Maritime Law 2017,vol. XXXIII
ISSN 0860-7338

IWONA ZUŻEWICZ-WIEWIÓROWSKA*
WOJCIECH WIEWIÓROWSKI**

RE-USE OF MARITIME PASSENGERS' PNR DATA FOR PUBLIC SECURITY PURPOSES

Abstract

The increasing threat of terrorist attacks in Europe and social demands for governmental actions towards facilitating an information exchange between the national authorities responsible for public security, lead to the spectacular shift towards collection of passengers' data. Initially, the idea had concerned mainly aviation passengers' data and was limited to international flights only. But soon it was extended in order to include the Passenger Name Records (PNR) from domestic transport. Recently, we can see tensions to expand the PNR collection scheme to other means of transport including maritime routes. The paper studies the most developed system created in Belgium and assesses its influence on possible all-European solutions. When presenting the main problems connected with profiling the passengers and data sharing between institutions, it discusses a lack of precise privacy impact assessment and the need for necessity and proportionality studies to be carried out both at the level of Member States and in the EU discussion on the implementation of the so called PNR Directive and on the new requirements for the digital registration of passengers and crew sailing on board European passenger ships included in 2017 amendments to Directive 98/41/EC.

Keywords: Passenger Name Records (PNR), public security

* Iwona Zużewicz-Wiewiórowska PhD, Maritime Law Department, Faculty of Law and Administration, University of Gdańsk.

** Wojciech R. Wiewiórowski PhD, European Data Protection Assistant Supervisor since December 2014. Adjunct professor at University of Gdansk. Inspector General for the Protection of Personal Data (GIODO) 2010-2014 and Vice Chairman of the Working Party from February to November 2014.

INTRODUCTION

The increasing threat of terrorist attacks in Europe and the social demands for governmental actions towards better security standards regarding all means of transport with special attention given to international routes, have caused a spectacular shift towards the collection of passengers' data. The data – which eventually is to be turned into information on possible terrorist routes – is collected in large interconnected and interoperable databases held by public authorities or at least controlled by such authorities. The European Union has added to the system the idea of international co-operation in the field of such data and enabled the EU agency – eu-LISA[1] – to create and manage an all-European system of research on passengers' information.

Initially, the idea had concerned mainly the aviation passengers' data and had been limited to international flights only. But soon, it was extended in order to include the Passenger Name Records (PNR) from domestic transport. Recently, some EU Member States pushed for extending such a duty to other means of transport including passengers transport by sea - at least the cross-border one. The paper studies the most developed – from the legislative point of view – system existing in Belgium and assesses its influence on possible all-European solutions.

1. PASSENGER NAME RECORD

The Passenger Name Record is a record in a database which is a part of a booking system (the Computer Reservation System – CRS) operated by an air carrier, a tour operator or a specialised third party. It consists of the so called PNR data descripting the reservation itself and the travel it applies to. There is no uniform list of PNR data for all CRSs in use in different sectors of passenger transport, as well as booking hotels or renting cars. However, a standard was somehow defined by the International Air Transport Association (IATA) for air traffic. Even that standard should be regarded as a minimum list. While PNR was initially designed

[1] European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) managing currently EURODAC, the Visa Information System (VIS) and the second generation Schengen Information System (SIS II) was established in 2011 (by Regulation (EU) No 1077/2011) and it started its operation on 1 December 2012. The headquarters of eu-LISA are based in Tallinn, Estonia, whilst its operational centre is in Strasbourg, France. There is also a business continuity site for the systems under management based in Sankt Johann im Pongau, Austria.

for air transport, it is today widely used in other modes of transport as well as for booking hotel rooms and the car rental.

PNR data should be distinguished from the API data (Advance Passenger Information) containing only basic information to identify a passenger or a crew member and which includes: name and surname, date of birth, gender, nationality and travel document (e.g. passport number). The whole scope of API data can be machine-readable from a passport or an identity card.

In addition to the API standard PNR data shall include information on: the operator's system(s) and may include the following data elements: address details (contact address, billing address, emergency contact, email address, mailing address, home address, intended address), contact telephone numbers, frequent flyer information, PNR locator code, number of passengers on PNR, passenger travel status, standby information, all date information (PNR creation date, booking date, reservation date, departure date, arrival date, PNR first travel date, PNR last modification date, ticket issue date, "first intended" travel date, date of first arrival, late booking date for flight, split or divided PNR information (multiple passengers on PNR, other passengers on PNR, other PNR reference, single passenger on booking), all ticketing field information (date of ticket issue and purchase, selling class of travel, issue city, ticket number, one-way ticket, ticket issue city, automatic fare quote [ATFQ] fields), all travel itinerary for PNR (including ports, itinerary history, origin city, board point, destination city, active itinerary segments, cancelled segments, layover days, flown segments, flight information, flight departure date, board point, arrival port, open segments, alternate routing unknown [ARNK] segments, non-air segments, inbound flight connection details, on-carriage information, confirmation status), form of payment (FOP) information (cash, electronic, credit card number and expiry date, prepaid ticket advice, exchange), details of the person or agency paying for ticket, staff rebate codes), all check-in information, check-in security number, check-in agent I.D., check-in time, check-in status, confirmation status, boarding number, boarding indicator, check-in order, seats requested in advance, actual seats, all baggage information (number of bags, bag tag numbers, weight of bags, all pooled baggage information, head of pool, number of bags in pool, bag carrier code, bag status, bag destination and offload point), travel agent information, name of a person making the booking, go-show information and no-show information as well as general remarks and all IATA codes. Other information such as time, pseudo-city code agencies are recorded automatically in the CRS[2].

The national authorities also require the supplementation of PNR with data on: gender, nationality, passport data (identifiers), expiry date, date of birth,

[2] Guidelines on Passenger Name Record (PNR) Data, Ed. 1, IATA, 2010, p. 27.

information on visas (visa number, city, which was issued, the date of issue, the country on whose territory the visa is valid), information relating to the local authorities to specific regions, the permanent residence card (such as a Green Card), the so-called Redress Number of the passenger, place of birth (city), address of residence in the country of destination, the temporary address in the country of destination, the address of the first accommodation in the country of destination and any information about payments and accounts[3].

It appears, however, that the explanations provided to passengers on processing of data by CMS and the legal provisions concerning the obligations on controllers of such systems do not reveal all information. Carriers – when the access to the data is required by the data subjects according to personal data protection law – reveal copies of the passenger's PNR showing additional information retained[4]. While such data as individual telephone numbers and e-mail addresses can be regarded as "contact details", the same does not refer to an IP address used by the passenger when booking the flight[5].

That may show that the general impression that PNR data processing is somehow less intrusive than retention of communications traffic and location data is a myth. Holbrook rightly states that PNR may disclose fewer details about private lives than communications metadata, especially when one does not travel by airplane very often. However, PNR can reveal one's travel habits, the relationship between two (or more) people, the fact that they shared the same flight as well as the same hotel, the person or company who paid for the ticket, and so on. Dietary information (such as requests for kosher or hala'l meals) typically serves as a substitution for sensitive information about religious beliefs[6]. What is even more important, the real reason why PNR data is so valuable to law enforcement authorities is that, thanks to the complex computer algorithms, it allows to identify individuals previously unknown. PNR makes possible what is known as "predictive policing".

The studies reported to the Council of Europe – when its consultative committee of data protection (T-PD) studied the PNR threats – stress that the most

[3] *E. Hasbrouck*, What's in a Passenger Name Record (PNR)? WWW service The Practical Nomad, constantly updated material, as it stands for 5.10.2017 https://hasbrouck.org/articles/PNR.html.

[4] *Poznaj swój PNR: jakie dane z linii lotniczych trafią w ręce służb?* Panoptykon Foundation, 13.7.2015 https://panoptykon.org/wiadomosc/poznaj-swoj-pnr-jakie-dane-z-linii-lotniczych-trafia-w-rece-sluzb

[5] E. Hasbrouck, *op. cit.*

[6] Pleading notes of the European Data Protection Supervisor (EDPS) on request for an opinion by the European Parliament, draft EU-Canada PNR agreement (Opinion 1/15), Hearing of 5.4.2016 accessible at: https://edps.europa.eu/sites/edp/files/publication/16-04-05_pleading_canada_pnr_en.pdf.

worrying issue, as far as predictive policing is concerned, is that it is explicitly aimed at allowing the use of PNR data for the kind of "rule-based" "identification" of people as posing certain "risks" (e.g., as "high-risk"). Nobody hides that the PNR processing systems aim at obtaining information on "unknown criminals or terrorists". While in other databases, such as the Schengen Information System (SIS) or Visa Information System (VIS), which provide information solely on identified persons regardless of whether they are being reported for specific goals (arrest warrants or refusal of entry), the transfer and especially the analysis of PNR data should assist national authorities of the Member States in identifying criminal offenders or associates or persons suspected of terrorism or serious crimes.

The advantage of PNR data processing is indeed enabling the national authorities to perform "a closer screening only of persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security". However, computerised profiling on the basis of "pre-determined criteria" – i.e., algorithms which had been entered into a computer, and then were dynamically "improved" – will never reduce discrimination that may appear when human check is involved, while it is seriously misleading and dangerous. The studies for the Council of Europe record even some wider implications – including the undermining of "respect for the human identity" made by the competent authorities, based on one of these discrimination grounds, which is still possible. Furthermore, the reference to "decisions" does not make clear that this prohibition also applies to the measures of the national authorities, including physical measures such as searches or preventing persons from entering the territory.

2. PASSENGER DATA ACCORDING TO EU LAW

The legislator in the European Union decided to intervene in that matter by issuing – paradoxically on the same day when the General Data Protection Regulation was issued –Directive 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 crimes[7]. The directive sets a new all-European system which is created in order to process data of all passengers travelling from or to the European Union[8].

[7] OJ L 119, 4.5.2016, pp. 132-149.

[8] *A.G. Zarza* (ed.), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin-Heidelberg 2015, pp. 219-222.

The national dedicated databases will store the profile of a person including:
– PNR record locator,
– date of reservation and issue of a ticket as well as date(s) of intended travel,
– names,
– address and contact information (telephone number, e-mail address),
– all forms of payment information, including billing address,
– complete travel itinerary for specific PNR,
– frequent flyer information,
– travel agency and travel agent,
– travel status of passenger, including confirmations, check-in status, no-show or go-show information,
– split or divided PNR information,
– general remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, languages 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),
– ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields,
– seat number and other seat information,
– code share information,
– all baggage information,
– number and other names of travellers on the PNR,
– any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time),
– all historical changes to the PNR listed in numbers 1 to 18. The data gathered on passenger airlines will be transferred to the newly created entities — the so-called Passenger Information Units (PIUs). Member States can decide what entity will perform these tasks. This may be a new independent authority, but arguably in most countries, it will be operated within the framework of the police or intelligence service. The data will be transmitted twice. For the first time, within 48 to 24 hours before the flight departure and immediately after closing of the gates, when the passenger list is already final. PIUs shall provide data to other authorities upon their explicit and reasoned request. Also in this case, the decisions under which the public authorities are to be entitled to such data are left to the Member States. On the basis of the new provisions, the PIU

may carry out its own analysis on the basis of the data collected, e.g. on trends in international crime and endorse the conclusions of the relevant services.[9]

For the first 30 days all the data collected by PIUs will be processed and transmitted to other authorities (on request). Later, the data will be kept separate from the passenger identification data. The association of passenger data and identification of the complete profile will require the consent of the Head of the PIU. "Pseudonymised" PNR profiles will be processed for 5 years and, when necessary, they will be forwarded to the competent services.[10]

The PNR Directive does not affect the possibility for Member States to provide, according to their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services – including the booking of flights – for which they collect and process PNR data. It also allows the Member States to establish law which requires such data from transportation providers other than those specified in that Directive. Such a norm opens the rules to other means of transport including the maritime one.

According to Annex II of the PNR Directive the data may be used in combating 26 kinds of serious offences:

– participation in a criminal organisation,
– trafficking in human beings,
– sexual exploitation of children and child pornography,
– illicit trafficking in narcotic drugs and psychotropic substances,
– illicit trafficking in weapons, munitions and explosives,
– corruption,
– fraud, including that against the financial interests of the Union,
– laundering of the proceeds of crime and counterfeiting of currency, including the euro,
– computer-related crime/cybercrime,
– environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
– facilitation of unauthorised entry and residence,
– murder, grievous bodily injury,
– illicit trade in human organs and tissue,
– kidnapping, illegal restraint and hostage-taking,
– organised and armed robbery,
– illicit trafficking in cultural goods, including antiques and works of art,
– counterfeiting and piracy of products,
– forgery of administrative documents and trafficking therein,

[9] *Poznaj swój PNR…*
[10] *Ibidem*

– illicit trafficking in hormonal substances and other growth promoters,
– illicit trafficking in nuclear or radioactive materials,
– rape,
– crimes within the jurisdiction of the International Criminal Court,
– unlawful seizure of aircraft/ships,
– sabotage,
– trafficking in stolen vehicles,
– industrial espionage.

3. BELGIUM EXPANDS PNR REGULATION TO MARITIME TRANSPORT

Last days of 2016 brought the first implementation of the act of the European Union into the national legal systems that extended the requirements relating to the collection of PNR data, the transfer thereof to the central national database and its secondary processing over the required limit. Belgian law introduced the mandatory system of undertaking such activities not only towards the data of air passengers but also to the travellers using other modes of transport, including maritime vessels, as long as the journey has an international dimension. Belgian law requires carriers and tour operators to collect and transfer data of passengers in international traffic to the special national database.[11] According to these provisions, the passengers entering, exiting or transiting through Belgium should be manifested by the registration on the passengers list. The crew members are not regarded as passengers.[12] The need to collect and transmit passenger data refers to the sector of passenger transport by air, rail, road and the sea. It includes international flights, international high-speed train services, international bus services and maritime transport.[13][14]'Transport by sea' - according to the law - means an international journey by sea using the vessel carrying passengers that enters, leaves or passes through a port located in Belgium.

[11] Law of 25.12.2016 on the processing of passenger data (*Loi relative au traitement des données des passagers*), Moniteur Belge, 25.1.2017, No 2017010166, p. 12905.

[12] Article 4 (10°).

[13] Maritime transport is defined in the statute as an international carriage by sea using the vessel carrying passengers entering, leaving or passing in transit through a port situated in Belgium (Article 7 paragraph 6).

[14] The recording of data of all passengers was one of the measures designed to combat terrorism announced on 19.11.2015 by the Prime Minister to the parliament (*Lutte contre le terrorisme - mesures décidées par le Gouvernement fédéral. Séance plénière Chambre*, 19.11.2015).

The framework law and clarification of the provisions in relation to the date of entry into force, will be implemented by sectoral regulations. The text contains many delegations to that issue implementing legislation (*Arrêté délibéré en Conseil des ministres*). They will clarify for each of the transport sectors which data is transmitted and how. The implementing regulation will take account of the specific characteristics of each sector concerned. The statute and the following implementing acts are meant to transpose three directives: a) Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, b) PNR Directive and c) in the marine sector, partially 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. The scope of the last Directive is wider than the framework law.

The drafters of the new law tried to take into account the provisions of European law developed in order to increase the maximum interoperability of data between the Passenger Information Units of different Member States.[15] The Belgian data protection authority, in its opinion, has expressed a reservation on the possible conflict thereof with EU law. It has assessed that the collection of passenger data entering and exiting the Schengen area may violate the principle of free movement of persons. The proposed measures may than indirectly lead to the re-introduction of internal border controls.[16]

The law states that "travellers' profiles" will be used for the purpose of:

– prevention and combating terrorist offences and serious crimes (e.g. smuggling, trafficking in human beings, arms, drugs and other illicit goods);
– prevention of serious disturbances of public security by monitoring developments and groups associated with violent radicalisation;
– searching, analysing and processing information on behaviour which may jeopardise the fundamental interests of the State. Passenger data will also be used by the police services and the Office for Foreigners in order to fulfil their missions of external border control and the application for residence and asylum. The aim is not only to tackle irregular immigration, but also to provide more effective control of the external borders. There is a close link between illegal immigration and terrorism. The latter two objectives are particularly in the spotlight of the Belgian data protection authority. Monitoring of ac-

[15] DOC 54 2069/003 Chambre des Représentants de Belgique, Projet de loi relatif au traitement des données des passagers, 4.10.2016, Chambre de la 54e 3e Session Législature; Exposé des motifs, p. 6.

[16] Avis N° 55/2015 of 16.12.2015, La Commission de la protection de la vie copie; DOC 54 2069/003 Chambre des Représentants de Belgique, Projet de loi relatif au traitement des données des passagers, 4 octobre 2016, Chambre de la 54e 3e Session Législature, p. 79 and ff.

tions, that may pose a threat to fundamental interests of the state, is defined too broadly and is not restricted to fighting terrorism and should be clarified. Processing data, relating to transport within the EU to combat irregular immigration, is neither appropriate nor justified.[17] The objectives permitted processing, five paragraphs are laid down in Article 8 of the Act in this regard. The legislature described the objectives of data processing by reference to the specific provisions of Belgian law.

The draft stated that there had already been some systems for collection of data on passengers in maritime transport and aviation. According to the opinion thereof – based on European and international law – the draft has the same objectives as the system that requires carriers to submit certain data concerning their passengers to be used by the border control while the application for the entry and residence is issued.[18] With regard to maritime transport the royal decree (*arrêté royal*) of 11 April 2005 on border checks at the external maritime borders transposed Directive 2002/6/EC (the directive was replaced by Directive 2010/65/EU). It imposed similar obligations on those provided for by the draft on shipping operators[19]. With regard to air transport, Directive 2004/82/EC has been transposed into Belgian law by the Royal Decree of 11 December 2006. Directive 2004/82/EC complements Directive 2010/65/EU with the Schengen rules on crossing borders. However, the new Belgian law has a wider scope than Directive 2004/82/EC, since the obligation imposed on carriers has been extended to all transport sectors[20].

The collection and processing of passenger data shall facilitate prediction of risks associated with criminal movements. The comparison of such data with other existing databases and the analysis thereof according to the predefined criteria should also allow for the discovery of criminal operational methods, the new trends and developments, as well as the identification of passengers who shall be subject to a thorough check[21].

According to the new passengers' statute PNR data will be uploaded in the national database (*banque de données des passagers*) managed by the Federal Public Service Interior (FPS Interior) [22]. The analysis of passenger data will be entrusted

[17] *Ibidem.*

[18] DOC 54 2069/003 Chambre des Représentants de Belgique, Projet de loi relatif au traitement des données des passagers, 4 octobre 2016, Chambre de la 54e 3e Session Législature; Exposé des motifs, pp. 10-11.

[19] *Ibidem*, p. 10.

[20] *Ibidem*, p. 11.

[21] *Ibidem*, p. 5.

[22] Chapter 8. Federal Public Service Interior (nl: *FOD Binnenlandse Zaken* , fr: *SPF Intérieur*, de: *FÖD Inneres,* abbreviated as FPS Interior) is a federal service of Belgium which was created by Royal Order on 14.1.2002 as a part of the plans of the Verhofstadt I Government to modernise the federal administration. It is responsible for guaranteeing the rule of law, the registration and identification

to the Passenger Information Unit (PIU) set up in the framework of FPS Interior[23]. Its tasks include the collection and storage of data as well as processing and managing the PIU database. It is also responsible for the exchange of passenger data and the result of processing thereof with similar organisations in other EU Member States, Europol and third countries.

The statute confirms that data is to be stored for a maximum of 5 years from the date of its registration and later it will be destroyed[24]; 6 months after the registration all data is depersonalised by masking data which could serve to identify directly the data subject[25]. From that date the access to full data shall be allowed only on a case-by-case basis and under the conditions established by law. The statute also confirms that a passenger has a right of accession and rectification of his or her data.

The Law introduces some mechanisms which should provide guarantees with respect to the protection of privacy. In particular, PNR data is to be made available only to the PIUs and the competent services laid down in the draft. It also clearly sets out the purposes of processing. Processing of data is differentiated depending on the access and type of infringement. The eligible services will not have direct access to all the data. They have to meet the precise and predetermined criteria. The manager – FPS Interior – will exercise its controlling functions independent of other services. FPS Interior should establish the position of a Data Protection Officer and processing itself should be tracked for 5 years[26].

The statute distinguishes data collected on booking and boarding. The maximum list of PNR data on booking includes a) code; b) the date of reservation and ticket issuance; c) the expected travel; d) the names, forenames and date of birth; e) the address and contact details (email address and telephone number); e) a complete description of the route; f) information on the participation of a passenger in loyalty programmes; g) information on the payment method (including the invoicing addresses); h) an indication of the travel agent or the agent; i) the status of a passenger (including information on booking, cancellation of booking, the last-minute booking); j) information on the distribution of PNR;[27] k) details of the travel of minors under 18 years accompanied or unaccompanied; l) information on the issuance of tickets and the digital attributes thereof as well as informa-

---

of natural persons, the immigration policy and for guaranteeing public order and safety. The FPS Interior is responsible to the Federal Minister of the Interior.

[23] Chapter 7.

[24] Article 18.

[25] Article 19, paragraphs 1 to 6.

[26] DOC 54 2069/003 ..., p. 12.

[27] With regard to the situations where the PNR issued for a group of passengers has been divided into individual or smaller groups of passengers.

tion on the ticket price; m) any additional characteristics and number of the case; n) the distribution code; o) all baggage information; p) data on other passengers under the same PNR or API data).

The list of maximum data from boarding includes: a) the type of the travel document;[28] b) the document number; c) information on citizenship; d) indication of the country of issue of the document; e) the expiry date of the document; f) the surname, first name, gender, date of birth of a passenger; g) an indication of the carrier and/or tour operator; h) the means of transport; i) the date of departure and arrival; j) the place of departure and the destination; k) the time of departure and the time of arrival; l) the total number of passengers; m) the number of seats assigned; n) the PNR code; o) the number, weight and identification of luggage and the border crossing point; p) the border crossing point which was used to enter the territory of Belgium or exit from the country.

The carriers and tour operators should destroy API data which they transmit to the Passenger Information Unit within 24 hours after the end of the journey (Article 31).

The most important provisions, however, cover the introduction of the new pre-screening procedures, according to which the authorities are allowed to make assessment of a potential risk represented by passengers before an entry, exit or transit through the territory of Belgium. It may lead to additional actions taken by the competent authorities towards passengers who are of particular interest for them (e.g. execution of an arrest warrant).[29] This preliminary assessment is to identify those who should be subjected to further analysis and further examination. Evaluation is carried out through the correlation with other databases and by the assessment on the basis of the criteria pre-defined by PIU[30]. Such previously defined criteria shall be based on one or more objective indicators. An assessment of passengers is limited to the positive correlation of passenger data with other databases when it prevents serious disturbance of public security in the context of violent radicalisation. The Belgian data protection authority pointed out, in its opinion, that there is a need for a clarification which databases will be used for correlation of data with the passenger. However, it may be done in implementing the acts to be drafted in the future[31]. The draft delivered to the Belgian Parliament

[28] The statute has finally introduced mandatory checks of the travel document and identity of the passenger. In relation to tour operators that duty implies reasonable diligence in checking the compatibility between passenger travel and identity documents. Many passengers travelling in Belgium were surprised that Belgian air carriers do not make such verification even at the international airport Zaventem in Brussels.

[29] DOC 54 2069/003 ..., p. 28.

[30] See Article 24-26 of the Statute.

[31] Avis N° 55/2015 ..., DOC 54 2069/003 ..., p. 79.

confirmed that – as it is stated in the European data protection law – no decisions producing legal effects for the person or likely to cause serious harm can be based solely on automated processing of data on his or her journey[32].

Specific rules are provided for with regard to processing passenger data for the external borders control, relating to migration and asylum. Chapter 11 deals with processing passenger data to improve border controls and combat illegal immigration. According to those rules, only API data can be passed to the police department responsible for border controls and to the Foreign Office. The purposes of processing passenger data are the same as those included in Directive 2004/82 EC.

4. CONTROVERSIES ON PNR DATA PROCESSING

Despite the attempts to address the most important data protection issues, the Belgian legislator failed to assess if using PNR data for the purpose of data mining and profiling can be dangerous for the fundamental rights of passengers. Some of these dangers are recognised inherent for data mining and profiling according to the legal theory[33]. As a UK government study acknowledges,[34] in all cases of profiling, a challenge will be to become certain that our understanding of human behaviour (both individual and collective), and our capability apply the model.

The most recent and constructive criticism of the PNR requirements came from the Court of Justice of the EU in the so called *PNR Canada Case*, where the European Parliaments asked the Court for the opinion on the recently signed agreement on the PNR data exchange between the EU and Canada[35]. Once again, the European Court confirmed that the European Commission had failed to understand which legal requirements were to be observed when – a generally

[32] DOC 54 2069/003 ...,p. 30.

[33] *D. Korff*, The use of the Internet & related services, private life & data protection: trends & technologies, threats & implications, presented to the Council of Europe Consultative Committee on Data Protection, March 2013 (T-DP(2013)07), available at: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/KORFF%20-%20TPD(2013)07Rev_Trends%20report%20-%20March2013.pdf.

[34] UK Government report on Technology and Innovation Futures: UK Growth Opportunities for the 2020s – 2012 Refresh (meaning the updated version of the 2010 report, issued in 2012), section 2.1(11), at p. 19: http://www.bis.gov.uk/assets/foresight/docs/horizon-scanning-centre/12-1157-technology-innovationfuturesuk-growth-opportunities-2012-refresh.pdf.

[35] Earlier history of PNR agreements negotiated by EU is summarised in: *M. Taylor*, Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement, The Spanish Yearbook of International Law No 19, 2015, pp. 223-225.

acceptable – idea of PNR found its implementation into statutory law.[36] On 26th July 2017 the Court declared that the agreement might not be concluded in its forms which had been passed to the European legislator[37]. The Parliament referred the agreement to the Court in order to assess the regularity of the agreement under EU law, in particular the Charter of Fundamental Rights of the European Union. In the Opinion of the CJEU it was declared that retention of bulk data was excessive and would, therefore, violate the fundamental rights of EU citizens. In its previous judgments on *Digital Rights Ireland*[38] (declaring that the Data Retention Directive[39] is invalid) and *Schrems*[40] (on a validity of the so called *Safe Harbor Agreement* with the USA) the CJEU found that the date of the retention period, was set between 6 and 24 months, and *'entails serious interference with those fundamental rights in the legal order of the EU'*. Similarly, the Court of Justice – deliberating on the PNR agreement between UE and Canada, which had been referred to the Court by the European Parliament, made a decision[41]. The Court admitted that the transfer itself – (even made on a systematic basis), the retention and use of all PNR were, in essence, permissible but it agreed with the Parliament that several provisions of the draft agreement did not meet the requirements stemming from the fundamental rights of the European Union. The Court questioned the systematic and continuous transfer of data of all air passengers to a Canadian authority with a view to that data being used and retained and possibly subsequently transferred, to the other authorities and the other non-member states, for the purpose of combating terrorism and serious transnational crimes. Since the period during which PNR data may be retained may last for up to five years that agreement makes it possible for information on private lives of passengers to be available for a particularly long period of time.

The Court has stated that the EU-Canada agreement should determine in a more clear and precise manner to ensure the PNR data to be transferred. It should also provide that the models and criteria used for the automated processing

[36] European Court Opinion: Canada PNR cannot be signed, EDRi 8.9.2016, https://edri.org/european-court- opinion-canada-pnr-deal-cannot-be-signed/.

[37] *H.Hijmans* PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators, European Data Protection Law Review No 3, 2017, 310-312.

[38] Cases C-293/12 and C-594/12.

[39] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[40] Case C-362/14.

[41] Similar concerns were also shared by EDRi and the European Data Protection Supervisor (EDPS). See: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2015-08-edps_pnr_en.pdf.

of PNR data will be specific, reliable and non-discriminatory. The use of databases should be limited to combating terrorism and serious transnational crimes only. The law should also provide for a right to individual notification for air passengers in the event of use of PNR data concerning thereof during their stay in Canada and after their departure from that country, and in the event of disclosure of that data to the other authorities or to individuals. The Court required the guarantee that the oversight of the rules relating to the protection of air passengers with regard the processing of PNR data was carried out by an independent supervisory authority[42]. Finally, it observed that the interferences which are entailed by the envisaged agreement were not all limited to what was strictly necessary and were therefore not entirely justified[43]. These requirements were poorly explained in the discussion on the Belgian statute allowing the collection of maritime passengers' data. Therefore, there is a reasonable doubt if the new law may resist judicial control.

5. MARITIME PASSENGERS' DATA COLLECTED FOR SAFETY PURPOSES

Even if it is decided that the collection of PNR data of maritime passengers is necessary and useful, it has to be noted that it is anyway repetitive in comparison with the duty, that has already been existing, to collect personal data of people sailing on board passenger ships for the purposes of maritime safety. Not only European, but also national law, requires the identification of persons on longer routes by sea which should assist an effective and efficient conducting search and rescue operations at sea. For those reasons, the carrier has to ensure that the number of persons on board does not exceed the number for which the ship has been intended but it should also observe the detailed rules for the calculation and registration of those travelling.

According to Belgian law the obligation is laid down in the Decree of the Minister for Transport, Construction and Maritime Economy of 23 April 2013 on counting and registering persons travelling[44]. At the European level, it is regulated by the provisions of Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the

[42] See also the position in this case of Advocate General Paolo Mengozzi in this case: http://curia.europa.eu/juris/documents.jsf?num=C-1/15.

[43] EU and Canada PNR Agreement Invalid, SCL The IT Law Society, https://www.scl.org/news/3734-eu-and-canada-pnr-agreement-invalid.

[44] Journal of Laws 2013, item 586.

Member States of the Community[45]. The directive requires physical counting of all persons on board a passenger ship departing from a port in the EU before the vessel commences a voyage. The list made onboard the ship shall remain in the hands of the ship's captain, but its copy should be delivered to the shore-based Information System together with detailed information, within 30 minutes of departure of the ship from the port. Any company responsible for operating a passenger ship shall set up a system for the registration of information on persons on board. The system shall meet the criteria for legibility, accessibility, facilitation of work (the system shall not cause any excessive delay of passengers embarking and/or disembarking) and security (protection of data against destruction, loss and unauthorised access). The company should appoint a passenger registrar responsible for keeping and transmission of information[46].

It does not relate to all maritime travels since the Member States of the EU may grant exemptions or derogations regarding counting and registering passengers in some circumstances. European law allows to exempt ships sailing exclusively in protected sea areas, providing regular transport services of a voyage from a port to port for less than one hour and the regular services in an area, where there is the probability of encountering waves of a height exceeding two metres, is less than 10 %, and if the voyages do not exceed 30 miles or where the primary purpose of the service is the provision of interconnection for the regions on the periphery. None of these exemptions affect international journeys.

In the case of any safety sea risk or accident, the shipowner shall send registered information to the Maritime Search and Rescue Service (SAR) and (if requested) to the administrative authorities (in Poland to the maritime office), the border guard, the Merchant Navy, the Police and the head of the Internal Security Agency. The European Union promotes digitalisation of that process to ensure that, in the event of an accident, the search and rescue services have an access to accurate information about the people on board. The currently discussed rule in this respect updates the requirements for registering passengers and crew on board European passenger ships[47]. Amendments to Directive 98/41/EC, in this respect, were passed by the European Parliament and the Council in October 2017 (on 4th and 23rd October) and they introduced the requirement to register passenger data in a digital manner, using harmonised administrative procedures of the so-called single window to facilitate search and rescue operations in case of emergency. For

[45] OJ L 188, 2.7.1998, p. 35, as amended.

[46] The framework of processing the data for statistical purposes is set in Directive 2009/42/EC as far as passengers of vessels calling at EU ports are concerned.

[47] EU digitalises passenger registration to make travelling by sea safer: the Council agrees its position, European Council & Council of the EU, http://www.consilium.europa.eu/en/press/press-releases/2017/03/21-passengers-registration-travelling-by-sea/.

a period of 6 years after the entry into force, the Member States may continue to apply the old rules, i.e. keeping data concerning persons on board by the companies' registrars. The delay in reporting data on persons on board is shortened from 30 to 15 minutes after the ship's departure. The new rules proposed also including nationality in the data to be recorded, in addition to the name, date of birth, gender and, if a passenger wishes so, the need for a special assistance in an emergency situation.

CONCLUSIONS

The demand to strengthen and fasten an information exchange between the national authorities responsible for public security lead the Member States of the European Union to creating the framework for an all-European system of collecting, sharing and further processing of passengers' data. It started with airlines' clients since this threat seemed to be the most urgent, but the relevant European law regulations left an open gate for the extension of the national PNR systems to other means of transport including passenger transport by see. The first EU Member State to introduce the legal background for the maritime PNR is Belgium, though until the end of 2017 the necessary secondary legislation has not yet been prepared nor even been discussed publicly.

The general discussion on the subject lacked the precise privacy impact assessment as well as the necessity and proportionality studies[48]. However, it led to the simultaneous interpretation of Directive 2004/82/EC on the obligation of carriers to communicate passenger data, b) PNR Directive and c) in the marine sector, partially, Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports. This process corelates with the amendments to Directive 98/41/EC on the registration of persons sailing on board passenger ships operating to or from ports of EU.

It is hard to deliberate on the constitutionality of the Belgian legal solutions for maritime passengers but it seems to be certain that in light of the test, set by CJUE in its current opinion on the EU-Canada PNR agreement, the preparation of maritime legislation has not met the standards required, though it can be supplemented during the discussion on secondary legislation.

[48] L. Bygrave, *Data Privacy Law. An International Perspective*, Oxford 2011, pp. 94–96 and 147–150.

WYKORZYSTANIE DANYCH PNR DOTYCZĄCYCH PASAŻERA PODRÓŻUJĄCEGO DROGĄ MORSKĄ DLA CELÓW BEZPIECZEŃSTWA PUBLICZNEGO

Słowa kluczowe: dane PNR, bezpieczeństwo publiczne

Abstrakt

Wzrost zagrożenia atakami terrorystycznymi w Europie i nacisk społeczny na rządy w celu podejmowania działań, które ułatwiłyby wymianę informacji pomiędzy krajowymi organami odpowiedzialnymi za bezpieczeństwo publiczne doprowadziły do stworzenia systemów informacyjnych, w których wtórnie przetwarzane są dane pasażerów. Początkowo scentralizowane systemy objęły pasażerów lotniczych podróżujących na trasach międzynarodowych, ale niedługo po tym zostały rozszerzone tak by objęły dane PNR (*Passenger Name Records*) dotyczące ruchu krajowego. Dziś obserwujemy tendencję rozszerzania ich na inne środki transportu, włączając w to sektor morski. W niniejszej pracy dokonano oceny najbardziej rozwiniętego z dotychczas stworzonych systemów przetwarzających dane PNR – wprowadzonego w Belgii – oraz przedstawiono wnioski płynące z jego stworzenia dla rozwiązań ogólnoeuropejskich. Przedstawiając najważniejsze problemy związane z profilowaniem pasażerów oraz z wymianą danych pomiędzy uprawnionymi instytucjami, omówiono w niej problem braku oceny wpływu przedsięwzięcia na prywatność osób, których dane są przetwarzane oraz zasygnalizowano potrzebę dokonania poprawnej oceny niezbędności i proporcjonalności rozwiązań wprowadzanych tak na poziomie państw członkowskich, jak i w unijnej dyskusji nad wdrożeniem dyrektywy PNR oraz nowych wymagań dotyczących elektronicznej rejestracji pasażerów rejestracji pasażerów i członków załogi na pokładzie europejskich statków pasażerskich zamieszczonych w pakiecie zmian do dyrektywy 98/41/WE.