THE PNR DIRECTIVE: AN ESSENTIAL SECURITY MECHANISM FOR THE EU OR A TOOL FOR THE BREACH OF PERSONAL DATA AND THE PRIVATE LIFE OF INDIVIDUALS?*

Mariam Pilishvili[1]

The validity of the Passenger Name Record Directive in relation to the Charter of the Fundamental Rights of the European Union has been repeatedly questioned. The subject of the criticism is the establishment of national databases including the personal data of every passenger entering or departing the European Union and enabling member states to keep data on anyone moving around the EU. The data includes private information on persons' airline tickets, the passengers they are traveling with, coordinates of the destination, personal credit card information, and many other things. Most of the society thinks that there is a high probability of the abuse and improper use of PNR's proposed database which on the one hand makes the right to privacy at great stake due to indiscriminate and excessive storing of large volumes of passengers' personal information, and on the other hand, it could lead to personal damages varying from fraudulent use of credit cards to governmental surveillance. Hence, in this paper, we will highlight and analyze the interplay between personal data protection and the Passenger Name Record Directive (PNR Directive), which caused an altercation in terms of data collection and preservation. In this regard, we intend to examine the case law of the Court of Justice of the European Union, namely the judgment in the case C-817/19 Ligue des droits humains.

Keywords
PNR Directive, Mass Surveillance, Personal Data Protection, Protection of Private Life, CJEU practice

1. Introduction

Since terrorism began to transcend national boundaries and take place on an international level, the global world has encountered the complex challenges of international security. The need for coordinated anti-terrorist actions is more necessary in the 21st century than ever. Without international cooperation, it is impossible to battle terrorism, and it is crucial that all international organizations and states participate, as the threat outlined affects the entire civilized world. The enormous role of the European Union in this regard is worth mentioning.

The US advocated for tougher regulation of public air travel in the wake of Al Qaeda's attack on the US on September 11, 2001 (9/11), in which terrorists affiliated with Al Qaeda hijacked commercial aircraft and crashed them into the World Trade Center in New York and the Pentagon in Washington. This event was instrumental to

* DOI 10.21868/PGnG.2024.1.5.
[1]*Mariam Pilishvili*, PhD student, Marton Géza Doctoral School of Legal Studies, University of Debrecen

the US passing legislation on documenting passenger name record (hereinafter PNR) data containing information about airline passengers, which was required by law under the US Aviation and Transport Security Act of 2001. The Act mandated that aviation businesses that operate passenger flights to, from, or through the US give US authorities electronic access to PNR data, which includes passenger names and addresses, bank and credit card information, and details about any onboard meal orders (Kaunert et al. 2012). Notably, the UK also started implementing defensive mechanisms against terrorism and adopted the e-Border initiative in 2003, which, following a pilot program that ran from 2004 to 2006, introduced an intelligence-led approach to border restrictions (Commons Committee 2016). Beginning in October 2005, the test program involved processing PNR data on several carefully filtered routes (HL Paper 2008, 22).

The EU's primary priority has always been combating terrorism. In order to stop terrorist acts and protect citizen security, EU member states collaborate closely. Over time, the European Union faced several challenges in the fight against terrorism. According to Europol's annual EU terrorism situation and trend reports from 2011 to 2021, the European Union has repeatedly become the target of jihadist / religiously inspired, right-wing, left-wing and anarchist, ethno-nationalist and separatist, other and non-specified groups (Europol 2022, 8-11). In the EU member states in 2021, there were 15 terrorist attacks. Due to a sharp decline in the number of incidents classified as left-wing terrorism, the overall number of attacks in 2021 was significantly fewer than in previous years. 29 jihadist or extreme right-wing plots were thwarted in the EU between 2019 and 2021. Attacks occurred most frequently in France, Germany, and Sweden. Most recorded terrorist assaults were classified as acts of jihadist terrorism of which three were successful attacks carried out in France, Spain, and Germany while eight were successfully prevented (Europol 2022, 8-11).

The European Union has implemented several measures to fight terrorism, including the joint statement of the European Leaders in 2015 which requested to direct the work of the EU and its member states. It urged actions in three major categories (European Council, Policies 2022):

I. Ensuring the security of citizens
II. Preventing radicalization and safeguarding values
III. Cooperating with international partners

Following the terrorist attacks in Brussels, EU ministers in charge of justice and home affairs as well as representatives of EU institutions met. They agreed upon a united statement that demanded the European Parliament's urgent adoption of the Passenger Name Record Directive (Joint Statement 2016). A directive on the use of PNR data for the investigation, prosecution, and prevention of severe crimes and acts of terrorism was approved by the Council on April 21, 2016 (PNR Directive 2016). The directive intends to monitor how PNR information about passengers on international flights is transferred by airlines to member states and processed by the appropriate authorities. According to the instruction, PNR information can only be used to prevent, identify, investigate, and prosecute major crimes and terrorist offenses (Press Release 2016).

Under the recently introduced directive, air carriers were requested to submit to member states' authorities the PNR information for flights coming into or going out from the EU. Additionally, it also permitted but did not oblige member states to gather PNR data on specific intra-EU flights (Article 2, PNR Directive). Additionally, each member state was required to establish a "Passenger Information Unit" which is in charge to receive information from the airlines (Article 4(1), PNR Directive). Consequently, it is the second article of the directive that we should analyze in our paper, which represented a major problem, and which has given rise to a number of critical views among lawyers and laymen alike.

2. The Framework of the Study

2.1. Theoretical Context

As mandayed by the PNR Directive, for the purposes of preventing serious crimes and terrorism the PNR data must be processed. According to the Article 2 of that Directive Member States are eligible of applying the Directive to intra-EU flights. The incroporation of Directive in Belgium has been challenged by the Ligue des droits humains (LDH) in 2017 (C-817/19 2022), citing violations of privacy rights and the protection of personal data under Belgian and EU law. LDH further questioned the directive's impact on freedom of movement, claiming it indirectly reintroduced border restrictions within EU by expanding the PNR system.

Therefore, the focus of our research will be on analyzing important issues of the abovementioned case and whether the nature of the PNR Directive violates the personal data and private life guaranteed and protected under the Charter of Fundamental Rights of the European Union (hereinafter EU Charter) and General Data Protection Regulation.

2.2. Legal Context

During our research, we will use document analysis, case studies, and social research methodologies to obtain as much knowledge as possible. By employing the document analysis method, we will be able to thoroughly examine the texts of law and articles in order to fully acknowledge the interplay between the fight against terrorism and the personal data protection of the passengers. We will analyze key issues from the judgment of the Court of Justice of the European Union (hereinafter CJEU) in case C-817/19 and outline the outcome of the court's ruling on the protection of personal data. By employing social research methods, we will be able to assess the opinion of the European Union Agency for Fundamental Rights (hereinafter FRA) which conducted research and together with the non-discriminate nature of the PNR Directive analyzed the importance of the general interest of the EU over limitations of fundamental rights.

2.3. Social Context

The social context that can be associated with our paper is the importance of protecting the personal data and privacy of each passenger as much as possible. Considering that in

the 21st century, an age of innovation, where it is quite easy to misuse information, identity theft and commit crimes with the help of the Internet, personal data should be collected, stored, and processed with increasing precision and accuracy, including by government agencies. In addition, it is necessary to consider from the social point of view that, while fighting a crime infringing on a certain right, the so-called golden ratio of another right must be preserved.

3. Data and Information

3.1. Historical Overview of the PNR Directive

The PNR Directive has been adopted by the European Parliament, and the Council in April 2016. It is scheduled to be adopted into national legislation in Member States by May 25, 2018 (Article 18(1), PNR Directive). The Directive's primary goal is to prevent, identify, investigate, and prosecute terrorism and serious crime by granting pertinent agencies access to PNR data pertaining to air travel (Article 18(1) para 2, PNR Directive). This is the EU's second attempt to enact a PNR data directive after their first attempt in 2011 was unsuccessful due to a lack of adequate protection for an individual's data privacy (European Commission, 32 final, 2011).

The deficiency of personal data protection, particularly in connection to the transfer of PNR data to third countries, was the fundamental issue with the 2011 PNR Data Directive. The security measures were found to be unsatisfactory in safeguarding personal data, even though the European Commission's (hereinafter Commission) assertion that the 2011 proposal had undergone a thorough examination to ensure that its provisions were consistent with fundamental rights, particularly Article 8 of the EU Charter on data protection.

The Article 29 Data Protection Working Party[2] has continually questioned the necessity and proportionality of PNR systems, and its 2011 proposal was no exception. From the viewpoint of the Working Party, the impact assessment, which accompanied the proposal, does not adequately evaluate the use of PNR and does not support the necessity of the proposal. The plan should make it clear whether the goal is to combat serious (transnational) crime, which includes terrorism, or merely offenses related to terrorism (Opinion 10/2011, 2). The Fundamental Rights Check List has been utilized, but that is all that is stated in Chapter 3.2 of the impact assessment titled "Respect for fundamental rights" – there is no other information to support this impact assessment's findings. Additionally, this chapter offers a circular justification for the infringement of private rights protected by Articles 8 of the European Convention on Human Rights (hereinafter ECHR) and Articles 7 and 8 of the EU Charter (Opinion 10/2011, 3). They have also stated that the strategy does not clearly meet these conditions only because its goal is to prevent major crime and terrorism; the necessity and proportionality still need to be established (Opinion 10/2011, 3).

[2] As per Article 29 of the Data Protection Directive 95/46/EC, the Article 29 Working Party constituted as an advisory body consisted of the data protection authorities of EU member states, the European Data Protection Supervisor, and the European Commission, providing professional guidance and opinions related to data protection in EU.

Member of European Parliament Timothy Kirkhope presented a new version of the text on a PNR data collection system for the European Union, which was discussed on February 26, 2015, in the European Parliament's Civil Liberties, Justice, and Home Affairs Committee (LIBE) (Bakowski, Voronova 2015). The draft text's introduction addresses topics raised by Members of the European Parliaments, such as an assessment of the proposal's necessity and proportionality in light of current security threats, its scope, retention periods, inclusion or exclusion of flights within the EU, and its relationship to the ongoing data protection reform. The European authorities' rapid efforts to introduce the 2015 PNR Directive proposal were motivated by the January and November 2015 terrorist attacks in Paris (Bakowski, Voronova 2015, 1).

The PNR Directive proposal was rapidly endorsed by the Council of the European Union on December 4th, 2015, after approval by the LIBE committee and the plenary session of the European Parliament at the beginning of 2016 (Lowe 2017, 22). As a result, on April 27, 2016, the PNR data Directive 2016/681 came into effect, allowing the transmission of PNR data between Member States and third-party nations.

3.2. The ruling of the CJEU

In this part, we will assess issues relating to the PNR Directive's validity and the Law of 25 December 2016's compliance with EU law based on the questions that the Belgian Constitutional Court sent to the Court for a preliminary ruling in October 2019.

The PNR Directive's provisions allowing for the processing of PNR data by competent Member State authorities were found to be compliant with the EU Charter by the Court of Justice of the European Union (hereinafter CJEU or Court) on June 21, 2022. According to the Court, the PNR Directive "entails undeniably serious interferences" of the rights protected by Articles 7 and 8 of the EU Charter, as it aims to establish a monitoring regime that is permanent, untargeted, and systematic, including the automatic evaluation of each user's personal information (C-817/19 2022, para 111). However, the Court outlined the non-absolute character of the abovementioned articles (C-817/19 2022, para 112) while declaring that, in terms of justifying the interference of the Member States, any limitation of the rights contained therein must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest is proportionate to that seriousness (C-817/19 2022, para 113-115).

Based on the judgment, only clearly identifiable and delimited information must be covered by the system established under the PNR Directive (C-817/19 2022, para 129). Along with this, the use of the system must be limited to terrorist offenses and serious crimes that have an objective connection, even if only indirectly, with the carriage of passengers by air (C-817/19 2022, para 251). Additionally, the Court stated that the possibility of extension of the application of the PNR Directive to selected or all intra-EU flights, which is up to the decision of Member States according to Article 2 of the Directive, should be limited to strictly necessary cases (C-817/19 2022, para 168). Regarding this issue, the Court noted that except in the specific circumstances when a Member State is faced with a terrorist threat that is demonstrated to be *genuine, present, or foreseeable*, PNR data cannot be gathered generally and indiscriminately for an intra-EU flight. Furthermore, only targeted PNR data collection is allowed for flights within

the EU in the absence of such a threat. Given the inherent risks of terrorism and severe crime that may result from the transportation of passengers between a third country and the EU, the Court determines that the collection of PNR data cannot be restricted to a specific category of passengers on extra-EU flights (C-817/19 2022, para 171-175).

Advocate General (AG) Pitruzzella of the CJEU issued his opinion on the matter on January 27, 2022 (Opinion of AG C-817/19 2022, para 287(2)). Specifically, he criticized the use of the category "General remarks" as an umbrella term for PNR data to be collected by airlines in point 12 of Annex I of the Directive, stating that this definition *"did not satisfy the conditions of clarity and precision"* required by the EU Charter. In the AG's opinion, other aspects of the Directive have also been criticized as being incompatible with the human rights framework of Articles 7 and 8 of the EU Charter. Additionally, the AG determined that the five-year retention time frame for all PNR data exceeded *"what is strictly necessary"* and that the preservation time is *"justified only where there is a serious threat to the security of the Member States" (*Opinion of AG C-817/19 2022, para 287(8)). The generalized retention of all PNR data was declared to be incompatible with the EU Charter, but a more significant result of this opinion was that the *"generalized and indiscriminate transfer of the PNR data is compatible with Articles 7 and 8 of the Charter" (*Opinion of AG C-817/19 2022, para 287(8)). Many have criticized the "indiscriminate" collection of personal data under the PNR Directive, such as scholar Christian Thönnes, who reacted to the AG's opinion by declaring it *"a cautious green light for technology-driven mass surveillance"* and subsequently argued for the Directive's invalidation (Thönnes 2022).

The CJEU agreed with the AG's above opinion, clarifying that PNR data outlined in Annex I has to be restricted to *"clearly identifiable and circumscribed information"* and asserting that the storage of all air passengers' PNR data after the initial six-month retention period goes beyond *"what is strictly necessary"* (Press Release No. 105/22 2022) In addition to prohibiting AI-based automated processing of PNR data and stating that the application of the PNR Directive to flights within the EU must be restricted to situations in which a Member-State is facing a "genuine and present or foreseeable" terrorist threat, the CJEU expanded its review of the Directive beyond the issues raised by the AG (Press Release No. 105/22 2022).

Consequently, in a major decision issued on June 21, 2022, the CJEU, sitting in for the Grand Chamber, maintained the EU's policy of collecting and using traveler records as long as it is strictly construed in accordance with the fundamental rights of the EU. And in circumstances of flights conducted only within the EU, indiscriminate data processing is prohibited unless there is a threat from terrorism. In terms of time, unless a link to terrorism or a significant crime has been proven, the data on the passengers must likewise be removed after six months at the latest.

4. Discussion

The Ligue des droits humains' attorney Catherine Forget told EU observer that the decision was a "victory" and undoubtedly called into question Belgium's law (Rettman 2022).

Estelle Massé, Europe Legislative Manager at Access Now, outlined that *"Considering the impact that the EU PNR Directive has on fundamental rights — as confirmed by the Court — the law should have been invalidated"* (Surveillance Scheme 2022).

From the viewpoint of Douwe Korff, emeritus professor of international law at the London Metropolitan University, the Court has put various complicated and challenging criteria and restrictions on the use of PNR data, particularly on the mining of the data to develop profiling, despite not completely disregarding the regulation. Korff asserted that "rather than expanding generalized data trawling and mining and profiling, as the EU wants to do through Europol, these invasive measures should be dropped," observing the decision as having greater implications for future EU law (Bertuzzi 2022).

According to the advocacy group European Digital Rights (EDRi), the Court placed an excessive amount of trust in the Member States to apply the PNR Directive in a limited manner to comply with the Charter obligations on a few important clauses. While the Directive does not sufficiently address the risks of misuse by investigating authorities and the use of PNR data for routine crime, the Court, for instance, relies on Member States to limit the use of the PNR surveillance system in the fight against terrorism and serious crime (EDRi 2022).

First, it should be noted that the approach that the Court took in its judgment marks a significant divergence from its earlier decisions on the Data Retention Directive in April 2014 (EDRi 2014) and the EU-Canada PNR agreement in July 2017 (EDRi 2017), both of which were declared unlawful due to the crucial EU Charter violations. The Court took a more permissible view in terms of the general and indiscriminate collection and preservation of personal data that is very invasive to the private lives of the persons.

A positive implication from the judgment is that the PNR data for an intra-EU flight cannot be collected indiscriminately except in the case of a terrorist threat. However, in terms of extra-EU flights, the data must be collected due to the high probability of threats from terrorism and serious crimes that may stem from the carriage of passengers between third countries and the European Union. Unfortunately, this approach is just the blanket acceptance of the broad nature of the PNR Directive that *"everyone is suspect until proven otherwise."*

It's obvious that the judgment really caused a difference of opinion in society. It is regrettable that even in terms of the relevant databases, the directive does not satisfy the criteria of clarity and precision which is a critical element for cross-checking. A similar situation is regarding the automated analysis of the PNR data, where the Court noted that the automated analysis presents some margin of error (C-817/19 2022, para 106) and that the appropriateness of the system depends on the subsequent manual verification (C-817/19 2022, para 124). The Court itself noted that five out of six individuals were incorrectly identified during the automated analysis of PNR data, according to the Commission's Working Document (C-817/19 2022, para 106). This should be substantial evidence that the automated analysis employed does not pass the necessity test for the purpose of preventing severe crime and terrorism. Hence, the Court does not even consider factors like the potential for creating precise standards for automated analysis. This is unfortunate, considering how confirmation bias and the "presumption to intervene" affect decision-making in the context of policing that is supported by technology, which was neglected by the Court.

According to the AG, the PNR Directive is consistent with the EU Charter. Even though the legal analysis closely follows the EU-Canada PNR Agreement, AG's opinion comes to a significantly different conclusion (Opinion of AG C-817/19 2022). This approach of the AG is disappointing for civil society organizations wishing for the PNR Directive to be invalidated, but it is not unexpected given that the AG Opinion points out the same flaws in the PNR Directive that the CJEU found to be the reason the EU-Canada PNR agreement was invalidated in 2017 (EDRi Resources 2022). A major letdown is the AG opinion's relatively scant focus on profiling all passengers through automated analysis of their PNR data, which could be the result of closely monitoring the EU-Canada PNR case, where the CJEU likewise did not raise an objection to the automated analysis under specific safeguards (EDRi Resources 2022). Therefore, it might have seemed more rational just to declare the PNR Directive invalid, as the CJEU did in its 2014 decision regarding the Data Retention Directive, given that the Advocate General's comprehension of the Directive clearly contradicts the intent of the EU legislature in at least one crucial area (generalized retention). The Commission would then have been able to submit a new PNR directive that complied with the EU Charter using the CJEU's guidelines.

5. FRA Opinion 1/2011

An expert opinion on the fundamental rights compliance of a proposal for a directive on the use of Passenger Name Record data for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crime was provided by the FRA at the request of the European Parliament. This was a request in response to the FRA's PNR-related opinion from October 2008 (COM(2011) 32 final 2011).

According to Article 294 of the Treaty on the Functioning of the European Union, the Commission's proposal for a PNR directive is subject to the ordinary legislative procedure (co-decision procedure with the European Parliament), and it could have an impact on a number of fundamental rights, including non-discrimination (Articles 21 of the EU Charter, 14 of the ECHR), and Article 1 of Protocol No. 12 to the ECHR); respect for private and family life (Articles 7 of the EU Charter and Article 8 of the ECHR); and protection of personal data [Article 8 of the EU Charter and Article 8 of the ECHR as interpreted by the European Court of Human Rights (hereinafter ECtHR)] (COM(2011) 32 final 2011, 5). The FRA concentrated on two more general fundamental rights issues (requirements for limitations of fundamental rights and effective supervision), which call for a more in-depth examination of this situation, as well as one specific fundamental right (non-discrimination), which is not specifically addressed in the Impact Assessment of the Commission services (COM(2011) 32 final 2011, 6).

It is essential to note that the FRA had expressed concerns about the potential for discriminatory profiling in the context of an EU PNR system in its prior opinion from October 2008. However, the new wording of the PNR Directive, which put an emphasis on the non-discriminatory manner of the assessment of passenger data, excluding from the assessment circumstances based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life, effectively reduces the risks of discriminatory profiling (COM(2011) 32 final 2011, 7).

Regardless of this, in terms of the PNR data sent by air carriers, there may still be a chance of direct discrimination. Under the heading "general remarks," which is a broad category that may include sensitive personal traits like dietary needs, they may include sensitive or special information. The air carrier may continue to transmit this kind of sensitive or special data if insufficient safeguards are in place to regulate its transmission to the Passenger Information Unit, even though the Passenger Information Unit can be expected to delete such information immediately as specified in the proposal (COM(2011) 32 final 2011, 8).

Regarding the second important topic, the FRA discussed Article 52 of the EU Charter in relation to the case law of the ECtHR. First, we should outline that, according to this Article, any restriction on the use of one's rights and freedoms must legitimately serve "objectives of general interest recognized by the Union". The FRA stated that the ECtHR's case law has established that preventing, detecting, investigating, and prosecuting terrorist offenses and serious crimes are justifiable goals. Specifically, national security and crime prevention are listed as valid goals under Article 8(2) ECHR for the restriction of the right to respect for private and family life.

The FRA outlined the case of *Klass and Others v. Germany*, where the ECtHR affirmed that the battle against terrorism and the fight against crime were justifiable goals (COM(2011) 32 final 2011, 11). In that case, the ECtHR explained that because highly sophisticated espionage and terrorism now threaten democratic societies, the State must be able to conduct surveillance of subversive elements operating within its borders in order to effectively counter these threats. Therefore, the ECtHR has acknowledged that, in exceptional circumstances, the existence of some legislation giving powers of surveillance is indispensable in a democratic society for the sake of national security and/or for the prevention of disruption or crime (COM(2011) 32 final 2011, 11). The FRA also brought up the example of the *Leander v. Sweden* case, where the ECtHR ruled that the clandestine gathering of personal data on a person for national security purposes furthers a justifiable goal (COM(2011) 32 final 2011, 11).

Hence, we can state that, in accordance with Article 52 of the EU Charter, measures adopted for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crimes are also appropriate in order to safeguard the rights and freedoms of others because they may pose threats to other fundamental rights, including the right to life, the right to physical integrity, or the right to protection from treatment that violates the prohibition against torture and other cruel, inhumane, or degrading treatment.

6. Conclusion

> *"Combating the rise of global terrorism has led airlines to collect passenger information and deliver it to the receiving country. These [new] EU regulations are just the beginning of data processing, delivery, and security of information required by EU member states and other countries."*
>
> Adam Mottram (Collins 2018)

The environment of the 21st century is more than friendly for innovation. The speed of technological growth is reaching the highest level. Technological advancement has facilitated the easy sharing of personal information. Personal data is fundamental to

both our businesses and daily lives. When it comes to volume, an astounding variety of devices are currently used to generate and share data on a global scale. Along with digital progress, it has become necessary to update personal data protection legislation and adapt it to new challenges. As we become more technologically empowered, our personal data becomes more at risk. Therefore, all proposed laws or directives need to be considered with the utmost care and properly adapted to practice or to prevent possible crimes in order not to create a threat to the protection of personal data.

The network of connections that link "smart things" to the World Wide Web has evolved from being limited to computer screens to include other items and intangible sensors. The Internet of Things ("IoT")[3] is the system that connects the offline and online worlds. The IoT presents substantial privacy, security, and data protection difficulties, which has necessitated a closer examination of how the legislative framework of the European Union is applied in the IoT environment. In addition to IoT, the general concept of technologies has regularly been subject to intense criticism for being tools for "destroying privacy" (Froomkin 2000, 1461-1465). In other words, those platforms and technological advancements are pushing us to zero private environments, which definitely will be a return to the era of "Big Brother".[4] Since obtaining a large amount of data through various and dispersed sources has significantly expanded, it is even more essential and vital to assess public awareness of the security of their personal data.

Utilizing biometric data has evident value and tangible advantages, which are increasingly understood in a variety of contexts, such as resolving cross-border issues, law enforcement and intelligence storing and preserving, border control, evidence, and forensics. However, assessments on the use of biometric data regarding personal data protection rights and the right to private life, analyses of the technology, and recommendations on its use are still inadequate, despite the technology's quick progress and broad application. Hence, the foremost aim should be the logical and relevant collection, processing, and retaining of personal data that falls under data protection legislation.

An essential aim of the PNR Directive is to improve the capacity of organizations and governmental agencies in combating terrorist attacks and track the personal data of passengers linked to terrorism. Although it is crucial for the European Union and its Member States to guarantee that the requirements of national security are tackled, it is also crucial that fundamental rights and freedoms are respected and maintained. Each is not exclusive of the other. In terms of PNR data, it's critical to preserve personal information while also striking a balance among both aspects since maintaining security is equivalent to maintaining a citizen's personal data protection and right to private life.

However, maintaining a balance between combating terrorism and protecting personal data is a complex challenge for any society, including the European Union. Finding the right balance between combating terrorism and protecting personal data requires ongoing dialogue, cooperation, and a commitment to upholding fundamental

[3] *"The Internet of Things (IoT) describes the network of physical objects — "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet."* ORACLE. What is IoT? https://www.oracle.com/internet-of-things/what-is-iot/, [08.04.2023].

[4] Fictional character from "1984, by George Orwell", who controls every aspect of people's lives.

rights. It is essential to constantly review and adapt the measures in place to ensure they align with evolving threats, technological advancements, and changing societal expectations regarding privacy and security. Hence, we do really suggest developing regular evaluations and reviews for the efficiency of the PNR Directive. Conducting periodic evaluations of the PNR system to assess its effectiveness, efficiency, and compliance with privacy and data protection standards, which will include evaluating the necessity and proportionality of data collection and retention periods will be the successful solution and outcome of this harsh debate.

All in all, it is important to outline that even though the PNR directive was found compatible with the EU Charter, we must outline the positive implications of the judgment itself: it is essential that PNR data cannot be collected on intra-EU flights, which will protect the personal data of the passengers and the private life of the persons concerned.

References

- Bakowski, P. & Voronova, S. (2015). The Proposed EU Passenger Name Record (PNR) Directive: Revived in the New Security Context. *European Parliamentiary Research Service* https://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf [accessed Februar 27, 2024]
- Bertuzzi, L. (2022). EU Court Limits Air Travel Surveillance to the 'Strictly Necessary. *Euractive* https://www.euractiv.com/section/data-protection/news/eu-court-limits-air-travel-surveillance-to-the-strictly-necessary/ [accessed March 12, 2024]
- Collins Aerospace (2018). Airports and Airlines Introduce Changes for GDPR and PNR Compliance. https://www.airport-technology.com/contractors/consult/arinc-airports/pressreleases/airports-airlines-gdpr-pnr-compliance/ [accessed March 10, 2024]
- Kaunert, C. & Leonard, S. & McKenzie, A. (2012). The Social Construction of an EU Interest in Counter-Terrorism: US Influence and Internal Struggles in the Cases of PNR and SWIFT. *European Security* 21(4): 474–496.
- Lowe, D. (2017). The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose? *International Criminal Law Review* 17(1): 78–106
- Rettman, A. (2022). Court Casts Doubt on EU's Flight-Data Regime. *Euobserver*. https://euobserver.com/rule-of-law/155293 [accessed March 5, 2024]
- Thönnes, C. (2022). A Cautious Green Light for Technology-Driven Mass Surveillance: The Advocate General's Opinion on the PNR Directive. *Verfassungsblog* https://verfassungsblog.de/green-light/ [accessed March 10, 2024]

- Article 29 Data Protection Working Party (2011). Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the

use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. 00664/11/EN, WP 181. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation//2011/wp181_en.pdf [accessed March 8, 2024]

- Court of Justice of the European Union. Judgment of the Court in Case C-817/19. https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105en.pdf [accessed March 7, 2024]
- Advocate General's Opinion in Case C-817/19. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62019CC0817 [accessed March 10, 2024]
- 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 offenses and serious crime, OJ L 119, 4.5.2016, p. 132–149.
- EDRi (2022). CJEU Advocate General states that PNR Directive does not violate fundamental rights despite mass surveillance concerns from civil society. https://edri.org/our-work/cjeu-advocate-general-states-that-pnr-directive-does-not-violate-fundamental-rights-despite-mass-surveillance-concerns-from-civil-society/ [accessed March 12, 2024]
- EDRi (2014). ECJ: Data Retention Directive Contravenes European Law. https://edri.org/our-work/ecj-data-retention-directive-contravenes-european-law/ [accessed March 12, 2024]
- EDRi (2022). Mass Surveillance of External Travelers May Go On, says EU's Highest Court. https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/ [accessed March 12, 2024]
- EDRi (2017). PNR: EU Court Rules that Draft EU/Canada Air Passenger Data Deal is Unacceptable. https://edri.org/our-work/pnr-eu-court-rules-draft-eu-canada-air-passenger-data-deal-is-unacceptable/ [accessed March 12, 2024]
- European Union Agency for Fundamental Rights (2011). Opinion on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM (2011) 32 final). http://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf [accessed March 13, 2024]
- European Commission (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) 32 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52011PC0032 [accessed March 13, 2024]
- European Council (2016). Council Adopts EU Passenger Name Record (PNR) Directive. https://www.consilium.europa.eu/en/press/press-releases/2016/04/21/council-adopts-eu-pnr-directive/ [accessed March 9, 2024]
- European Council (2016). Joint statement of the EU Heads of State or Government and the leaders of the EU institutions on the terrorist attacks in

Brussels. https://www.consilium.europa.eu/en/press/press-releases/2016/03/22/joint-statement-hosg/ [accessed March 9, 2024]

- European Council (2022). The EU's Response to Terrorism. https://www.consilium.europa.eu/en/policies/fight-against-terrorism/ [accessed March 9, 2024]
- Europol (2022). European Union, Terrorism Situation and Trend Report. https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat [accessed March 9, 2024]
- House of Commons Committee of Public Accounts (2016). E-Borders and Successor Programmes. Twenty-seventh Report of Session 2015-16. https://publications.parliament.uk/pa/cm201516/cmselect/cmpubacc/643/643.pdf [accessed March 9, 2024]
- House of Lords European Union Committee (2008). The Passenger Name Record (PNR) Framework Decision: Report with Evidence. https://www.statewatch.org/media/documents/news/2008/jun/eu-pnr-uk-hol-report.pdf [accessed March 9, 2024]
- AccessNow (2022). In a bittersweet ruling, EU Court of Justice allows EU-wide border surveillance scheme but clarifies its limits. https://www.accessnow.org/press-release/eu-court-of-justice-ruling-pnr-directive/ [accessed March 10, 2024]