RUCH PRAWNICZY, EKONOMICZNY I SOCJOLOGICZNY
ROK LXXXIII – zeszyt 1 – 2021
https://doi.org/10.14746/rpeis.2021.83.1.9

JULIA WOJNOWSKA-RADZIŃSKA[*]

LEGITIMIZING PRE-EMPTIVE DATA SURVEILLANCE UNDER EU LAW – THE CASE OF THE PNR DIRECTIVE[**]

I. INTRODUCTION

The September 11 attacks on the United States and the rising threat of terrorism in the EU Member States have contributed to the development of various surveillance solutions as an attempt to ensure a high level of security and prevent another 9/11. Rather than focusing on the detection of past acts, governments are now focusing on the pre-emption of future terrorist attacks.[1] The logic of pre-emption in the counter-terrorism strategy is best summarized by a famous statement of the former US President George W. Bush: 'if we wait for threats to fully materialize, we will have waited too long'.[2] In other words, 'authorities can punish or intervene pre-emptively because they (think they) know the future and believe their prediction is always true'.[3] Therefore, pre-emptive surveillance does not start with a suspicion against a particular person or persons. It has a proactive element, aimed at identifying a danger rather than identifying a known threat. The pre-emptive approach to security threats that concentrates on prediction requires 'new imaginative technologies […] to be deployed in order to detect and disrupt possible plots at the earliest stage'.[4] Data surveillance is one of them.

Ursula von der Leyen, President of the European Commission, expressed the view that 'terrorist attacks that have struck at the heart of our Union in recent years and the ever evolving nature of organized crime have brought into sharp focus the need to improve cooperation on internal security issues

[*] Julia Wojnowska-Radzińska, Adam Mickiewicz University, Poznań, juliaw@amu.edu.pl, https://orcid.org/0000-0003-4443-652X.

[**] The author would like to thank anonymous reviewers for valuable comments.

[1] Mitsilegas (2016): 2.

[2] Bush (2002).

[3] Van Brakel (2016): 191.

[4] De Goede (2008): 162.

and build an effective Security Union. […] We must ensure that we deny terrorists the means and space to plan, finance and carry out attacks'.[5] From 2000 to 2018, 753 people were killed in terrorist attacks in the EU.[6] As Europol indicates, the threat to EU citizens from jihadist attacks either perpetrated or inspired by Islamic State (IS) and al-Qaeda and their affiliates remains high.[7] At the same time, security agencies point out that in recent years the modus operandi of terrorist organizations has changed, including target selection, choice of weapons, and the means of attack.[8] All of this poses a number of challenges for the EU and its Member States. Faced with the threat of possible nuclear, chemical, biological and conventional attacks in the Union, and bearing the responsibility for pre-empting those attacks by 'connecting the dots',[9] for security purposes the EU has decided to enhance the collection and exchange of personal data in order to generate useful and reliable correlations and ultimately to identify suspects. Personal data are perceived as one of the major assets in the fight against terrorism and transnational organized crime. As a result, the EU has adopted a pre-emptive data surveillance policy to monitor actual and potential risks and their sources through the PNR system. The Passenger Name Record (PNR)[10] is flight information provided by passengers while booking tickets and checking in. The PNR is collected by air carriers for their own commercial purposes and includes different types of information, such as travel dates, travel itinerary, date of birth, ticket information, passport details, contact details (address, e-mail, telephone number), the travel agent at which the flight was booked, the means of payment, and the seat number and baggage information. At the same time, the PNR may reveal sensitive data relating to one's religion or ethnic origin (a passenger's meal preferences) or health (medical assistance required by the passenger).

The present article aims to examine how the mass processing of PNR data under the PNR Directive affects innocent individuals. The first part outlines the background of the EU PNR system. The second part briefly explores the processing of the PNR data. The third part analyses the PNR directive as a tool for profiling passengers. The final part summarizes the article and draws some provisional conclusions.

[5] Ursula von der Leyen, Mission letter for Ylva Johansson, Commissioner-designate for Home Affairs, Brussels, 10 September 2019: 5, available at: <https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-ylva-johansson_en.pdf> [accessed: 10 January 2021].

[6] M. Pagazaurtundua-Ruiz, White and Black Book of Terrorism, available at: <https://europediplomatic.com/2019/03/04/black-white-paper-on-terrorism-victims/> [accessed: 10 January 2021].

[7] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM (2020)605 final, 24 July 2020: 4. See also Europol, European Union Terrorism Situation and Trend Report, 2020.

[8] Policy Department for Citizens' Rights and Constitutional Affairs, The European Union's Policies on Counter-Terrorism. Relevance, Coherence and Effectiveness, 2017: 39–40.

[9] Connecting the dots 'has become a metaphor for discovering the "big picture" from seemingly unrelated facts'. See Taipale (2003–2004): 3.

[10] The Passenger Name Record is a generic name given to the files created by airlines for each flight any passenger books.

II. THE BACKGROUND OF THE EU PNR LEGAL FRAMEWORK

Originally PNR data were introduced by the U.S. government in the aftermath of September 11, 2001 as a useful tool to identify people who may pose a terrorist threat.[11] The United States began assigning risk assessment ratings to all individuals entering or leaving the country.[12] It is worth mentioning that nine out of the nineteen hijackers of the 9/11 attacks had been identified as flight risks by the airport security, but were nevertheless allowed to board their planes[13].

Michael Chertoff, the former U.S. Secretary of Homeland Security, explained that 'PNR data [...] is critical for law enforcement authorities and immigration authorities to detect people who should not be allowed to enter the country or who pose a risk to others [...]. Without this data, in effect, we're without our radar. We have no way of determining in advance who is coming into this country'.[14] In November 2001, believing that the processing of PNR data could contribute to keeping terrorists out of the United States, the Aviation and Transportation Security Act was adopted, which obliged air carriers operating flights to and from the United States to provide the U.S. Bureau of Customs and Border Protection (CBP) and the Department of Homeland Security (DHS) with electronic access to data contained in their automated booking and departure control systems, called Passenger Name Record (PNR)[15]. Imposing this obligation on airlines flying from the EU has raised doubts regarding the compliance of the US PNR law with the EU data protection and privacy law. It turned out that PNR data belong to 'personal data' under the EU data protection law, as they refer to 'any information relating to an identified or identifiable natural person'.[16] As a result, the U.S. authorities put European air carriers in an awkward position, since, on the one hand, their regulations violated the EU data protection and privacy law. On the other hand, European airlines were liable to sanctions under the U.S. law if they followed the EU law.[17]

The United States and the European Union resolved that conflict by signing the first PNR agreement on 28 May 2004[18]. Nevertheless, two years later

[11] Lowe (2017): 80. See also Casagran (2015); Kaunert, Leonard, McKenzie (2012): 483; De Hert, Papakonstantinou (2010a): 369.

[12] Rizer (2010): 77.

[13] Tzanou (2017a): 108; Dummer (2006): 584.

[14] Rasmussen (2008): 583.

[15] Kaunert, Leonard, McKenzie (2012): 483.

[16] Article 2 of the Directive 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. However, this Directive is no longer in force. Currently it is Article 4 item 1 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).

[17] Tzanou (2015b): 88. See also De Hert, Schutter (2008): 322.

[18] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of

the agreement was annulled by the European Court of Justice, as it was based upon a flawed legal basis[19]. Following the Court's judgment, on 3 July 2006 the Council and the Commission notified the US Government that the said Agreement had to be terminated with effect from 30 September 2006. Bearing in mind the tight deadline, the conclusion of the new PNR agreement before September 2006 seemed unrealistic. Thus, the EU concluded an Interim Agreement[20] until a new PNR Agreement with the US was signed on 23 July 2007.[21] The fourth and last agreement for the processing of PNR data between the EU and the US, which is still in force today, entered into force on 1 June 2012.[22] Meanwhile, the EU was challenged by similar requests from other third countries, such as Canada,[23] Australia[24] and Japan[25].

Ultimately, in the Stockholm Programme the European Commission was called upon to introduce an EU PNR system.[26] In 2011 a proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was submitted. However, the European Parliament, having regard to the opinions of the European Economic and Social Committee, the European Data Protection Supervisor and the EU Agency for Fundamental Rights, rejected the propos-

PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ 2004 L 183/ 83 and corrigendum at OJ 2005 L 255/168. The Council's decision was based on the Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection, OJ 2004 L 235/11.

[19] Judgment of the CJEU of 30 May 2006, *European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities* (C-318/04).

[20] Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298 of 27 October 2006.

[21] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ L 204 of 4 August 2007.

[22] 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, OJ L 215 of 11 August 2012.

[23] On 26 July 2017, the Court of Justice of the European Union issued an opinion which stated that the draft agreement between the EU and Canada on the transfer of PNR data may not be concluded in its current form, since several provisions of the draft agreement did not meet the requirements stemming from the fundamental rights of the EU. However, the negotiations for a revision of the envisaged PNR agreement with Canada have been concluded and are pending finalization.

[24] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186 of 14 July 2012.

[25] In February 2020, the Council adopted a decision authorizing the opening of negotiations between the EU and Japan for a PNR agreement.

[26] European Council, The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens, 2010, OJ C 115/01: 19.

al in April 2013. The Commission and the European Parliament reactivated the negotiations for an EU PNR Directive after the terrorist attack on the editorial office of *Charlie Hebdo* in Paris in January 2015 and the further acts of violence which took place in this city in November 2015. Bearing in mind that an estimated 5,000 Europeans have joined terrorist organizations in Iraq and Syria and returning foreign fighters have posed a threat to security, the Council recalled the urgency and importance it attaches to the European PNR directive. In December 2015 the European Parliament and the Council reached a compromise on Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[27] In doing so, the European legislator was faced with the need to strike a proper balance between the fight against terrorism and serious crime on the one hand and protecting personal data and respecting the private life of the passengers on the other.

The PNR Directive is based on Article 87(2)(a) and Article 82(1) of the Treaty on the Functioning of the European Union. The essential objective of the PNR Directive is to 'ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities'.[28] This is to be accomplished through an assessment of PNR data leading to identify 'unknown' persons, namely persons previously unsuspected of involvement in serious crime and terrorism, but whom an analysis of the data suggests may be involved in such crime, and who should therefore be subject to further examination by the competent authorities[29].

III. PROCESSING OF THE PNR DATA UNDER DIRECTIVE 2016/681

The PNR Directive aims to harmonize Member States' provisions on the obligations for air carriers to transfer the PNR data of passengers on extra-flights[30] and the processing of those data, including their collection, use, and retention by the Member States, as well as their exchange between them[31]. Member States are obliged to ensure that air carriers transmit PNR data us-

[27] 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 (hereinafter: 'PNR Directive', 'Directive', 'Directive 2016/681'). The Directive was adopted by the 28 EU Member States on 27 April 2016 and came into effect on 28 May 2018. See also First Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2020)305 final.

[28] See Recital 5 Directive 2016/681

[29] See Recital 7 Directive 2016/681.

[30] It should be mentioned that Directive 2016/681 leaves Member States with the option of an additional opt-in to obtain passenger data from intra-EU flights, Article 2(1).

[31] Article 1(1) Directive 2016/681.

ing the ‘push method’, which means transferring data into the database of the authority requesting them.

PNR data[32] should only contain details of passengers’ reservations and travel itineraries that enable the competent authorities to identify air passengers representing a threat to internal security.[33] The Directive stipulates that nineteen categories of PNR data must be transmitted.[34] Simultaneously, PNR data cannot include a person’s race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation.[35]

PNR data may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.[36] The definition of terrorist offences applied in this Directive should be the same as in Council Framework Decision 2002/475/JHA. In turn, the definition of serious crime[37] should encompass the categories of offence listed in Annex II to this Directive. Air carriers are obliged to transfer the PNR data of all passengers to the Passenger Information Unit (PIU) established at the domestic level by the Member States.[38] PIUs are responsible for collecting PNR data from air carriers, storing, processing and transferring those data to the competent national law enforcement authorities, and for exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol.[39] PNR data are processed by the PIU’s for three purposes: firstly, to carry out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination; secondly, to respond to a request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases; and thirdly, to analyse PNR data for the purpose of updating or creating new criteria to be used in the passenger assessment in order to identify any persons who may be involved in a terrorist offence or serious crime.[40] When carrying out the passenger assessment, PIUs may compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, or process these data against ‘pre-

[32] According to Article 3(5) Directive 2016/681 PNR data ‘means a record of each passenger’s travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities.’

[33] Recital 15 and Article 3(5) Directive 2016/681.

[34] Annex 1 Directive 2016/681.

[35] Recital 15 Directive 2016/681.

[36] Article 1(2) Directive 2016/681.

[37] Serious crime refers to crimes 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.

[38] Article 4(1) Directive 2016/681.

[39] Article 4(2) Directive 2016/681.

[40] Article 6(2) Directive 2016/681.

determined criteria'.[41] Nevertheless, the Directive indicates that the assessment of passengers must be carried out in a non-discriminatory manner and these pre-determined criteria must be targeted, proportionate and specific. The criteria cannot be based on a person's sensitive data, including race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.[42] Simultaneously, the Directive specifies that Member States shall ensure that any positive match resulting from the automated processing of PNR data is individually reviewed by non-automated means to verify whether the competent authority needs to take action under the national law.[43]

IV. PNR DATA AND PROFILING

PNR data provide a detailed picture of the journey and the passenger. In order to prevent and detect serious crime, including acts of terrorism, the European Commission indicated that PNR data can be used by law enforcement authorities in three different ways: reactively, in real-time and proactively[44]. The 're-active' use refers to the use of data in investigations, prosecutions and the unravelling of networks after a crime has been committed.[45] The 'real-time' use means that PNR data are used prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed, or because a crime has been or is being committed.[46] The Commission specifies that in such cases PNR data are necessary for running against pre-determined assessment criteria in order to identify previously 'unknown' suspects and for running against various databases of persons.[47] The 'proactive' use refers to the use of PNR data for the analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers[48]. Therefore, 'PNR data are used to create patterns (future) which will be subsequently used to identify "unknown" suspects (present), which in their turn may generate further patterns [...]'.[49] For example, the use of PNR data, by comparing PNR data against various databases on persons and objects sought, enables gathering evidence and, where relevant, detecting offenders of specific crimes and unravelling criminal networks. It should be noticed that even PNR data from a few years ago, inter alia, such

[41] Article 6(3) Directive 2016/681.

[42] Article 6(4) Directive 2016/681.

[43] Article 6(5) Directive 2016/681.

[44] Proposal for a Directive of the European Parliament and 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: 3.

[45] Ibid.: 3.

[46] Ibid.: 4.

[47] Ibid.

[48] Ibid.

[49] Tzanou (2017a): 109–110.

as addresses, telephone numbers, e-mail addresses, and frequent flyer information can have a significant meaning for finding links between persons who are suspected of conducting terrorist activity or organized crime (e.g. human trafficking, drug trafficking). Hence, effective use of PNR data, for example by comparing PNR data against various databases on persons and objects sought, is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime, and thus enhance internal security. The Court of Justice has corroborated that the fight against terrorism in order to maintain international peace and to ensure security constitutes an objective of general interest recognized by the EU. Examining the draft agreement between Canada and the European Union on the transfer and processing of PNR data, the Court of Justice recognized that 'processing of [PNR] data may be regarded as being appropriate for the purpose of ensuring that the objective relating to the protection of public security and safety [...]'.[50] It should be stressed that the CJEU has accepted that the transfer, retention and use of PNR data can be a useful tool in the fight against terrorism, but only if strict and precise requirements are respected.

Nevertheless, it should be stressed that 'the PNR data transfers establish a system of mass, generalized surveillance of all passengers, citizens and foreigners alike'.[51] Regardless of whether individuals are aware of being targets of mass surveillance, the blanket collection of data has important ramifications with regard to the rule of law and fundamental rights.[52] It should be indicated that the PNR Directive affects all passengers who arrive in the territory of one Member State flying from a third country or flying from the territory of a Member State and depart in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries. It applies to all travellers, not merely those that have been identified as potentially 'risky' or even 'guilty'. Thereby, the PNR Directive applies to a large population of passengers irrespective of the country they come from, shifting the focus of risk from suspect individuals and individual groups to 'a suspect population'.[53] As Paul De Hert and Vagelis Papakonstantinou observe, 'each one is presumed a criminal suspect unless his or her profile hints at the opposite'.[54]

In essence, the assessment of every passenger prior to their scheduled arrival in or departure from the Member State on the basis of pre-determined criteria entails profiling. Profiling can generally mean 'an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or

[50] Opinion 1/15 of the CJEU of 26 July 2017.

[51] Mitsilegas, Vavoula (2017): 244.

[52] It is worth mentioning that on 31 October 2019 Belgian Constitutional Court referred ten preliminary questions to the CJEU concerning the obligation to transfer passenger information (C-817/19). In turn, on 20 January 2020 the District Court of Cologne submitted to the CJEU a preliminary question on whether the PNR Directive violated the fundamental rights.

[53] Vavoula (2017): 238. See also Rubinstein, Lee, Schwartz (2008); Rasmussen (2008).

[54] De Hert, Papakonstantinou (2015b): 163.

predicting her or his personal preferences, behaviours and attitudes'.[55] The idea of profiling is not new. However, 'the new pre-emptive surveillance technique [...] is based on inductive profiling [...] [which focuses on] clustering data in such way that information is inferred and predictions or expectations can be proposed'.[56] 'The profiles obtained are patterns that are the result of probabilistic processing of data'.[57] Then, intelligence and law enforcement authorities search 'databases containing transactional and personal information for "hits" that indicate a match between the model and patterns left by potential evidence of terrorist plans or by potentially culpable individuals'.[58] The fundamental difference in comparison with traditional criminal profiling is that 'the decision-making is done by machines and not humans, and [it] becoming difficult to trace back where certain motivations behind the decisions come from'.[59]

The main use of PNR data and 'their alleged added value is found exactly in the pattern-based analysis that can be performed on this set of data'.[60] Consequently, when a predefined profile is found in a database, the matching passenger will be further examined.[61] Thus, the PNR Directive provides national authorities with a legal instrument that allows them, on the basis of the analysis of PNR data, to apply methods relating to the identification of passengers who have not been known to the law enforcement services, on the basis of patterns of behaviour of 'risk' or presenting a 'high-risk'. However, none of these methods have been defined in Directive 2016/681 and, in fact, seem to be entirely within the discretion of the Member States. What is more, the PIU may process PNR data against pre-determined criteria and compare PNR data against relevant databases. It should be noted that the Directive does not comprise any specific provisions that refer to the principles and methods of setting up these databases. Nor is it explained which specific assessment criteria have to be applied. How these criteria have to be determined is left to the Member States, which may raise serious doubts as to whether the Directive actually establishes a legal framework providing for uniform guarantees and safeguards for the protection of PNR data for all EU citizens. Since the Directive does not lay down precise provisions that clarify how the processing of PNR data will be performed, passengers cannot predict the full impact of this regulation on their lives.

It should be highlighted that pattern-based searching depends on the power of the statistical model which is used to detect suspicious individuals[62]. As a result, 'this approach may intrude in known and unknown ways into the lives

[55] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies.

[56] Van Brakel, De Hert (2011): 173.

[57] Van Brakel, De Hert (2011): 173.

[58] Rubinstein, Lee, Schwartz (2008): 263.

[59] Van Brakel, De Hert (2011): 173.

[60] Tzanou (2017a): 175.

[61] Leese (2014): 501.

[62] Rubinstein, Lee, Schwartz (2008): 263.

of innocent people'.[63] Some scholars have criticized this approach. It is worth quoting J. Dempsey and L. Flint, who present the view that pattern-based searches raise concerns with 'the constitutional presumption of innocence and the Fourth Amendment principle that the government must have individual suspicion before it can conduct a search'.[64] In turn, Rosamunde Van Brakel and Paul De Hert state that passenger profiling leads to 'social sorting: they sort people into categories assigning worth or risk'.[65] As a result, religious minority such as Muslim people are much more vulnerable to thorough checks and greater scrutiny, before they can get on a plane, as they are perceived as more suspicious than other passengers.[66] Finally, there is a danger of false positives. A false positive refers to innocent individuals that are wrongly identified by the algorithm. It is possible to find out profiles that provide valuable insights to law enforcement authorities about suspected individuals, but (at the same time) it is also inevitable that while using profiles the authorities will misinterpret the results and come to wrong conclusions about individuals. Inaccurate profiling can lead to an innocent passenger being blacklisted, investigated, humiliated or detained.[67] Therefore, the question remains of how to verify the risks inherent in these profiles regarding 'false positives' or the discriminatory and abusive effect of them on certain groups in society.[68]

It is true, as has already been mentioned, that Directive 2016/681 specifies that the assessment of passengers must be carried out in a non-discriminatory manner and that these pre-determined criteria must be targeted, proportionate and specific. Nevertheless, like the criteria, this provision should also cover the databases against which PNR data are compared to prevent these databases from being based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. According to the case law of the European Court of Human Rights, applying databases and assessment criteria should above all make it possible to obtain results which would be focused on the person with regard to whom there exists a reasonable suspicion of them being involved in a serious crime or terrorist activity, in other words, there are factual indications for suspecting that person of planning, committing or having committed a terrorist offence or serious crime.[69] In *Digital Rights*, the Court of Justice of the EU stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[70] Furthermore, in Opinion 1/15 the CJEU specified that

[63] Rubinstein, Lee, Schwartz (2008): 263.

[64] Dempsey, Flint (2004): 1466.

[65] Van Brakel, De Hert (2011): 176.

[66] Van Brakel, De Hert (2011): 176.

[67] Rubinstein, Lee, Schwartz (2008): 263. See also Leese (2014): 496 and 499.

[68] Tzanou (2017a): 177.

[69] Judgment of the ECtHR of 4 December 2015, Application no. 47143/06, *Zakharov v. Russia*: para. 260.

[70] Judgment of 8 April 2014 of the CJEU, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases No. C-293/12 and C-594/12: para. 64.

provisions concerning retention of PNR data have to satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued. In the Court's view 'the retention of [PNR] data after the air passengers' departure must be limited to that of passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime'.[71] The PNR Directive does not stipulate objective reasons that would justify the necessity of retaining all PNR data for five years.[72] Since a vast number of persons are affected, additional criteria to limit the scope of targeted passengers must be added to Directive 2016/681.

V. CONCLUSION

9/11 has given way to pre-emptive forms of surveillance, leading to gathering, retaining and analysing a vast amount of personal data of millions of people on an unprecedented scale in order to investigate a person who has yet to commit a crime, and to determine their guilt with regard to a future crime based on past events. Pre-emptive surveillance assumes that everyone is untrustworthy.

Using PNR data, the individual is profiled and encoded in terms of degrees of risk. The transfer of the specified personal data of air passengers, as well as their retention, aims to allow for the comparison of the data against pre-determined criteria or databases in order to identify persons previously unknown to law enforcement authorities. Nevertheless, the analysis of such a huge amount of data can easily lead to the entry of false data, which are then hard to correct. Although, the PNR Directive provides that any positive match resulting from the automated processing of PNR data requires human review, it is an illusory safeguard. To be clear 'data-driven profiling in security screening relies on the assumption that all revealed patterns must necessarily be scrutinized in order to ascertain whether they pose an actual threat. But, as the output of neural networks is most likely only machine readable, the human operator must act on the basis of the translation of algorithmic terms into risk levels'.[73] In fact, 'the human reviewers lose true agency, as they only enact what algorithmic categorizations indicate'.[74] When algorithms increasingly dictate the decisions of law enforcement authorities regarding, for instance, placing a passenger on a terrorist 'risk' or 'high-risk' list, the data subject – the individual included in profile-based selections – is less able to question those outcomes.

Furthermore, the provisions on these pre-determined criteria and databases, as well as the retention of PNR data for a period of five years, do not

[71] Opinion 1/15 of the CJEU of 26 July 2017.

[72] Article 12(1) Directive 2016/681.

[73] Leese (2014): 505.

[74] Leese (2014): 505.

meet the necessity requirement for interference under the principle of proportionality. These provisions do not make any distinction based on the passengers concerned and therefore allow the retention of the PNR data of all air passengers. In other words, the legislator has not limited PNR data in a clear and precise way to what is strictly necessary according to the European data protection standard.

Bush, G.W. (2002). Delivers Graduation Speech at West Point, United States Military Academy West Point, New York, June 1, 2002. <https://georgewbushwhitehouse.archives.gov/news/releases/2002/06/20020601-3.html> [accessed: 1 March 2020].

Casagran, C.B. (2015). The future EU PNR System: will passenger data be protected? European Journal of Crime, Criminal Law and Criminal Justice 3: 241–257.

De Goede, M. (2008). Beyond risk: premediation and the post-9/11 security imagination. Security Dialogue Special Issue on Security, Technologies of Risk, and the Political 39(2–3): 155–176.

De Hert, P., De Schutter, B. (2008). International transfer of data in the field of JHA: the lessons of Europol, PNR and Swift, [in:] B. Martenczuck, S. Thiel (eds.), Justice, Liberty and Security: New Challenges for EU External Relations. Brussels: VUB Press/Brussels University Press: 303–340.

De Hert, P., Bellanova, R. (2011). Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals. Migration Policy Institute: 1–27. <https://www.immigrationresearch.org/system/files/dataprocessing-2011.pdf> [accessed: 10 April 2020].

De Hert, P., Papakonstantinou, V. (2010a). The EU PNR framework decision proposal: towards completion of the PNR processing scene in Europe. Computer Law & Security Review 26(4): 368–376.

De Hert, P., Papakonstantinou, V. (2015b). Repeating the mistakes of the past will do little good for air passengers in the EU: the comeback of the EU PNR Directive and a lawyer's duty to regulate profiling. New Journal of European Criminal Law 6(2): 160–165.

Dempsey, J., Flint, L. (2004). Commercial data and national security. The George Washington Law Review 72: 149–1502.

Dummer, S.W. (2006). Secure flight and dataveillance, new type of civil liberties erosion: stripping your rights when you don't even know it. Mississippi Law Journal 75(2): 583–618.

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.

Leese, M. (2014). The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union Security Dialogue 45(5): 494 –511.

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.

Mitsilegas, V. (2016). Surveillance and digital privacy in the transatlantic 'war on terror': the case for a global privacy regime. Columbia Human Rights Law Review 47(3): 1–77.

Mitsilegas, V., Vavoula, N. (2017). The normalization of surveillance movement in an era of reinforcing privacy standards, [in:] P. Bourbeau (ed.), Handbook on Migration and Security. Edward Elgar Publishing: 232–251.

Rasmussen, D. (2008). Is international travel per se suspicion of terrorism – the dispute between the United States and European Union over passenger name record data transfers. Wisconsin International Law Journal 26(2): 551–590.

Rizer, A. (2010). Dog fight: did the international battle over airline passenger name records enable the Christmas-day bomber? Catholic University Law Review 60(1): 77–105.

Rubinstein, I.S., Ronald, L.D., Schwartz, P. (2008). Data mining and internet profiling: emerging regulatory and technological approaches. The University of Chicago Law Review 75(1): 261–285.

Taipale, K.A. (2003–2004). Data mining and domestic security: connecting the dots to make sense of data. Columbia Science and Technology Law Review 5(1): 1–83.

Tzanou, M. (2017a). The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Hart Publishing.

Tzanou, M. (2015b). The war against terror and transatlantic information sharing: spillovers of privacy or spillovers of security? Utrecht Journal of International and European Law 31(80): 87–103.

Van Brakel, R. (2016). The rise of preemptive surveillance of children in England: unintended social and ethical consequences, [in:] E. Taylor, T. Rooney (eds.), Surveillance Futures: Social and Ethical Implications of New Technologies on Children and Young People. Routledge: 190–203.

Van Brakel, R., De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies. Journal of Police Studies 20(3): 163–192.

Vavoula, V. (2017). EU immigration databases under scrutiny: towards the normalisation of surveillance of movement in an era of "privacy spring"? [in:] G. Vermeulen, E. Lievens, Data Protection and Privacy under Pressure. Transatlantic Tensions, EU Surveillance, and Big Data. Maklu: 215–251.

LEGITIMIZING PRE-EMPTIVE DATA SURVEILLANCE UNDER EU LAW: THE CASE OF THE PNR DIRECTIVE

Summary

The paper analyses the PNR Directive as pre-emptive data surveillance practice. The 2016/681 Directive regulates the use of Passenger Name Record (PNR) data in the EU for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. It obliges airlines to hand national authorities passengers' data for all flights from third countries to the EU and vice versa, but Member States can also extend it to 'intra-EU' ones (i.e. from an EU country to one or more other EU countries), provided that they notify the EU Commission. Thus, PNR Directive affects all passengers who arrive in the territory of one Member State originating from a third country, or who depart from a Member State's territory to a non-EU country, including any transfer or transit flights. Using PNR data, the individual is profiled and encoded in terms of degrees of risk.

Keywords: PNR data; passenger; profiling; mass surveillance; pre-determined criteria; risk assessment