed the PNR Directive and the API Directive into Belgian law.[5]

The law required international passenger transport carriers in various sectors (air, rail, international road and sea), as well as tour operators, to transfer data of their

[4] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. 2022
[5] CJEU. *Ivi*. Para 51

passengers to a database managed by the Belgian Home Affairs Federal Public Service *(Service public Federal intérieur)*.[6]

The LDH raised two pleas, the first, claiming a violation of Articles 7 and Article 8 of the Charter of Fundamental Rights of the EU, respectively the right to respect for private life and right to the protection of personal data, as well as Article 52(1) of the Charter and, inter alia, the principle of proportionality. [7] The NGO criticized[8]:

1) the extremely wide scope of that law and the definition of the data collected

2) the concept of 'passenger', within that same law, which leads to systematic, non-targeted automated processing of the data of all passengers.

3) the not sufficiently clear definition of the nature and detailed rules of the 'pre-screening' method and the databases against which those data are compared

4) the five-year retention period laid down by that law, which is considered disproportionate

5) the fact that Law of 25 December 2016 pursues objectives that are different from those of the PNR Directive.

Furthermore, the *Ligue des droits humains* asserted in its second argument that certain provisions of the Law of 25 December 2016, which extend the system provided for by the PNR Directive to intra-EU transport operations, have the consequence of indirectly reestablishing internal border control, which is against the principle of free movement of people.[9] Indeed, when someone arrives into Belgian territory, also just for a stopover, their information is automatically gathered.

The Belgian Council of Ministers disputed those arguments, asserting that the first plea was inadmissible because it concerned the GDPR, which does not apply to Law of 25 December 2016, and emphasized that data processing was a necessary and appropriate weapon in the war against terrorism and serious crime.[10]

The Belgian Constitutional Court, having doubts about the compatibility of such national legislation with obligations under EU law, had therefore decided to suspend the proceedings pending before it. In October 2019, the referring court, as part of its

[6] CJEU. *Ivi*. Para 52
[7] CJEU. *Ivi*. Para 54
[8] *Ibidem*
[9] CJEU. "Opinion on the Broader and Core Issues Arising in the PNR Case Currently before the CJEU (Case C-817/19)." SSRN, November 2021. Para 55
[10] CJEU. *Ivi*. Para 56

preliminary reference, asked the CJEU 10 questions. Given the high number of questions and the cryptic nature of some of them, the Court reformulated and group the questions, which resulted in a rather complicated structure of the decision itself.[11]

In particular, the *Cour costitutionelle* asked the Court of Justice of the EU, on the one hand, to interpret certain provisions of the GDPR[12], the API Directive[13], and Directive 2010/65[14]. On the other hand, several of the questions raised by the Belgian Constitutional Court concerned the interpretation and validity of the PNR Directive, in the light of Articles 7, 8 and 52(1) of the Charter. For the purposes of this dissertation, only the judgment's implications for the PNR Directive will be considered, while the other EU legal instruments will be left aside.

The referring court asked whether the PNR Directive complies with the Charter where, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security, it:

- Introduces a "system of generalised collection, transfer and processing of passenger data" (Question 4)
- Provides for "an advance assessment of passenger which is made by comparing passenger data against databases and pre-determined criteria" (Question 6)
- Prescribes a general data retention period of five years (Question 8)[15]

Question 5 and Question 7 concern the specific Belgian legislation that transposes the PNR Directive. The referring court asked whether the Law of 25 December 2016 is in conformity with the Charter where it:

[11] Beauregard-Lacroix, Raphaël. "Ligue Des Droits Humains (C-817/19): A Display of Consistency by a Steadfast and Pragmatic Court." *European Law Review* 48, no. 2. 2023: 220–31. p.221
[12] European Union. 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) (Text with EEA relevance). OJ L 119. 4.5.2016.
[13] *Council Directive 2004/82/EC* of 29 April 2004 on the obligation of carriers to communicate passenger data.
[14] European Union. Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC. *OJ L 283, 29.10.2010*
[15] Irion, Kristina. "Repairing the EU Passenger Name Record Directive: The ECJ's Judgment in Ligue Des Droits Humains (Case C-817/19)." *European Law Blog*, October 12, 2022. p. 4

- Includes monitoring activities within the remit of the intelligence and security services among the purposes for which PNR data is processed (Question 5)
- Grants power to the PIU (Passenger information unit) to authorise access to PNR data after six months had passed, for the purposes of *ad hoc* searches (Question 7)[16]

2. Interferences with fundamental rights

As a preliminary point at the beginning of its reasoning, the Court of Justice reiterated the general principle of interpretation, according to which an act of the European Union must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter of Fundamental Rights. Thus, "if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law."[17]

Additionally, the Court made it clear that when a Directive allows the Member States discretion to define transposition measures, "they must, not only interpret their national law in a manner consistent with the Directive in question but also ensure that they do not rely on an interpretation of the Directive that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law."[18]

The Court also observed that the PNR Directive itself contains a large number of recitals and provisions requiring such an interpretation. This highlights the importance that the European Union attaches to full respect for the fundamental rights enshrined in the Charter.

It can be noted how from the first paragraph the Court of Justice demonstrated that case C-817/19 is an *interprétation conforme* case.[19]

[16] *Ibidem*
[17] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 86
[18] CJEU. *Ivi*. Para 87
[19] Beauregard-Lacroix, Raphaël. "Ligue Des Droits Humains (C-817/19): A Display of Consistency by a Steadfast and Pragmatic Court." *European Law Review* 48, no. 2. 2023: 220–31. p.221

Bearing these premises in mind, the Court of Luxemburg evaluated, first of all, whether the PNR Directive's regulations conflicted with the fundamental rights protected by Articles 7 and 8 of the Charter.

The CJEU observed that the PNR data covered by that Directive include "besides the name(s) of the air passenger(s), information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers." Following the precedent set in Opinion 1/15[20], the Court reiterated that since PNR data contains information on the air passengers concerned, who are identified individuals, the various forms of processing to which those data may be subject affect the fundamental right to respect for private life (Article 7 of the Charter).[21] Additionally, the Court stated that the processing of PNR data is covered by Article 8 of the Charter and must therefore necessarily comply with its data protection requirements.

Recalling its established case law, the Court considered that "both the transfer of PNR data by air carriers to the PIU of the Member State concerned […] and the framework of conditions governing the retention of those data, their use and any further transfer to the competent authorities of that Member State, to the PIUs and the competent authorities of the other Member States, to Europol or to the authorities of third countries […] constitute interferences with the rights guaranteed in Articles 7 and 8 of the Charter."[22]

In its reasoning, the Court of Justice also pointed out that the interferences that the PNR Directive entails with the fundamental rights guaranteed in Articles 7 and 8 of the Charter are "undeniably serious interferences"[23], as the PNR Directive "seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services."[24] Furthermore, given how common the use of air transportation services is, the Court

[20] CJEU. Opinion 1/15 delivered on 26 July 2017, ECLI:EU:C:2016:656. para 121-122
[21] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 94
[22] CJEU. *Ivi*. Para 97
[23] CJEU. *Ivi*. Para 111
[24] *Ibidem*

recognized that the PNR Directive affects "a very large part of the population of the European Union."[25]

Having established the existence of such interference, the Court of Justice recalled the possibility for member states to justify such interference under Article 52(1) of the Charter. Thus, it decided to assess whether the conditions of that provision are met.

First, for what concerns the observance of the principle of legality the Court found that the PNR Directive is a valid legal text, which lays down in a clear manner the scope of the limitation on the exercise of the rights concerned, the purposes for processing PNR data and detailed rules for this operation.[26]

Furthermore, the Court affirmed that the interferences that the PNR Directive entails do not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter.

From the Court's reasoning, it can be inferred that the essence of the right to respect for private life is the type of data in question and what it reveals about the person it concerns. Indeed, according to the Court the essence of Article 7 is respected because even if PNR data may, in some cases, expose incredibly particular details about a person's private life, the nature of that information is still restricted to specific aspects of a person's private life: air travel. This is in line with what the CJEU had already stated in Opinion 1/15[27].

Furthermore, the PNR Directive expressly forbids the processing of sensitive data. Thus, "the data covered by that Directive do not by themselves allow for a full overview of the private life of a person."[28] Indeed, in Opinion 1/15, the Court had criticised the possibility of transferring sensitive data to the Canadian authority and had declared this action incompatible with the fundamental rights enshrined in the Charter.

For what concerns the essence of Article 8, it is considered to be respected because the PNR Directive "circumscribes the purposes for which those data are to be processed […] and lays down the rules governing the transfer, processing and retention of those data as well as the rules intended to ensure, inter alia, the security, confidentiality and integrity

[25] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 110
[26] Irion, Kristina. "Repairing the EU Passenger Name Record Directive: The ECJ's Judgment in Ligue Des Droits Humains (Case C-817/19)." *European Law Blog*, October 12, 2022. p. 6
[27] CJEU. Opinion 1/15 delivered on 26 July 2017, ECLI:EU:C:2016:656. Para 150
[28] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI :EU :C :2022 :491. Para 120

of those data, and to protect them against unlawful access and processing."[29] Indeed, the Court of Justice confirmed what it had already declared in Opinion 1/15: purpose limitation constitutes the essence of the right to data protection.

Then, the Court of Luxemburg clarified that since the purposes of the Directive are to ensure the internal security of the EU and to combat terrorism and serious crime[30], they "undoubtedly constitute objectives of general interest of the European Union that are capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter."[31]

Turning to the question of whether these measures are appropriate to reach the objectives provided for by the PNR Directive, the Court noted that although the automated data processing provided for by the Directive encounters limitations, they are not capable of rendering that system inappropriate for contributing to the attainment of the objectives pursued.[32]

Although the Court acknowledged that the number of false positive matches from automated processing is fairly substantial, amounting in 2018 and 2019 to at least five out of six individuals identified[33], it considered these measures appropriate for achieving the goal of protecting the life and safety of persons and the internal security of the EU. Indeed, according to the Court, the appropriateness depends on the proper functioning of the subsequent verification of the results, carried out by the PIU.[34] Thus, from the Court's perspective, error rates above 80% are not a problem, as long as there is a manual review of the automated matches.

3. The principle of proportionality and the necessity test

After having concluded that the interferences with fundamental rights are provided for by law, respect the essence of those rights, and are appropriate for reaching the objectives provided for by the Directive, the Court answered the question of whether the interferences from the PNR Directive are necessary. The necessity test envisioned for

[29] *Ibidem*
[30] Irion, Kristina. "Repairing the EU Passenger Name Record Directive: The ECJ's Judgment in Ligue Des Droits Humains (Case C-817/19)." *European Law Blog*, October 12, 2022. p. 4
[31] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI :EU :C :2022 :491. Para 121-122
[32] CJEU. *Ivi*. Para 123
[33] CJEU. *Ivi*. Para 106
[34] CJEU. *Ivi*. Para 124

the limitation of the right to data protection has, in the CJEU's jurisprudence, a high threshold: the measure providing for the interference must be 'strictly' necessary in light of the goals it sets.[35] Meeting the necessity test's threshold for a measure providing for a restriction of the right to personal data protection, particularly in matters relating to mass surveillance and data retention, requires "a careful drafting of the substantive content of that measure."[36]

The result of the Court's assessment is that the transfer, processing and storage of PNR data may be regarded as limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, provided that that Directive is interpreted in accordance with the fundamental rights in question. In its reasoning, the Luxemburg Court provided a number of interpretative clarifications for the PNR Directive to be held valid.

3.1. Air passenger data covered by the PNR Directive and the purposes for which those data may be processed

First of all, the Court assessed whether the data headings in Annex I to the PNR Directive defined in a clear and precise manner the PNR data that air carriers are required to provide to the PIUs. As a preliminary point, the Court of Justice clarified that "PNR data collected and provided in accordance with Annex I to the PNR Directive must relate directly to the flight operated and the passenger concerned and must be limited in such a way as to, on the one hand, meet solely the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime and, on the other, exclude sensitive data."[37]

With a Charter-conforming interpretation, certain PNR items in Annex I that contain open-ended formulations (like "including") and nonspecific data categories (like "frequent flyer information", "payment information" and "general remarks") are corrected for their flaws.[38] For instance, heading 5 "address and contact information (telephone number, email address)," is limited by the Court to the items in the parenthesis,

[35] Dalla Corte, Lorenzo. "On Proportionality in the Data Protection Jurisprudence of the CJEU. *International Data Privacy Law* 12, no. 4, 2022: 259–75. P.268-269
[36] *Ibidem*
[37] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI :EU :C :2022 :491. Para 128
[38] Irion, Kristina. "Repairing the EU Passenger Name Record Directive: The ECJ's Judgment in Ligue Des Droits Humains (Case C-817/19)." *European Law Blog*, October 12, 2022. p. 4

leaving out any details about third parties, such as someone making the reservation on the passenger's behalf.[39] The same applies for the heading 12, " general remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)." This is particularly important because this field may contain sensitive personal data, such as meal requests that indirectly reveal the passenger's religious practices or political orientations.[40]

Consequently, based on the analysis presented, the Court concluded that Annex I to the PNR Directive exhibits a satisfactory level of clarity and precision.

Second, the Court clarified that the PNR data collected are to be processed for the purposes of combating "terrorist offences" and "serious crime." Thus, it reiterated that only the objective of combating such crimes can justify the serious interference that the PNR Directive entails with the fundamental rights guaranteed by Articles 7 and 8 of the Charter. The same is not true of the objective of combating ordinary criminality, since the latter objective "may justify solely non-serious interferences."[41]

As regards the concept of "serious crime", the CJEU explained how, according to the PNR Directive, "serious crime" refers to those offences, listed in Annex II, that are "punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State."[42]

Thus, the PNR Directive provides only for a maximum penalty applicable, and not also for a minimum penalty. However, the Court clarified that "it cannot be ruled out that PNR data may be processed for the purposes of combating offences which, although meeting the criterion laid down by that provision relating to the threshold of severity, amount to ordinary crime rather than serious crime, having regard to the particular features of the domestic criminal justice system."[43]

---

[39] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 131

[40] Lund, Jesper. "Mass Surveillance of External Travellers May Go on, Says EU's Highest Court." European Digital Rights (EDRi), July 7, 2022. Last accessed 01/09/2023 at https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/.

[41] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 148

[42] CJEU. *Ivi*. Para 144

[43] CJEU. *Ivi*. Para 151

The Court recognised this problem and placed a burden on the Member States, stating that "it is for the Member States to ensure that the application of the system established by the PNR Directive is effectively limited to combating serious crime and that that system does not extend to offences that amount to ordinary crime." The Court further limited the scope of criminal offences by stating that they must also have an objective link, at least indirectly, with the carriage of passengers by air, and consequently with the categories of data transferred, processed and retained in the application of the PNR Directive.[44]

However, it cannot go unnoticed that the Court of Justice did not offer any more direction on how to interpret the goal of fighting crime or how the relationship to passenger air transportation is to be achieved.[45] This, as Brouwer observes, "leaves an important task not only for the national legislatures to ensure these limitations when implementing the PNR Directive, but also for the data protection authorities and courts when supervising this."[46]

3.2. Air passengers and flight concerned

According to Article 8(1) of the PNR Directive, the PNR data of any passenger are transferred to the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, regardless of whether there is any objective material from which it may be inferred that the passengers concerned may present a risk of being involved in a terrorist offence or serious crime. [47]

The data transferred are processed by automated means in connection with the advance assessment provided for by the PNR Directive, which has the goal of identifying people who were not previously suspected of involvement in serious crimes or terrorist offences but who should be subject to further investigation by the relevant authorities.[48]

In its reasoning, the Court of Justice drew a distinction between flights between a Member State and a third State (extra-EU) and flights between Member States (intra-EU).

---

[44] CJEU. *Ivi*. Para 153-157
[45] Brouwer, Evelien. "Ligue Des Droits Humains and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in Times of New Technologies." *Common Market Law Review* 60, no. Issue 3, 2023: 839–62. p. 849
[46] *Ibidem*
[47] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 158-159
[48] *Ibidem*

In the first case, the Court of Justice, following its precedent in Opinion 1/15, considered that the systematic transfer and prior assessment of the PNR data of air passengers entering or leaving the Union facilitates and expedites security checks, in particular at borders. Furthermore, a targeted data transfer, for instance with the exclusion of certain categories of persons, or of certain areas of origin, would prevent the achievement of the objective of identifying persons who could present a risk to public security from amongst all air passengers.

Thus, the Court concluded that "it must be found that the necessary connection between those data and the objective of combating such offences exists, with the result that the PNR Directive does not go beyond what is strictly necessary merely because it imposes on Member States the systematic transfer and advance assessment of the PNR data of all those passengers."[49]

As regards intra-EU flights, first of all, the Court noted that the Directive does not impose an obligation on Member States to extend the system to intra-EU flights. Instead, Member States are given discretion to do so. Furthermore, a Member State that wishes to avail itself of that option, must verify that the extension of the system established by the Directive to all or some of the intra-EU flights is "strictly necessary, […] in order to ensure the internal security of the European Union or, at least, that of that Member State and, thus, protect the life and safety of persons."[50] Drawing from its decision in *La Quadrature du Net*[51], the Court recognized that if a Member State acknowledges the existence of a terrorist threat, which is real, present or foreseeable, the extension of the PNR scheme to intra-EU flights from or to the said Member State is strictly necessary and therefore justified. However, the Court required additional limitations: (1) the terrorist threat must be genuine and present or foreseeable, (2) the extension must be limited in time to what is strictly necessary and (3) it must be subject to effective review, either by a court or by an independent body whose judgment is binding.[52]

By contrast, the Court underlines that "in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, the indiscriminate application by that Member State of the system established by the PNR

[49] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 162
[50] CJEU. *Ivi*. Para 169
[51] CJEU. Joined Cases C-511, 512 & 520/18, *La Quadrature du Net and others*, EU:C:2020:791. Para 137
[52] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 171-172

Directive not only to extra-EU flights but also to all intra-EU flights would not be considered to be limited to what is strictly necessary."[53]

In other words, when Member States are unable to demonstrate the existence of a terrorist threat, they cannot extend the application of the PNR Directive to all intra-EU flights, but only to flights related to certain routes, travel patterns, or airports. The Court did not explicitly mention the grounds for which the extension could be deemed to satisfy the strict necessity test.

Furthermore, the Court did not require an effective review of the extension by an independent authority, but in this case, the Member States themselves must regularly reassess the strictly necessary nature of such application to the selected intra-EU flights, in the light of developments of the conditions that justified their selection.[54] Therefore, "it appears that independent review is required for the collection of PNR data when that collection is applied to all intra-EU flights, but the Member States have more flexibility as regards review of their assessments leading to a selection of intra-EU flights."[55]

3.3. Advance assessment of PNR data by automated processing

For what concerns the preliminary assessment of PNR data using automated processing, the purpose of which is to identify passengers to be subjected to further verification before their arrival or departure, the Court explained that the PNR Directive provides the advance assessment to be carried out in two stages.[56]

In the first phase, the PIU of the Member State concerned processes PNR data by comparing them with databases or pre-determined criteria. In a second phase, in the event that such automated processing results in a positive match (hit), that unit carries out a non-automated individual review to verify whether an intervention of the competent authorities of the Member States is necessary (match).

As for the first phase, in order to ensure that the advance assessment is in conformity with the Charter, the Court imposed restrictions on the databases against which the PIU may compare PNR data: they must be the non-discriminatory databases

[53] CJEU. *Ivi*. Para 173
[54] CJEU. *Ivi*. Para 174
[55] 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, last accessed 20/08/2023.
[56] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 177

on persons sought or under alert and must be used in connection with the fight against terrorist offences and serious crimes which have an objective connection, at least indirectly, with the carriage of passengers by air.[57] This excludes other databases[58], such as those "managed and exploited by the security and intelligence agencies of Member States in order to pursue objectives other than those referred to in the Directive."[59]

However, Member States can also process PNR data by comparing them with pre-determined criteria. The European Commission in its 2020 report on the PNR Directive has defined these algorithms as "search criteria, based on the past and ongoing criminal investigations and intelligence, which allow to filter out passengers which corresponds to certain abstract profiles, e.g. passenger travelling on certain routes commonly used for drug trafficking, who bought their ticket in the last moment and paid in cash, etc."[60]

In the event that the PIU decides to carry out the advance assessment on the basis of pre-determined criteria, the Court clearly excluded the possibility of using artificial intelligence technologies in self-learning systems (also referred to as "machine learning") because these systems (1) modify without human intervention and (2) may be opaque and unexplainable. In this passage, the Court addressed one of the contemporary challenges: the lack of transparency in decision-making based on machine-learning systems.[61] Opacity was indeed crucial in determining the exclusion of such systems, because it makes them impossible to dispute, as the Court noted "given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter."[62] However, as the words "might" and "may" in the aforementioned quote show, this paragraph does not impose a permanent ban on the use of self-learning algorithms for surveillance

[57] CJEU. *Ivi*. Para 190-191
[58] Irion, Kristina. "Repairing the EU Passenger Name Record Directive: The ECJ's Judgment in Ligue Des Droits Humains (Case C-817/19)." *European Law Blog*, October 12, 2022. p. 4
[59] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 184
[60] 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). 24 July 2020. p.11, footnote 36
[61] Brouwer, Evelien. "Ligue Des Droits Humains and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in Times of New Technologies." *Common Market Law Review* 60, no. Issue 3, 2023: 839–62. p. 855
[62] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491.Para 194

purposes, should these algorithms become simple to interpret/review by a human and, as a result, be explainable and challengeable.[63]

Then, the Luxemburg Court made clear that pre-determined criteria used for the purposes of advance assessment must respect certain requirements: they must be targeted, proportionate and specific. To be deemed targeted, specific, and proportionate four criteria have to be respected.

First of all, they must be defined in such a way that "while worded in a neutral fashion, their application does not place persons having the protected characteristics at a particular disadvantage."[64]

Second, they must identify only "individuals who might be reasonably suspected of involvement in terrorist offences or serious crime covered by that Directive."[65]

Third, they must be defined in such a way as to take into consideration both 'incriminating' as well as 'exonerating' circumstances, suggesting that the traveller is perhaps implicated in serious crimes or terrorist offences.

Lastly, they must be subject to regular review, meaning that they must be updated in accordance with the circumstances justifying their being taken into consideration, but also taking into account acquired experience to reduce as much as possible the number of "false positives".[66]

The Court of Justice also highlighted the concern about potential discrimination, building upon the recognition of these risks in Article 6(4) of the PNR Directive, according to which pre-determined criteria can never be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. The Court then clarified that this provision encompasses both direct and indirect forms of discrimination. [67]

As Thönnes and Vavula observed, this clarification of the Court of Justice holds utmost importance, because predetermined criteria could be founded on seemingly harmless personal information that, however, might actually act as proxies of prohibited

[63] Korff, Douwe. "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. p.13
[64] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 197
[65] CJEU. *Ivi*. Para 198
[66] CJEU. *Ivi*. Para 201
[67] *Ibidem*

characteristics.[68] For instance, a person's address might inadvertently serve as an indicator of their religion, race, or ethnic background.

In view of the error rate inherent in automated processing of PNR data and of the rather substantial number of "false positive" results obtained during 2018 and 2019, the Court underlined that the appropriateness of the system to attain the objectives pursued depends essentially "on the proper functioning" of the individual review carried out by the PIU. This refers to the second stage of the advance assessment, when, in the event of a positive match following automated processing, the PIU carries out a non-automated individual review to verify whether intervention by the national competent authorities is required. This review must be guided by "clear and precise rules", which Member States have to come up with, but remain not specified in the decision.[69]

Then, the Court of Justice explained first of all that Member States have the responsibility to ensure that the unit "maintains documentation relating to all processing of PNR data carried out in connection with the advance assessment, including in the context of the individual review by non-automated means, for the purpose of verifying its lawfulness and for the purpose of self-monitoring."[70] This is also particularly important to ensure that the data subject can exercise his or her right to judicial redress.

Moreover, the Court underlined that Member States are prohibited from taking any decision that produces an adverse legal effect on a person or significantly affects a person only because of the automated processing of PNR data. They must give preference to the result of the individual review conducted by non-automated means by the PIU over that obtained by automated processing.[71]

To summarize, competent authorities must ensure:

1. The lawfulness of automated processing

2. The non-discriminatory character of automated processing

3. The individual review, in case of result of a "positive match", to be carried out by non-automated means.

[68] Thönnes, Christian, and Niovi Vavoula. "Automated Predictive Threat Detection after Ligue Des Droits Humains: Implications for Etias and CSAM (Part I)." *Verfassungsblog.* 2023.
[69] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 205
[70] CJEU. *Ivi*. Para 207
[71] CJEU. *Ivi*. Para 207-208

4. The comprehensibility of the functioning of the predetermined assessment criteria and of the programmes applying those criteria for data subjects.
In this way, data subjects can decide with full knowledge of the facts, whether to exercise their right to a judicial remedy, in order to challenge, where appropriate, the unlawful and discriminatory nature of those criteria.[72]

As a result, results can only be transferred to the competent national authorities when the PIU, after having conducted the individual review, establishes that there is a "reasonable suspicion of involvement in terrorist offences or serious crime of persons identified by means of automated processing operations."[73]

3.4. The disclosure and subsequent assessment of PNR data

Six months after the collection of data, "disclosure of the full PNR data shall be permitted only" when it is "reasonably believed [to be] necessary"[74] and to respond "on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities […] in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime."[75]

The Grand Chamber interpreted the terms "sufficient grounds" and "reasonably" in Article 6 (2)(b) and Article 12(3)(a) of the PNR Directive, respectively, in light of Articles 7 and 8 of the Charter, as referring to "objective material capable of giving rise to a reasonable suspicion that the person concerned is involved […] in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air […] and when there is objective material from which it can be inferred that the PNR data could, in a given case, contribute effectively to combating such offences"[76]

The Court then recalled the procedural conditions governing the disclosure and processing of PNR data, which, except in the event of duly justified urgency, can only take place after a prior review carried out either by a court or by an independent administrative authority, following a reasoned request by the competent authorities.[77]

[72] CJEU. *Ivi*. Para 209-210
[73] CJEU. *Ivi*. Para 204
[74] European Union. Directive (EU) 2016/681. Art.6(2)(b)
[75] European Union. Directive (EU) 2016/681. 12(3)(a)
[76] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 220
[77] *Ibidem*

Finally, the Court of Justice specified the characteristics that the authority responsible for such a prior review must possess. That authority must in fact have "all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue."[78] Therefore, such an authority must have a status that enables it to act objectively and impartially when carrying out its duties and must, therefore, be free from any external influence. [79]

The Court then answered the question of whether the PIU can also be designated as a competent national authority with the power to approve the disclosure of PNR data upon expiry of the period of six months, as it was provided for in the Belgian legislation implementing the PNR Directive. The CJEU concluded that this interpretation has to be rejected.[80]

Indeed, the PIU may very possibly consist of employees from the same agency as the one making the request, such as the police, state security, general intelligence, or customs. Therefore, it cannot be viewed as a neutral third party.

In conclusion, the Court stated that the provisions of the PNR Directive governing the subsequent disclosure and assessment of PNR data can be interpreted in a way that is consistent with Articles 7 and 8 as well as Article 52(1) of the Charter and are thus within the limits of what is strictly necessary.

3.5. The data retention period

As regards the retention period, the Court held that the retention of the PNR data of all air passengers during the initial period of six months, without any indication as to their involvement in terrorist offences or serious crime "does not appear, as a matter of principle, to go beyond what is strictly necessary."[81]

However, Article 12(1) of the PNR Directive provides that "Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing."[82] The Court of Justice found that the

[78] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 225
[79] CJEU. *Ivi*. Para 226
[80] CJEU. *Ivi*. Para 244-245
[81] CJEU. *Ivi*. Para 255
[82] European Union. Directive (EU) 2016/681. Article 12

five-year period provided for by Article 12(1) of the Directive "entails an inherent risk of disproportionate use and abuse."[83]

Thus, the Court, giving a Charter-conforming interpretation, stated that PNR data can be retained for a maximum of five years, only if it is strictly necessary, that is if there is objective evidence suggesting that the passenger may have been involved in serious crimes or terrorist offences.[84]

In conclusion, the Luxemburg Court, altering the Directive and going against the words of the EU legislator, precluded "national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers."[85]

4. Key findings and unresolved questions

The Grand Chamber has put all of its efforts *not* to invalidate the PNR Directive, and it was able to do so by providing a Charter-compliant interpretation of its text.[86]

Indeed, as a preliminary point, the Court emphasized that "if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law."[87] However, as Thönnes[88] has noted, it is also an established principle of EU law that, at least for national law, a valid interpretation must not trespass on the limit of *contra legem.* It is very difficult to understand why this would not apply to the compatibility of EU secondary legal acts, like the PNR Directive, with primary EU law. If a secondary legal act does not already contain language that meets the requirements for compatibility with primary law, the Court should not invent it.[89]

---

[83] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491.. Para 256
[84] CJEU. *Ivi*. Para 260
[85] Brouwer, Evelien. "Ligue Des Droits Humains and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in Times of New Technologies." *Common Market Law Review* 60, no. Issue 3, 2023: 839–62. p. 861
[86] Thönnes, Christian. "A Directive Altered beyond Recognition: On the Court of Justice of the European Union's PNR Decision (C-817/19)." Verfassungsblog. Last accessed 29/08/2023 at https://verfassungsblog.de/pnr-recognition/.
[87] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 86
[88] Thönnes, Christian. "A Directive Altered beyond Recognition: On the Court of Justice of the European Union's PNR Decision (C-817/19)." Verfassungsblog. Last accessed 29/08/2023 at https://verfassungsblog.de/pnr-recognition/.
[89] *Ibidem*

This is more than just a democratic legitimacy issue because, without a supporting legal text, it will be impossible for Member States to comply with the revised PNR Directive.[90]

Furthermore, in its decision the Court of Justice decided to apply a different standard for extra-EU and intra-EU flights.

First, it must be reminded that the Directive requires only the collection of PNR data of passengers of extra-EU flights (flights from third countries to the European Union or from the European Union to third countries).[91] Article 2(1) of the Directive then allows for the potential expansion of this regime to cover flights within the EU.[92]

In line with its judgement in Opinion 1/15 on the EU-Canada PNR agreement, the Court chose not to apply its case law on communications data retention and stated that, for what concerns extra-EU flights, the indiscriminate transfer of PNR data is proportionate and limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime.

Instead, the collection and processing of PNR data from intra-EU flights is only limited to what is strictly necessary given that certain requirements set by the Court are respected. Indeed, in order to extend the PNR scheme to intra-EU flights, there must be an effective review carried out by a Court or by an independent administrative authority whose ruling is binding.

The Court underlined that the application of the PNR Directive to all intra-EU flights from or to that Member State, for a period that is limited to what is strictly necessary (but may be extended), does not go beyond what is strictly necessary in the one circumstance where the Member State establishes that there are sufficiently strong grounds for considering that it is confronted with a terrorist threat, which is genuine and present or foreseeable.

If that is not the case, the application of the said Directive must be limited to intra-EU flights relating to certain routes or travel patterns or to certain airports for which there are, at the discretion of the Member State indications that would justify that application. Furthermore, in light of changes in the conditions that led to the chosen intra-EU flights'

[90] *Ibidem*
[91] European Union. Directive (EU) 2016/681. Art. 1
[92] *Ivi.* Art.2(1)

selection, the strictly necessary character of that applicability to those flights must be periodically evaluated.

Among the questions that have not been answered yet, is the reliability of the PNR data collected. Indeed, as Korff observes, travellers themselves submit the PNR data. Air carriers are required to send PNR data in line with Article 8 of the Directive to the extent that they have previously gathered such data as part of their regular business operations.[93] However, they are not required to make sure that the information sent to the authorities is true, complete, accurate, and updated. Only failure to send PNR data or failure to transmit it in the proper format are grounds for sanctions under Article 14 of the PNR Directive. The biggest obstacle preventing national authorities from using PNR data to its fullest extent is problems resulting from the low quality and incompleteness of the data[94]. Both in Opinion 1/15 and in case C-817/19, the Court failed to address the declaratory and unverified nature of PNR data.

Moreover, the Grand Chamber failed to take into account the consequences and the impact of the errors resulting from automated data processing on the lives of innocent individuals. In order to understand those consequences, the following example may be helpful.

Mario Rossi lives in Rome and has a flight booked to Los Angeles at the end of May because his daughter is getting married. A few days before the flight, the US Embassy in Italy informs him that his electronic travel authorisation has been cancelled. For this reason, Mario Rossi decides to go to the US Embassy to apply for a visa. However, the consular officer informs him that his travel authorisation had been revoked because the algorithm has identified him as a security threat.

The officer did not know what had triggered the algorithm but suggested that it could be something Mario was involved in, people he is or was in contact with, places to which he had travelled, hotels at which he stayed, or a certain pattern of relations among these things. The officer said that Homeland Security investigators could assess the case more promptly if he supplied the embassy with additional information, including 15 years

[93] Korff, Douwe. "Opinion on the Broader and Core Issues Arising in the PNR Case Currently before the CJEU (Case C-817/19)." SSRN, November 2021. p.59
[94] *Ibidem*

of travel history, in particular where he had gone and who had paid for it, or the names of anyone in his network whom he believed might have triggered the algorithm. [95]

Although this example refers to the US security system, in light of the Court's judgment in case C-917/19, comparable situations might soon occur in the European Union as well.[96]

In line with Opinion 1/15, the Court does not take much into account the margin of error inherent in the automated processing of PNR data and the fairly substantial number of 'false positives' obtained as a result of their application in 2018 and 2019. From the Court's perspective, the number of innocent persons identified can be largely reduced thanks to individual review by non-automated means.

However, according to the Commission staff working document, which accompanied the 2020 Report from the Commission, 0.59% of all passengers whose data have been collected have been identified through automated processing as requiring further examination, and an even smaller fraction of 0.11% was transmitted to competent authorities.[97] Based on these data, the Commission concluded that "overall, PNR systems deliver targeted results which limit the degree of interference with the rights to privacy and the protection of personal data of the vast majority of bona fide travellers."[98]

Looking closer at the figures, a sixth (0.11%) of the positive hits for the initial advance assessment, were transmitted to national law enforcement after the manual review step. This indicates that 0.48% of those people were unjustly flagged as suspicious by an automated processing system.[99]

Although this may seem like a small portion, it represents almost two and half million air travellers annually, considering the Eurostat estimate of 500 million individual air passengers a year.[100]

---

[95] Weizman, Eyal. "The Algorithm Is Watching You." LRB Blog, February 19, 2020. Last accessed 29/08/2023 at https://www.lrb.co.uk/blog/2020/february/the-algorithm-is-watching-you.
[96] Guild, Elspeth, and Tamas Molnar. "The European Legal Architecture on Security: New Developments in the Complex Relationship between the Public and Private Sectors in Data Processing." Verfassungsblog. Last Accessed 28/08/2023. https://verfassungsblog.de/pnr-architecture/.
[97] European Commission. Commission Staff Working Document accompanying the Commission Report. SWD(2020) 128 final. COM(2020) 305 final. 24 July 2020. p.28
[98] *Ibidem*
[99] Beauregard-Lacroix, Raphaël. "Ligue Des Droits Humains (C-817/19): A Display of Consistency by a Steadfast and Pragmatic Court." *European Law Review* 48, no. 2. 2023: 220–31. p.230
[100] Korff, Douwe. "Opinion on the Broader and Core Issues Arising in the PNR Case Currently before the CJEU (Case C-817/19)." SSRN, November 2021. p.84

Furthermore, the Court of Justice put its trust in Member States to come up with "clear and precise criteria" for an effective individual review of automated processing, but these criteria are nowhere to be found in the decision.

It is challenging to imagine any review criterion that would be effective in reducing the excessive rate of false positives. The base rate fallacy, as previously mentioned, makes this rate a statistical near certainty, which is why many believe that the PNR system is and will continue to be ineffective in reducing terrorism and serious crime.[101]

Moreover, for what concerns automated data processing the Court prohibited the use of self-learning algorithms that:

(1) are able to modify their evaluation criteria without human intervention or review;

(2) are too opaque to allow for an effective judicial remedy against their recommendations has been largely appreciated.

However, while at first glance this prohibition may seem like a victory, it is important to underline how it does not represent a complete ban. In other words, the Court prohibited the majority of the AI software that is now available, but it is not unlikely that AI software might eventually give adequate justifications for their choices.[102]

Therefore, although the ban on self-learning algorithms is a positive step in the right direction, without additional legal clarification, security agencies might still get around this ban by using the appropriate AI systems.[103]

[101] Thönnes, Christian. "A Directive Altered beyond Recognition: On the Court of Justice of the European Union's PNR Decision (C-817/19)." Verfassungsblog. Last accessed 29/08/2023 at https://verfassungsblog.de/pnr-recognition/.
[102] *Ibidem*
[103] *Ibidem*

Conclusion

The judgement of the CJEU in case C-817/19 fits perfectly into the Court's case law concerning the conflicting relationship between public safety and the protection of the privacy of individuals and their data.

With its declaration of incompatibility with fundamental rihts PNR Agreement between the EU and Canada in Opinion 1/15, the Court of Justice of the EU upheld the high standards for privacy and data protection that it had outlined in the landmark previous trilogy of decisions (*Digital Rights Ireland, Schrems, Tele2 Sverige*).[104] Indeed, for years the Court had seemed "like a steady bulwark against surveillance scenarios."[105]

While many had expected and hoped for the CJEU's decision in *Ligue des droits humains* to result in the total or partial annulment of the PNR Directive, given its resemblance to provisions in the EU-Canada PNR Agreement, which were declared incompatible with the Charter of Fundamental Rights of the EU in Opinion 1/15, the Court's verdict was a different one.

The Luxemburg Court carefully interpreted the PNR Directive with a Charter-compliant approach, seeking to preserve EU secondary law while striving to strike the right balance between privacy and security at the national level.

To that end, the Court imposed so many limitations that some scholars have criticized how this Directive was altered "beyond recognition": the PNR Directive that is upheld by this ruling differs significantly from the one that was submitted for review, with almost none of its central provision unrestricted.[106]

For instance, the Luxemburg Court restricted the application of Article 2(1), which allows Member States to expand the PNR system to intra-EU flights. Almost all of the Member States used this option, and some, like Belgium, even expanded the PNR system to other forms of transportation including buses, trains, and ferries.

The CJEU considered this indiscriminate expansion excessive and clarified that it could only permitted under extraordinary circumstances, specifically when the Member State is confronted with a terrorist threat that is shown to be genuine and present or

[104] Mendez, Mario. "Opinion 1/15: The Court of Justice Meets PNR Data (Again!)". *European Papers*, *Vol. 2, No 3, 2017: 803-818*. p. 817
[105] Thönnes, Christian. "A Directive Altered beyond Recognition: On the Court of Justice of the European Union's PNR Decision (C-817/19)." Verfassungsblog. Last accessed 29/08/2023 at https://verfassungsblog.de/pnr-recognition/.
[106] *Ibidem*

foreseeable, and this decision has to be reviewed by a court or an independent administrative body.[107]

A stricter approach was also adopted for what concerns the storage period and once again the Court altered the words of the EU legislator.

Indeed, although Article 12[108] of the Directive provides for a five-year retention period, applied indiscriminately to all air passengers, the Court underlined that the retention of the PNR data of all air passengers does not go beyond what is strictly necessary only during the initial period of six months. PNR data can be retained for a maximum of five years, only if there is objective evidence suggesting that the passenger may have been involved in serious crimes or terrorist offences.

However, even after this ruling, there are significant issues that remain unaddressed, such as the reliability of the PNR data collected, or the potential negative effects of errors resulting from automated processing on innocent individuals. Furthermore, the Court's reliance on individual review as a means to rectify false positives raises questions about the overall effectiveness of the PNR system.

Also, it has to be noted that the Court of Justice placed a disproportionate amount of faith in the Member States to apply the PNR Directive in a limited manner to comply with the Charter's requirements.[109] For instance, while the Directive does not sufficiently address the dangers of misuse by investigating authorities and the use of PNR data for ordinary crime, the Court relied on Member States to limit the use of the PNR system in the fight against terrorism and serious crime.

Still, the considerations of the Court of Justice of the European Union about mass data retention, the use of automated risk models, and the creation and application of pre-determined criteria are relevant far beyond the scope of the PNR Directive.[110] They underscore the need for continuous scrutiny, legal clarification, and ongoing dialogue to ensure that fundamental rights are preserved while addressing modern security challenges.

---

[107] CJEU. Case C-817/19, *Ligue des Droits Humains v. Council of Ministers,* ECLI:EU:C:2022:491. Para 172-173

[108] European Union. Directive (EU) 2016/681. Art.12

[109] Lund, Jesper. "Mass Surveillance of External Travellers May Go on, Says EU's Highest Court." European Digital Rights (EDRi), July 7, 2022. Last accessed 01/09/2023 at https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/.

[110] Brouwer, Evelien. "Ligue Des Droits Humains and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in Times of New Technologies." *Common Market Law Review* 60, no. Issue 3, 2023: 839–62. p. 861

CONCLUSIONS AND FINAL REMARKS

As stated in the introduction, this research aimed at understanding if the Court of Justice of the European Union has been able to uphold the right to privacy and the right to protection of personal data of air passengers while ensuring national security, in particular in the context of combating terrorism. In order to provide an answer to this question, two rulings of the CJEU which relate to the sharing of Passenger Name Record data of air passengers have been analysed: Opinion 1/15 and *Ligue des droits humains*.

In Opinion 1/15, the Court of Justice was asked to assess the compatibility of the EU-Canada PNR Agreement with the Charter of Fundamental Rights of the EU and with the Treaties. The CJEU stated that the Agreement could not be concluded in its current form because of the incompatibility of several provisions with the fundamental rights recognised by the Union.

In this landmark judgment, the Court of Justice applied numerous principles which were elaborated in its previous decisions on privacy and data protection, to the particular area of PNR data and international agreements between the European Union and third countries. Therefore, the Court of Justice seized this opportunity, presented by the request for an opinion from the European Parliament, to strengthen its authority as a constitutional Court upholding fundamental rights. Furthermore, the Court of Justice of the European Union had the chance to clarify that it enjoys specific competences regarding the conclusion, interpretation and application of international treaties to which the EU is a party.[111] In particular, it can determine *ex ante*[112] or *ex post*[113] whether an international treaty is compatible with the EU treaties. On this particular occasion, the Court of Justice of the EU evaluated the compatibility of an international agreement with the rights outlined in the Charter of Fundamental Rights of the EU for the first time.

At the same time, the Luxemburg Court was able to consider national security concerns: it declared the massive collection and retention of PNR data a measure

[111] Think Tank European Parliament. "European Court of Justice and International Agreements." Last Accessed 10/09/2023 at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)696171.

[112] Article 218(11) TFEU provides that a Member State, the European Parliament, the Council or the European Commission may obtain the opinion of the ECJ as to whether an international agreement is compatible with the Treaties.

[113] The CJEU can also verify the legality of an international agreement after it has already entered into force. Indeed, within the hierarchy of acts constituting the EU legal order, international agreements are placed below the EU Treaties.

appropriate to fight terrorist offences and serious crime, and also a measure compatible with the Charter of Fundamental Rights, but only as long as the transfer of sensitive data is prohibited. Indeed, this transfer could lead to discriminatory treatment, in direct violation of Article 21 of the Charter, and according to the Court, this could only be permitted with a precise and robust justification, one that goes beyond the mere protection of public security against terrorism and serious transnational crime. By carefully highlighting the flaws of the Agreement and explaining in detail what guarantees were lacking, the Court of Justice set an important standard for future negotiations of PNR agreements between the European Union and third countries. Indeed, this decision serves as a benchmark for future negotiations, promoting a more responsible and rights-oriented approach to data sharing on a global scale.

For what concerns Opinion 1/15, from the analysis carried out in this thesis it can be concluded that the Court acknowledged the importance of security measures, which are necessary to face the terrorist threat. However, it also upheld fundamental rights, by imposing stringent requirements on the legality of such measures, emphasizing the need for clear and precise rules, proportionality, and safeguards to prevent abuse.

In the second ruling, *Ligue des droits humains*, the Court of Justice had the opportunity to evaluate the validity of the EU PNR Directive. Even though certain provisions of the said Directive are identical to those contained in the Agreement between the European Union and Canada, the Court decided not to invalidate the PNR Directive and declared it compatible with the Charter of Fundamental Rights. Precisely for this reason, one might think that the Court changed direction, and that the conflicting relationship between national security and privacy, in the face of the threats of international terrorism, ended up being hugely unbalanced in favour of national security.

One thing that must be considered is that in respect of democratic legitimacy, the Court of Justice of the European Union must always consider very carefully the option of invalidating a Directive. Indeed, the adoption of a Directive at the EU level is a long and complex legislative process, as it was shown in the first chapter of this work through the description of the long and difficult journey that led to the adoption of the EU PNR Directive. This process involves the European Commission, the European Parliament and the European Council. It involves lengthy discussions, negotiations and multiple approvals.

After the European Commission's proposal, the European Parliament and the Council must reach an agreement on the text of the Directive, which implies a broad consensus and sometimes even compromises between Member States before the Directive is adopted. Thus, the Court is always very cautious in invalidating a Directive and in leaving a legal vacuum.

Moreover, as demonstrated through the analysis of the *Ligue des droits humains case*, an act of the European Union must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter of Fundamental Rights.

It is quite difficult to provide a straightforward answer to the question as to whether the Court's judgment in *Ligue des droits humains* signifies a turning point where national security interests weighed more heavily in the balance with data protection. It can be affirmed with certainty that in this case the Court of Justice was presented with a complex balancing exercise.

On the one hand, the CJEU declared the EU PNR Directive valid, thus allowing bulk data collection and retention in order to protect national security. On the other hand, to ensure the compatibility of such Directive and to ensure the protection of air passengers' fundamental rights, the Court of Justice imposed significant restrictions on the Directive's text. This approach led to substantial revisions and the introduction of safeguards, ensuring that any potential invasion of privacy is kept to a minimum.

As a result, almost none of the central provisions of the original Directive submitted for review remain unaltered. Furthermore, some of the interpretations provided for by the Court of Justice are in open contradiction with the original text of the Directive. For example, although Article 12[114] of the PNR Directive provides for a five-year retention period, applied indiscriminately to all air passengers, the Court underlined that the retention of the PNR data of all air passengers does not go beyond what is strictly necessary only during the initial period of six months.

For this reason, some have observed how the Court has adopted a "rule-creating role."[115] In other words, the Court by avoiding to invalidate the Directive showed respect to the EU legislative body. However, this led the Court to adopt a legislative role of its

[114] European Union. Directive 2016/681. Art.12

[115] Duroy, Sophie. "Case C-817/19, Ligue Des Droits Humains V. Council of Ministers (C.J.E.U.)." *International Legal Materials*, 2023, 1–60. https://doi.org/10.1017/ilm.2023.08. p.3

own. Indeed, the Court of Justice of the European Union acted not only as a constitutional court but also as a political actor, with the power of altering almost completely legislative acts to ensure that the fundamental rights of the EU citizens are protected. Indeed, now Member states face a revised standard for compliance: the recommendations and changes made by the Court of Justice rather than the PNR Directive's text.

At the same time, it could be argued that if a secondary legal act does not already contain language that meets the requirements for compatibility with primary law, the Court should not invent it.[116]

In conclusion, it is clear that the Luxemburg Court plays a key role in guiding Member States, policymakers, and legal experts in finding a fair balance between two competing and conflicting interests such as national security and data protection. In this sense, it can be stated that also in *Ligue des droits humains*, through the numerous restrictive interpretations of the PNR Directive, the Court of Justice was able to ensure the protection of air passengers' fundamental rights, while safeguarding national security.

However, this judgment of the Court of Justice also leaves many open questions. Indeed, without a supporting legal text, it will be impossible for Member States to comply with the revised PNR Directive.[117] For this reason, it is possible to affirm with certainty that this will not be the last case on PNR before the Court of Justice of the European Union.

[116] Thönnes, Christian. "A Directive Altered beyond Recognition: On the Court of Justice of the European Union's PNR Decision (C-817/19)." Verfassungsblog. Last accessed 29/08/2023 at https://verfassungsblog.de/pnr-recognition/.
[117] *Ibidem*

BIBLIOGRAPHY

Advocate General Paolo Mengozzi. Opinion 1/15 delivered on 8 September 2016, ECLI:EU:C:2016:656.

Alenka Kuhelj. 2010. The Twilight Zone of Privacy for Passengers on International Flights Between the EU & USA, 16 U.C. DAVIS J. INT'L L. & POL'Y, 2010: 383-408.

Beauregard-Lacroix, Raphaël. 2023. "Ligue Des Droits Humains (C-817/19): A Display of Consistency by a Steadfast and Pragmatic Court." *European Law Review 48, no. 2.* 2023: 220–31.

Bernabe, Elisabeth. 2023. "Central counterterrorism coalition: an analysis of intelligence sharing and the challenges it faces in the European union." *Minnesota Journal of International Law*, 32(1), 241-268.

Bignami, Francesca, and Giorgio Resta. 2015 "Transatlantic Privacy and Regulation: Conflict and Cooperation." *Law and Contemporary Problems* 78, no. 4: 231–266.

Bignami, Francesca. 2011. "Privacy and Law Enforcement in the European Union: The Data Retention Directive." *Chicago Journal of International Law*, Article 13, Volume 8, no. 1. 233–55

Brouwer, Evelien. 2009. "Towards a European PNR System ? Questions on the Added Value and the Protection of Fundamental Rights: Think Tank: European Parliament." Think Tank. European Parliament.

Brouwer, Evelien. 2023. "Ligue Des Droits Humains and the Validity of the PNR Directive: Balancing Individual Rights and State Powers in Times of New Technologies." *Common Market Law Review 60*, no. Issue 3, 2023: 839–62.

Bug, Mathias. & Bukow, Sebastian. 2017. "Civil liberties vs. security: Why citizens accept or reject digital security measures". *German Politics,* 26(2), pp. 292-313

Buttarelli, Giovanni. 2016. "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard." *International Data Privacy Law* 6, no. 2, 77–78.

Carpanelli, Elena & Lazzerini, Nicole. 2019. *Use and misuse of new technologies contemporary challenges in international and European law*. Cham: Springer.

Carpanelli, Elena. & Lazzerini, Nicole. 2017. "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU." *Air and Space Law,* 42: 377–402.

Carrera, Sergio, & Mitsilegas, Valsamis. 2017. *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*. Brussels: Centre for European Policy Studies (CEPS).

Cerrina Feroini Ginevra. 2022. "Luci e ombre della Data Strategy europea" - *Intervento di Ginevra Cerrina Feroni, Vicepresidente del Garante per la protezione dei dati personali.* AgendaDigitale

Chiappetta, Andrea & Battaglia, Andrea. 2018. "The impact of privacy and cybersecurity on e-record: The PNR Directive adoption and the impact of GDPR." *Journal of Sustainable Development of Transport and Logistics*, 3(3), pp. 77-87

CJEU, *Joined Cases C-317/04 and C-318/04.* 2006

CJEU. 2006. *European Parliament v Council of the European Union and Commission of the European Community*. Joined Cases C-317/04 and C-318/04. ECR I-4721.

CJEU. 2014. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Karntner Landesregierung and Others,* Joined Cases C-293/12 and C-594/12, ECR I-238

CJEU. 2015. C-362/14, *Maximillian Schrems v. Data Protection Commissioner.*

CJEU. *European Parliament v Council of the European Union and Commission of the European Community*, Joined Cases C-317/04 and C-318/04, 2006, ECR I-4721.

CJEU. *Joined Cases C-293/12 and C-594/12,* 2014, ECR I-238

CJEU. *Joined Cases C-511, 512 & 520/18, La Quadrature du Net and others*, EU:C:2020:791.

CJEU. *Opinion 1/15 delivered on 26 July 2017*, ECLI:EU:C:2016:656

CJEU. *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Case C-203/15*, 2016.

Commission of the European Communities. 2003. *Communication from the Commission to the Council and the Parliament on the Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach.* COM(2003).

Council of Europe. 1953. *European Convention on Human Rights (ECHR).*

Council of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*

Dalla Corte, Lorenzo. 2022. "On Proportionality in the Data Protection Jurisprudence of the CJEU. *International Data Privacy Law 12*, no. 4: 259–75.

De Terwangne Cécile. 2020. "Article 5. Principles relating to processing of personal data" In *The EU General Data Protection Regulation (GDPR): A Commentary.*

Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC. OJ L 283, 29.10.2010

Docksey, Christopher. 2017. "Opinion 1/15: Privacy and security, finding the balance". *Maastricht Journal of European and Comparative Law 24*, no. 6: 768–73.

Duroy, Sophie. 2023. "Case C-817/19, Ligue Des Droits Humains V. Council of Ministers (C.J.E.U.)." *International Legal Materials*: 1–60.

EDPS. Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data. 30/09/2013, Brussels.

Erdos, David. 2019. "The Development of European Data Protection Law and Regulation." *European Data Protection Regulation, Journalism, and Traditional Publishers*, 35–54.

European Commission, 2017. *Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM(2017).*

European Commission. "Border and Law Enforcement - Advance Passenger Information (API) Revised Rules." *Migration and Home Affairs*.

European Commission. "Passenger Data". *Migration and Home Affairs*. Available at: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/passenger-data_en

European Commission. 2005. Commission Decision of 6 September 2005 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the Canada Border Services Agency. OJ 2005, 29.3.2006. L 91/49.

European Commission. 2010. *Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries. Brussels*, 21.9.2010 COM(2010) 492 final.

European Commission. 2016. *Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. SWD(2016).*

European Commission. 2020. *Commission Staff Working Document accompanying the Commission Report. SWD(2020) 128 final. COM(2020) 305 final*. 24 July 2020. p.28

European Commission. 2020. *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).

European Commission. 2020. *Roadmap 24 July 2020.* Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-Air-travel-sharing-passenger-name-data-within-the-EU-and-beyond-assessment-_en

European Commission.2013 *Proposal for a Council decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*. Brussels, 18.7.2013 COM(2013) 529 final

European Council. 2004. *Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data*.

European Council. 2010. *The Stockholm Programme An open and secure Europe serving and protecting citizens* (2010/C 115/01). OJ C 115.

European Council. 2022. *Improving Compliance with the Judgment in Case C-817/19 – Ideas for Discussion,* 11911/22 https://www.statewatch. org/media/3496/eu-council-pnr-way-forward-discussion-paper-11911-22.pdf, last accessed 20/08/2023.

European Parliament. "Personal Data Protection: Fact Sheets on the European Union". Accessed June 20, 2023. Available at https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection.

European Parliament. "Timeline of the EU-US PNR Agreements". News: European Parliament. 26-03-2012. Last accessed September 7, 2023 at https://www.europarl.europa.eu/news/en/press-room/20120326BKG41893/transfer-of-air-passengers-data-to-the-us-what-s-at-stake/7/timeline-of-the-eu-us-pnr-agreements.

European Parliament. 2010. *Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada,* OJEU C 81E, 15.3.2011

European Parliament. 2014. *Resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the EU on the transfer and processing of PNR data. (*2014/2966(RSP)).

European Parliament. 2015. *Resolution of 11 February 2015 on anti-terrorism measures* (2015/2530(RSP).

European Parliament. 2016 "EU Passenger Name Record (PNR) Directive: An Overview: News: European Parliament.".

European Parliament. *Understanding EU Data Protection Policy*. Accessed June 16, 2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf.

European Union. "Types of Legislation". Accessed June 20, 2023. Available at https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.

European Union. 1995. *Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Data Protection Directive (DPD). OJ L 281.

European Union. 2000. *Charter of Fundamental Rights of the European Union.*

European Union. 2002. *Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector*. E-Privacy Directive. OJ L 201.

European Union. 2004. *Council Decision 2004/496/CE of 17 May 2004 on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security, Bureau of Customs and Border Protection*, OJL 183/84.

European Union. 2004. *Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data*. API Directive. OJL 261.

European Union. 2007. *Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the EU, of an Agreement between the EU and the US on the processing and transfer of PNR data by air carriers to the US Department of Homeland Security.*

European Union. 2007. *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01*

European Union. 2011. *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.

European Union. 2012 *Council Decision 2012/381/EU of 13 Dec. 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record data by air carriers to the Australian Customs and Border Protection Service, OJ 2012 L 186/3.*

European Union. 2012. *Agreement between the United States of America and the European Union on the use and transfer of PNRs to the US Department of Homeland Security*, OJ 2012 L 215/13

European Union. 2016. *Directive (EU) 2016/680 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. OJ L 119, 4.5.2016.* Eu PNR Directive.

European Union. 2016. *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, repealing Directive 95/46/EC.* General Data Protection Regulation (GDPR). OJ L 119.

European Union. 2016. *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, 4.5.2016.*

European Union. 2018. *Communication from the Commission to the European Parliament, the European Council and the Council. Fifteenth Progress Report towards an effective and genuine Security Union*. COM(2018).

European Union. 2020. *Communication from the Commission on the EU Security Union Strategy. Brussels*, 24.7.2020. COM(2020) 605 final

European Union. 2020. *Council of the EU. EU-Japan PNR Agreement: Council authorises opening of negotiations*. Accessed July 1, 2023. https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/.

Evans, A. C. 1981. "European Data Protection Law." *The American Journal of Comparative Law* 29, no. 4: 571-582.

Fahey, Elaine, Elspeth Guild, and Elif Kuskonmaz. 2023. "The Novelty of EU Passenger Name Records (PNR) in EU Trade Agreements: On Shifting Uses of Data Governance in Light of the EU-UK Trade and Cooperation Agreement PNR Provisions." *European Papers.* Last accessed 08/09/2023 at https://www.europeanpapers.eu/en/e-journal/novelty-eu-passenger-name-records-eu-trade-agreements.

Francesco, Rossi dal Pozzo. 2016. *EU legal framework for Safeguarding Air Passenger Rights*. Cham: Springer.

Fuster, Gloria González. 2014. *Emergence of personal data protection as a fundamental right of the EU*. Cham: Springer

Gerace, Diane. 2021. "A Look at How Airport Security Has Evolved Post 9-11." Last accessed 08/09/2023 at https://www.phl.org/newsroom/911-security-impact.

Government of Canada. 1985. *Customs Act R.S.C. C.1 (2nd Supp.)*

Government of Canada. 2001. *Anti-Terrorism Act. SC 2001. C.41*

Government of Canada. 2001. *Immigration and Refugee Protection Act. S.C. C. 27*

Government of Canada. 2021. *Canada Border Services Agency. Memorandum D2-5-11 - Guidelines for commercial air carriers for the processing of prescribed traveller information.*

Government of the United States. 2001. *US Aviation and Transportation Security Act*. 2001.

Graziani, Chiara & Vedaschi, Arianna. 2019. "National Security and Counter-Terrorism in Canada: Past, Present and Future.". *DPCE Online.*

Graziani, Chiara. 2018. "PNR EU-Canada, La Corte Di Giustizia Blocca l'accordo: Tra Difesa Dei Diritti Umani e Implicazioni Istituzionali." DPCE Online. 2018: 959-966.

Guild, Elspeth, and Tamas Molnar. 2023. "The European Legal Architecture on Security: New Developments in the Complex Relationship between the Public and Private Sectors

in Data Processing." Verfassungsblog. Last Accessed 28/08/2023. https://verfassungsblog.de/pnr-architecture/.

Hijmans Hielke. 2020. "Article 51 Supervisory authority". In *The EU General Data Protection Regulation (GDPR): A Commentary the EU General Data Protection Regulation (GDPR): A Commentary*.

Hobbing, Peter. 2008. "Tracing Terrorists: The EU-Canada Agreement" in *PNR Matters*. CEPS Special Report/September.

House of Commons. 2013. *Documents considered by the Committee on 4 September 2013 - European Scrutiny Committee.*

Hudobnik, Matthias M. 2020. "Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?" *ERA Forum* 21, no. 3: 485–500.

Hustinx, Peter. 2017 "EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation." *Oxford Scholarship Online*.

Irion, Kristina. 2022. "Repairing the EU Passenger Name Record Directive: The ECJ's Judgment in Ligue Des Droits Humains (Case C-817/19)." *European Law Blog*.

Karjalainen, Tuulia. 2022. "All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm." *European Data Protection Law Review* 8, no. 1: 19–30.

Kolliarakis, Georgios. 2017. *In quest of reflexivity. Towards an anticipatory governance regime for security*. In: M. Friedewald, et al. edits. Surveillance, privacy and security. Citizens' perspectives. Abingdon: Routledge, pp. 233-254

Korff, Douwe. 2021. "Opinion on the Broader and Core Issues Arising in the PNR Case Currently before the CJEU (Case C-817/19)." SSRN

Korff, Douwe. 2022. "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*.

Krahulcova, Estelle Massé, Lucie. 2016. "The Stormy Seas of Privacy in Europe." Access Now. April 14. https://www.accessnow.org/stormy-seas-privacy-europe/. Accessed 3 July 2023.

Kranenborg, Herke. 2008. "Access to documents and data protection in the European Union: On the public nature of personal data". 2008., 45, *Common Market Law Review*, Issue 4, pp. 1079-1114.

Kranenborg, Herke. 2022. "Article 8 – Protection of Personal Data." *The EU Charter of Fundamental Rights*, 231–290.

Křepelka, Filip. 2021. "Transformations of Directives into Regulations: Towards a More Uniform Administrative Law?". European Public Law 27 (Issue 4): 781–806.

Kuner, Christopher. 2017. *Data protection, data transfers, and international agreements: The CJEU's Opinion 1/15.* Available at https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/

Kuner, Christopher. 2018. "International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR." *Common Market Law Review*, 55(3), pp. 857-882

Kuşkonmaz, Elif Mendos. 2023. "The Grand Gala of PNR Litigations: Case C-817/19,Ligue Des Droits Humains v Conseil Des Ministers." *European Constitutional Law Review* 19, no. 2: 294–319.

Lazzerini, Nicole, and Elena Carpanelli. 2017. "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum after Opinion 1/15 of the CJEU." Air and Space Law 42 (Issue 4/5),: 377–402.

Lenaerts, Koen, and Marlies Desomer. 2005. "Towards a Hierarchy of Legal Acts in the European Union? Simplification of Legal Instruments and Procedures." *European Law Journal* 11, no. 6,: 744–65.

Louks, Douglas. 2013. "(Fly) Anywhere but Here: Approaching EU-US Dialogue Concerning PNR in the Era of Lisbon." *Indiana International & Comparative Law Review* 23, no. 3 (2013): 479–522.

Lowe, David. 2017. The European Union's Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?. *International Criminal Law Review*. 17: 78-106. p. 83

Lund, Jesper. 2022. "Mass Surveillance of External Travellers May Go on, Says EU's Highest Court." *European Digital Rights (EDRi).* Last accessed 01/09/2023 at https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/.

Mendez, Mario. 2017. "Opinion 1/15: The Court of Justice Meets PNR Data (Again!)". *European Papers, Vol. 2, No 3*: 803-818.

Mitsilegas, Valsamis. 2017. *The security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law*. In: S. Carrera & V. Mitsilegas, edits. *Constitutionalising the security Union. Effectiveness, rule of law and rights in countering terrorism and crime*. Brussels: CEPS, pp. 5-20

Nardone, Valentina. 2019. "The Passenger Name Record Case: Profiling Privacy and Data Protection Issues in Light of CJEU's Opinion 1/15." In *Use and Misuse of New Technologies*, 135–50.

Nesterova, Irena. 2019. "The Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security." *How International Law Works in Times of Crisis*, 2019, 109–26.

Obendiek, Anke Sophia. 2023. "Passenger Data in Air Travel Establishing Data as a Security 'Tool.'" Essay. In *Data Governance: Value Orders and Jurisdictional Conflicts.* Oxford, United Kingdom: Oxford University Press.

OECD. 1980. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

Olsen, Henrik Palmer, and Cornelius Wiesener. 2021. "Beyond Data Protection Concerns – the European Passenger Name Record System." *Law, Innovation and Technology*. 13, no. 2: 398–421.

Opinion of Advocate General Pitruzzella delivered on 27 January 2022, Ligue des droits humains, C-817/19.

Orrù, Elisa. 2022. 'The European PNR Directive as an Instance of Pre-emptive, Risk-based Algorithmic Security and Its Implications for the Regulatory Framework': 131 – 146.

Pfisterer, Valentin M. 2019. "The right to privacy a fundamental right in search of its identity: uncovering the CJEU's flawed concept of the right to privacy." *German Law Journal*, 20(5), 722-733.

Propp, Kenneth. 2021. "Avoiding the next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data." *Atlantic Council.*

Propp, Kenneth. 2022. "Why Sharing Passenger Data Doesn't Fly for the EU's Top Court." Atlantic Council. Last accessed 05/08/2023 at https://www.atlanticcouncil.org/blogs/new-atlanticist/why-sharing-passenger-data-doesnt-fly-for-the-eus-top-court/.

Rossi Dal Pozzo, Francesco. 2015. *EU Legal Framework for Safeguarding Air Passenger Rights*, Springer International Publishing Switzerland

Santos, Juan. 2014. "The Role of the European Parliament in the Conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon."

Tambou, Olivia. 2018. "Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights." *European Foreign Affairs Review 23, no. Issue 2*: 187–202.

Thönnes, Christian, and Niovi Vavoula. 2023. "Automated Predictive Threat Detection after Ligue Des Droits Humains: Implications for Etias and CSAM (Part I)." *Verfassungsblog*.

Thönnes, Christian. 2022. *A cautious green light for technology-driven mass surveillance: The Advocate General's Opinion on the PNR Directive*. Verfassungsblog. Available at https://verfassungsblog.de/green-light/.

Thönnes, Christian. 2022. *A Directive altered beyond recognition: On the Court of Justice of the European Union's PNR decision (C-817/19*). Verfassungsblog. Available at https://verfassungsblog.de/pnr-recognition/

Tosoni, Luca and Lee A. Bygrave. 2020. "Article 4(1). Personal data." In *The EU General Data Protection Regulation (GDPR): A Commentary the EU General Data Protection Regulation (GDPR): A Commentary*.

Tzanou, Maria. 2013. “Data Protection as a Fundamental Right next to Privacy? ‘Reconstructing’ a Not so New Right.” *International Data Privacy Law* 3, no. 2: 88–99.

Tzanou, Maria. 2019. *The fundamental right to data protection: Normative Value in the context of counter-terrorism surveillance*. Oxford: Hart.

UN Security Council. 2017. *Resolution 2396.*

United Nations General Assembly. 1948. *The Universal Declaration of Human Rights (UDHR).*

Vagelis Papakonstantinou, and Paul De Hert. 2009. “The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic.” *Common Market Law Review* 46 (Issue 3): 885–919.

Van Wasshnova, Matthew R. 2008. “Data Protection Conflicts between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange.” *Case Western Reserve Journal of International Law* 39 (3): 827-865.

Vedaschi, Aranna. 2018. “The European Court of Justice on the EU-Canada Passenger Name Record Agreement.” *European Constitutional Law Review 14*, no. 2: 410–29.

Vedaschi, Arianna, and Lubello, Valerio. 2015. “Data Retention and Its Implications for the Fundamental Right to Privacy.” *Tilburg Law Review 20, no. 1*: 14–34.

Vedaschi, Arianna. & Graziani, Chiara. 2018. *PNR agreements between fundamental rights and national security: Opinion 1/15*. Available at: http://europeanlawblog.eu/2018/01/23/pnr-agreementsbetween-fundamental-rights-and-national-security-opinion-115/

Vedaschi, Arianna. 2018. “Privacy and data protection versus National Security in Transnational Flights: The EU–canada PNR agreement.” *International Data Privacy Law, 8*(2), 124-139.

Vedaschi, Arianna., 2019. *Privacy versus security: Regulating data collection and retention in Europe*. In: B. Goold & L. Lazarus, edits. Security and human rights. 2nd edition. Oxford: Hart Publishing, pp. 275-296

Villani, Susanna., 2018. “Some further reflections on the Directive (EU) 2016/681 on PNR data in the light of the CJEU Opinion 1/15 of 26 July 2017”. *Revista de Derecho Político*, 1(101), pp. 899- 928

WCO/IATA/ICAO. 2022. *Guidelines on Advance Passenger Information (API).*

Weiss, Martin, and Kristin Archick. 2016. “U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield.” *Congressional Research Service*.

Weizman, Eyal. 2020. “The Algorithm Is Watching You.” LRB Blog, February 19, 2020. Last accessed 29/08/2023 at https://www.lrb.co.uk/blog/2020/february/the-algorithm-is-watching-you.

Wilson, Kerianne M. 2016. “Gone With the Wind?: The Inherent Conflict between API/PNR and Privacy Rights in an Increasingly Security-Conscious World.” *Air And Space Law* 41, no. Issue 3. 229–64.

Zalnieriute, Monika. 2018. “Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement.” *The Modern Law Review* 81, no. 6: 1046–63.

Zanfir, Gabriela. 2016. “Analysis of the AG Opinion in the ‘PNR Canada’ Case: Unlocking an ‘Unprecedented and Delicate’ Matter”. Available at https://pdpecho.com/2016/09/12/analysis-of-the-ag-opinion-in-the-pnr-canada-case-unlocking-an-unprecedented-and-delicate-matter/ (last accessed 29/07/2023).