MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
INTERNATIONAL LAW DEPARTMENT

GINTARĖ JANULAITYTĖ

AVIATION SECURITY AFTER 9/11 AND HUMAN RIGHTS

Master thesis

Supervisor assoc.
prof. dr. J. Žilinskas

VILNIUS, 2008

MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
INTERNATIONAL LAW DEPARTMENT

AVIATION SECURITY AFTER 9/11 AND HUMAN RIGHTS

Joint International law master thesis
Program of the studies 62401S118

Supervisor assoc.
prof. dr. J. Žilinskas
2008 12

Reviewer

2008 12

Prepared by
TTAmd7-01 gr.stud.
G. Janulaitytė
2008 12

VILNIUS, 2008

TABLE OF CONTENTS

TABLE

FIGURES

ACRONYMS

ACLU – American Civil Liberties Union

ASA – ICAO Aviation Security Audit

ATSA – US Aviation and Transportation Security Act

API(S) – Advanced Passenger Information (System)

CBP – US Bureau of Customs and Border Protection

DHS – US Department of Homeland Security

ECAC – European Civil Aviation Conference

EC – European Commission

EDPS – European Data Protection Supervisor

ECHR - European Convention on Human Rights

EU – European Union

EP – European Parliament

FAA – US Federal Aviation Administration

FAL – ICAO Facilitation progamme

ICAO – International Civil Aviation Organization

ICCPR – International Covenant on Civil and Political Rights

MoU – Memorandum of Understanding

OSI – Other Service related Information

OECDG – Organization's for Economic Co-operation and Development Guidelines

PANS - Procedures for Air Navigation Services

PNR – Passenger Name Record

SARP's – ICAO international Standards and Recommended Practices

SFP – Security and Facilitation Policy

SSI/SSR – Special Service Information/ Special Service Request

TSA – Transportation Security Administration

TIP – Threat Image Projection

USA/US – United States of America/ United States

USAP - Universal Security Audit Programme

WTMD – Walk-through Metal Detector

INTRODUCTION

Freedom of movement is a fundamental and internationally recognized human right, and a vital prerequisite for the exercise of other fundamental rights[1]. Also it is an indispensable condition for the free development of a person[2]. That is why this thesis concerns of two elements- air law (focusing on air transportation - civil aviation security) and human rights law. I will restrict research focus to a specific aspect of human rights- within right to privacy scope I will examine the **object of this thesis**. That is Passenger Name Record (PNR) data analyzed within dimension of aviation security. The **actuality and problematic aspect** related to thesis object is how to balance between privacy rights and aviation security, when the United States of America dictate "security above all" norms to the rest of the community. US seem to create rule of law according to its own benefits and so remains one of super powers state. Meanwhile European Union adjusts itself to those norms and consequently faces inaccuracy with own privacy laws.

The necessity of this balance was long ago reflected in the words of Benjamin Franklin (1759), which precisely captured the nature of a modern society facing imminent threats: "Those who would give up essential liberty for a little temporary safety deserve neither liberty nor safety"[3]. The terrorist attacks of 9/11 accelerated the creation of new security measures to ensure safety of every citizen, while often treating civil liberties as less of a priority. Moving towards "security above all" system, policy makers seem to have forgotten the words of B. Franklin, making entire international community wonder whether various increases of security are worth the restrictions of privacy and of other civil liberties.

After 9/11 counter-terrorism has made it of vital importance for states to monitor and control flight into, out of and over their territory, for this purpose it was necessary detailed exchange of information about passengers and crew on those flights. Under adopted Aviation and Transportation Security Act (November, 2001), US obliged its security agencies to get access to the personal

[1] International Covenant on Civil and Political Rights, Article 12 (1966) // http://www.unhchr.ch/html/menu3/b/a_cescr.htm [retrieved November 28, 2008].

[2] United Nations Human Rights Committee, General Comment No 27 (1999)// http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/6c76e1b8ee1710e380256824005a10a9?Opendocument; [retrieved October 24, 2008]

[3] Benjamin Franklin (1759)// http://www.theamericanpatriotsite.com/pages.asp?pageid=51523 [retrieved October 24, 2008]

information provided by passengers when booking a flight ticket[4]. In May 2002 another law was adopted requiring airlines to transfer passenger data to the US Immigration and Naturalization Service through Advanced Passenger Information System (APIS). Refusing to comply with these provisions airlines were threatened with a withdrawal of their US landing authorization. Meaning if there is no PNR transferred, there is no ability to land in the US territory[5]. Moreover, living in an innovative information technology century it tends to be easy to exchange data, virtually access to it and also to misuse it.

So this thesis concerns about right to privacy issues and PNR data transfers between EU and US through necessity to maintain international aviation security. Also it focuses on PNR data legal dilemma and doubtful PNR data Agreements of 2004[6], 2006[7] and 2007[8]. Finally all mentioned aspects are being discussed while paying attention to aviation security importance after 9/11 and necessity to balance it with privacy rights. That is why International Civil Aviation Organization is presented also for its crucial role to set up legal standards on its Member States in order to preserve security in air transportation sector at the same time ensuring balance of fundamental right to privacy.

Through this thesis I will analyze whether mentioned PNR data Agreements and PNR data *per se* are effective measures for strengthening and safeguarding air transportation. So **hypothesis** is that EU-US legal dilemma for ensuring aviation security can not be solved only by PNR data transfer and collection; this measure can be additional to combat terrorism, used in narrower scale and so posing less risk for privacy rights.

I have chosen this area to research firstly because of its actuality to nowadays' society. With this thesis I intend to cause public awareness that collection of personal information in the airports and while booking the flight is for a reason and may leave consequences. Also after 9/11 attacks in New York and Washington DC aviation security was greatly improved giving priority to strict precautionary measures in the airports and on board. The main focus was to combat terrorism and prevent any possible threats in the future. Such "war on terror" within air transportation sector endangered privacy

---

[4] USA Aviation and Transportation Security Act (19 November, 2001) // http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf [retrieved April 28, 2008]

[5] See answer of the Commission to the Written Question P-0871/03 OJ 222 E, 18.09.2003 P 0239-0241

[6] OJ L 235, 6.7.2004 P 0011-0022

[7] OJ L 298, 27.10.2006 P 29

[8] OJ L 204, 4.8.2007, P.0018-0025

rights (case studies of San Francisco incident with electrically warmed shoes[9], new screening Backscatter X-ray technologies[10] etc). The conclusions of my research will be useful to a wide range of people: to ordinary travelers (mainly to those who constantly travel to the US and do not exactly know about PNR data collection), to EU law makers who should consider upcoming PNR data Agreements more attentitive and should not leave possibility to the US be a dominant Contracting party. Finally this thesis will be useful for such audience who is interested in international law and precisely EU- US cooperation on privacy rights matters. Presumably it will leave a lasting value for future researches on counterterrorism measures within aviation security and privacy rights scope.

Aim of the thesis is to examine 3 concluded PNR data Agreements together with 95/46/EC Privacy Directive and to evaluate their legal importance ensuring aviation security and right to privacy balance for counter- terrorism; also to research how those legal documents could be amended in order not to pose risk to privacy rights. For completing this aim, it is necessary to set up main **tasks**:

1. To present the necessity of equilibrium between right to privacy and guaranteed security.
2. To evaluate the input of 3 PNR data Agreements to ensure aviation security and combat terrorism after 9/11.
3. To propose articles to be amended in PNR data Agreements in order to solve EU-US legal dilemma.
4. To examine why collecting such data is crucial (or is not) for aviation security and how effectively it helps to combat terrorism.

I will analyze this dilemma using empirical methods and qualitative research[11] of 2004, 2006, 2007 Agreements, also, 2320/2002 Regulation and 95/46/EC Directive. Moreover there will be examined recent PNR data legislation of November 2008. Research will be done using 2 **types of sources**: US laws, EU Directives/Regulations, 3 PRN data Agreements and International Conventions related to right to privacy and other crucial literature on the issue: EU Joint Press Releases, EU Committees Reports, US Intelligence and Senate Reports, American Civil Liberties Union and ICAO Documents, Human Rights Brief and Political Philosophy Journals, Amnesty International USA, Amnesty.org and Privacy International webpage data, Congressional Researches of US Department of

[9] BBC NEWS, Shoes trigger airport security alert (April, 11, 2002) // http://news.bbc.co.uk/2/hi/americas/1922748.stm [retrieved October 19, 2008]

[10] SHNEIER B. Backscatter X-Ray Machines and your Privacy// http://www.schneier.com/blog/archives/2006/12/backscatter_xra.html [retrieved October 19, 2008]

[11] Silverman D. Doing qualitative research. A Practical Handbook (second edition) - London, Thousand Oaks, New Delhi: Sage Publications, 2005. – 99 p. – ISBN 1-4129-0197-9. – ISBN 1-4129-0196-0

Homeland Security, US Government Accountability Office Reports and etc. To have very recent knowledge on the topic I used BBC, CNN News, Washington Times and Lithuanian portal delfi.lt. For statistical information I used Eurobarometer (2004-2008) and Rasmussen Reports (2008). Finally I concluded interview with Lithuanian Civil Aviation Administration officers and got very interesting data to be used in this thesis[12].

Revising used literature it is prominent to mention its diversity and embodied disagreements. US publications and laws justify "security above all" position and necessary intervention into privacy rights. EU is more concerned on privacy of its citizens and so stands for opposite philosophy on how PNR data should be treated. Above it all, there are neutral philosophers who seek for the true evaluation on security vs. privacy issues. Essential person for getting objective information for this research was Bruce Schneier - internationally renowned security technologist and former Secure Flight Working Group on Privacy and Security specialist[13].

My work will be phenomenological. I will reveal my critics and suggestions, based on gotten knowledge from above mentioned literature on how the PNR data legal dilemma could be solved. Diversity of literature leaves opportunity to make own conclusions and this way permits this thesis to be original and scientifically useful.

Concerning about the **structure -** the substantial part of this thesis is divided into three parts corresponding to legal dilemma of aviation security and right to privacy. First part examines aviation security as a necessary tool within G8, ICAO, EU and US legal and practical framework. Civil aviation as such exists in order to prevent criminal activities on aircraft and in airports. The abuse to it can threaten national security in general and endanger human rights. In contrary secure civil aviation grants people ability to enjoy their fundamental rights and to conclude their legal duties to others. I have chosen to examine right to privacy within aviation security scope.

The second part focuses on privacy and security dichotomy. Firstly it is presented international documents which had embodied right to privacy. Reviewing regional level legislation, EU privacy directive 95/46/EC with embodied 5 key principles is examined. Lastly additional privacy legal instrument so called Safe Harbor[14] principles is analyzed as well (in order to bring US companies up to a minimum level of compliance with the EU Directive 95/46/EC).

Third part contents legitimate framework of PNR data, which caused EU-US legal dilemma. After describing PNR data as an object of aviation security I incorporate in this thesis practical debate

[12] See Chapter 3.2

[13] See http://www.schneier.com/ [retrieved September-December, 2008]

[14] OJ L 215, 25.8.2000. P 7 – 47

on security vs. privacy using Lithuanian Civil Aviation Administration officers' interview. Finally using empirical methods I analyze and criticize PNR data Agreements of 2004, 2006 and 2007. Consequently, using recent European Data Protection Supervisor and European Parliament legislation there is provided several proposals, how PNR data Agreements can be amended and how EU-US legal dilemma could be solved. Finally according to such evaluation the answer is given whether collecting PNR data is effective measure to combat terrorism and to ensure civil aviation security.

The thesis concludes with an evaluation of presented dilemma and sums up core proposals on what changes EU and US should reach in order to ensure security and fundamental right to privacy.

Accordingly, analysis of PNR data as a privacy right object within aviation security scope is very important to international community in order to have good political, economical, social relations between US and EU, preserve peace, security and human rights at the same time. Countries' cooperation in the aviation security is also very essential, because global air transportation remains a driver of nowadays economic development, core point for business and tourism the same as the important feature for the worlds cultural, social communications.

1. AVIATION SECURITY AS A NECESSARY TOOL: SOURCES AND PRACTICES

1.1. G8 Cooperative legal action and proposals for ICAO

The events of 11 September introduced a new type of security threat to civil aviation, calling for new countermeasures while at the same time emphasizing that those measures already in place be vigorously maintained. In June 2002, the G8 set up cooperative actions to promote greater security of land, sea and air transport. As for air transportation, G8 group emphasized the necessity to maintain financial support for the ICAO to fulfill its standards and recommended practices, known as SARP's. Also it foresaw the necessity to review aviation security conventions, implement common global standard for the collection and transmission of advance passenger information (API) and focused on enhancing sharing of information internationally with law enforcement and other appropriate counterparts with respect to passengers for whom there are specific and serious reasons to consider that they might be engaged in a terrorist acts. By API system customs and/or immigration officials of the destination country got ability to organize clearance process in advance of the arrival of the flight. Moreover it started to control entry/exit system, which compiled entry/exit data to detected overstays.

For ensuring this initiative, the G8 experts were reviewing the progress every six months while promoting policy coherence and coordination within ICAO. Next crucial steps included the following:

1. Implemented new standards to ensure the safety of travel for citizens. G8 airlines got new tight security standards (within EU, see the Regulation 2320/2002 together with 622/2003[15]);
2. G8 provided substantial voluntary contributions to ICAO, particularly to its aviation security programme in order to ensure compliance with international standards and develop new safeguards to protect travelers.
3. For identifying terrorists traveling illegally, G8 adopted global standards for travel documents (e.g. biometrics) and improved security related technologies (X-Rays, Backscatters, screenings, prescreening).

[15] See O J L 335, 30/12/2002 P. 0001-0022 and OJ L 89 5.4.2003 P 0009-0010

4. G8 provided to improve national laws that complemented international conventions and increase the exchange of evidence for making it easier to prosecute or extradite terrorist[16].

Such propositions by G8 assisted to ICAO programmes to ensure safe air transportation after 9/11. Following chapter examines precisely aviation security measures taken by ICAO.

1.2. General approach on aviation security: ICAO

ICAO is in the leading role to assure that civil aviation remains safe and secure at all times and so it has always been to establish the international standards for civil aviation, to assist its Contracting States in the implementation of these standards and procedures, and to provide global leadership in promoting safe and orderly development of international civil aviation.

ICAO is a specialized agency of the United Nations Organization[17], created on 7 December, 1944 with signing the Convention on the Civil Aviation (Chicago Convention[18]). This Organization comprises of 190 Contracting States, with its headquarters in Montreal (Canada). ICAO is the permanent body charged with the administration of the principles laid down in the Chicago Convention and sets the standards for aviation safety, security, efficiency and regularity. Article 44 of the Chicago Convention states that the aims and objectives of the Organization are to develop the principles and techniques of international air navigation and to foster the planning and development of international air transport so as to: "a) insure the safe and orderly growth of international civil aviation throughout the world; <…> d) meet the needs of the people of the world for safe, regular, efficient and economical air transport; <…> h) promote safety of flight in international air navigation…" Moreover, ICAO possesses legal personality both at the level of international and national law, and can enjoy it in the territory of each contracting state as necessary for the performance of its institutions. "Full juridical personality is granted wherever compatible with the constitution and laws of the State concerned"[19]. ICAO stands for preserving aviation security issues, international security arrangements "with respect to air matters within its competence directly affecting world security<…> and preserve peace"[20].

---

[16] Organization for Economic Co-operation and Development, Background material on biometrics and enhanced network systems for the security of international travel (2004) // http://www.oecd.org/dataoecd/16/18/34661198.pdf P 6

[17] Weber L. International Civil Aviation Organization. An Introduction. Kluwer Law International, 2007. P. 11.

[18] The Chicago Convention (1944) // http://www.icao.int/cgi/goto_m.pl?/icaonet/dcs/7300.html; [retrieved May 20, 2008].

[19] Ibid Article 47.

[20] Ibid Article 64.

Finally Chicago Convention Article 54(L) establishes necessity to adopt SARPs[21] for the safeguarding of international civil aviation. This also refers to the Article 37 whereas "Each contracting State undertakes to collaborate in securing the highest practicable degree of uniformity in regulations, standards, procedures<…>in all matters in which such uniformity will facilitate and improve air navigation". According to this provision and assistance of G8 ICAO had adopted international SARPs which are periodically updated and are under supervision of ICAO'S Facilitation Programme FAL. This programme provides Contracting States the means of attaining and maintaining high-quality security and law enforcement with a view to improving air transport productivity and enhancing customer service quality. Also it works on the issue of the Machine Readable Travel Documents (passports, visas etc.) In close correlation with SARPs there are Procedures for Air Navigation Services- PANS, which have become essential tool for the planning processes of ICAO, both on the global and regional basis, as well as for the planning processes of contracting States.

It is important to mention the ICAO Aviation Security and Facilitation Policy Section SFP, which is responsible for the management of the ICAO Aviation Security Programme. SFP section also manages Annex 9 (Facilitation), Annex 17 (Security and Facilitation Manuals) and Machine Readable Travel Documents programme.

Above mentioned programs become effective because of cooperation with UN Terrorism Committee, UN Office of Drug and Crime, INTERPOL, regional organizations such as the Organization for Security and Co-operation in Europe, and the mentioned G8 group, in the global effort to combat terrorism, in matters regarding standards, regulations and guidance materials[22]. Moreover, another section of the ICAO, regularly promoting global aviation security throughout the Contracting States, is the Aviation Security Audit Section with its Universal Security Audit Programme. The Audits evaluate the implementation of legal basis on aviation security issues and provide recommendations to States on achieving better implementation and global harmonization of aviation security measures. This programme started in 2002 and had a five-year cycle with the initial audits of all Contracting States until December 2007. Generally speaking, the audits take place from 4 to 6 months with accordance of

[21] Shawcross and Beaumont, Air Law - Contemporary Tables and Index. Butterworths, 2007. Division II, P. 12-20. **Standards** mean any specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as *necessary* for the safety or regularity of international air navigation and to which member states will conform in accordance with the convention. **Recommended Practices** means any specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as *desirable* in the interests of safety.

[22] Aviation Security and Facilitation Branch // http://www.icao.int/atb/sfbranch/index.asp? [retrieved April 8, 2008]

the bilateral memorandums of understanding (MoU) signed between ICAO and the State to be audited[23]. After careful inspection and under terms of the MoU, the audited State agrees to submit a corrective action plan detailing the particular action it intends to take to implement ICAO recommendations. Immediate and direct assistance may be available through ICAO mechanism on aviation security. This type of cooperation with the auditing bodies promotes States a greater understanding of systematic security issues, leading to remedial solutions and strategies that can be addressed at regional and global level. But auditing and issuing assistance is not the final point on safeguarding aviation- the final responsibility for the safety and security of civil aviation lies with States. Each one must remain committed to the implementation of international standards**.**

In 2008 it has started a second cycle of security audits with some novelties.

As already mentioned since 2002 ICAO has been responsible under Chicago Convention Annex 17 to conclude Audits in its Contracting States, including the EC Member States. On the basis of Regulation (EC) No 2320/2002, the Commission conducts security inspections in order to monitor the application by Member States of this Regulation. Annex 17 and mentioned Regulation contain similar standards. As a consequence to this, Member States are confronted with two compliance monitoring systems with the same objective and the same scope. To cancel this legal dualism and reduce individual audits by ICAO in Member States the European Community and ICAO issued draft Memorandum of Cooperation[24] regarding security audits/ inspections and related matters on 25 January 2008. It was adopted on 7 October, 2008. Article 1.4 of Memorandum provides that "ICAO auditors may occasionally join the European Community inspections of EU airports as observers, after an explicit agreement of the EU Member State concerned has been received by the European Commission". Meaning that now Member States have right to complete audits in their airports without constant interruption of ICAO.

Lithuania joined ICAO in 1992 and had ratified the Chicago Convention 1944, Authentic Trilingual Text 1995, The Hague Protocol 1955, Guadalajara Convention 1961, Tokyo Convention 1963, The Hague Convention 1970, Montreal Convention 1971 and its supplementary Protocol 1988, and Convention on Plastic Explosives 1991.

---

[23] ICAO Journal, VOL.58, No.7. September 2003. Page 5-6.

[24] Memorandum of Cooperation between the International Civil Aviation Organization and the EC regarding security audits and inspections and related matters (2008)// http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008PC0335(01):EN:HTML [retrieved October 7, 2008]

ICAO itself and mentioned aviation security conventions had contributed to a gradual significant reduction in the number of criminal acts. But it is crucial to develop its practices constantly in order to be adjusted to present aviation security needs.

1.3. European Union input

European Union has great importance in the field of aviation security. The EU Member States, in the aftermath of 9/11, responded quickly and on broad scale to the new dimension of terrorist threats in 2001. EU focused not only on the terrorist threats and its prevention in the future, but also on the improvement of the aviation security as such[25]. Firstly, EU issued Plan of Action on Combating Terrorism, including the measures in the field of visa policy, border control, foreign policy, civil and health protection, aviation and maritime security. Secondly EU Regulation No 2320/2002[26] of the European Parliament and of the Council established common rules for the Member States in the field of civil aviation security which came into force in 2003.

At the beginning, recital 1 states the basic reason of taking such measures: "The criminal acts committed in New York and Washington <…> show that terrorism is one of the greatest threats to the ideals of democracy and freedom and the values of peace, which are the very essence of the European Union." Meaning that it is important to establish prevention mechanism from any future acts of unlawful interference against civil aviation in the Member States. Moreover each Member State should adopt a national civil aviation security programme (within the period of 3 months following the entry into force of this Regulation), as well as a corresponding control programme and a training programme" (within 6 months following the entry into force of this Regulation) [27]. Apart of such programmes Member States shall set "common basic standards on aviation security measures", and appropriate compliance monitoring mechanisms[28]. Also, in relation with third countries, Article 10 defines that Commission, assisted by the Security Committee, consider, together with the ICAO and ECAC, the possibility to develop a mechanism to assess whether flights coming from third country airport meet the essential security requirements.

[25] ICAO Journal, VOL.58, No.7. September 2003. Page 7, 28.

[26] O J L 335, 30/12/2002 P. 0001-0021

[27] Ibid Recital 8 in correlation with Articles 5.1 and 7.2

[28] Ibid Article 1.3 a) and b)

Consequently form such provisions EU is willing to create safer aviation security network within its territory assuring that any other non member state has to meet EU aviation requirements. Talking about other specific issues in the EU regulation, its Annex Article 2- 13 describe measures which should be implemented in the Member States airport security systems. Article 2.1 defines the necessity of direct access of airport, passenger and cargo terminal with other buildings relating this essential requirement to security controls and protection to security restricted areas and other sensitive airport areas and facilities. Each airport of Member States must have security restricted areas, to which the access shall be controlled at all times and no unauthorized person enters these areas (Article 2.2.2.). All airport staff is required to be regularly trained in aviation security and fulfill special technical requirements of their official status (e.g. wearing identification cards at all times, being screened before entering any security restricted areas). Article 3 defines the aircraft security requirements: 3.1.1 a) "aircrafts not in service shall be subject to an aircraft security search immediately before and immediately after being taken into a security restricted area for a flight", 3.1.1. b) "aircrafts in service, during turn-around or transit stops, shall be subject to an aircraft security check immediately after passenger disembarkation or as late as possible before passenger boarding…" These measures are taken in order to make sure that either aircraft is or is not in service, security is integral and the aircraft presumably is sterile at all times.

Article 4 of the Annex emphasizes the requirements for passengers and cabin baggage. The most important issues are as following: 4.1.1 states that all departing passengers are subjects for screening in order to prevent any possible dangerous goods to be introduced into the security restricted areas and on board an aircraft. The screening can be concluded searching by hand (4.1.1.a) OR by Walk-Through-Metal-Detection equipment (4.1.1.b)[29]. Talking about cabin baggage, it also has to be screened by full hand search of the content of each bag (4.3.1.a), OR by conventional x-ray equipment with hand searching of screened bags (4.3.1.b), OR screening can be concluded by High Definition x-ray equipment fitted with TIP installed and employed (4.3.1.c). Diplomat screening is the exception in both personal and their baggage cases (4.4.). Article 5- 12 defines other important measures for maintaining safe aviation. All the mentioned harmonized rules had served gradually to increase civil aviation security.

[29] In several airports it was observed that both methods are being used, and it screened by hand and by WTMD equipments. So it is doubtful why the Regulation uses definition "OR"

1.4. US New security measures after 9/11: passenger and baggage screening

The object of this chapter is only passenger and baggage screening, because it closely correlates with general thesis object - PNR data: passengers and their possessions fall under the required information field, which is collected for PNR. Consequently airport security, aircraft security, cargo, courier and express parcels, mail and air carrier materials do not fall under this research scope[30]. For this reason only two mentioned elements will be analyzed.

One of main factors for aviation security on board is to assure that passengers do not posses any dangerous goods that might cause potential threat. After 9/11 the process of screening passengers became stricter. At the same time it was observed the necessity to balance between the complicated screening procedure and the speed of passage through security checkpoint in order not to cause delays and hassles to travelers in the airports. The greatest attention was paid on procedures for screening passengers for explosives. In the framework of the USA legal system, the Intelligence Reform and Terrorism Prevention Act of 2004[31] was amended with special part for deployment and use of detection equipment at airport screening checkpoints. Title IV, subtitle B, section 4013 (a) states that the Department of Homeland Security "shall give a high priority to developing, testing, improving and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons and explosives <…> on individuals and in their personal property."

In order to achieve high results, it is important to improve the screener job performance. Section 4015 emphasizes that "Transportation Security Administration shall take such action as may be necessary to improve the job performance of airport screening personnel" (section 111 of the ATSA of November 2001[32] also emphasizes the importance of training and employment of security personnel). Before 9/11 it was no such provision mentioned, and 2004 Act started to require specialized training for screeners on security skills such as behavioral observation and analysis, explosives detection and

[30] See O J L 335 30/12/2002 P. 0001-0021 and its amended Regulation 662/ 2004, OJ L 229 29.6.2004 P.0003-0004.

[31] Intelligence Reform and Terrorism Prevention Act (2004) // http://www.nctc.gov/docs/pl108_458.pdf [retrieved November 17, 2008]

[32] The USA Aviation and Transportation security Act (2001) // http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf [retrieved May 5, 2008]

document examination. According to ATSA section 110 explosive detection systems has to be deployed to all US airports no later than December 31, 2002 and it has to be “fully utilized <…> and if explosive detection equipment at any airport is unavailable, all checked baggage is screened by an alternative means”. Moreover, there is necessity to concentrate on the chemical and biological weapon detection. Section 120 defines the need to “maximize the use of technology and equipment that is designed to detect or neutralize potential chemical or biological weapon”.

It is crucial to improve screening process for ensuring that dangerous prohibited items are not being carried into the sterile areas of heavily used airports or do not enter the checked baggage system. Talking about the technologies a dual or multi-view x-ray machine has to be mentioned. With this technology screeners are provided with high resolution 3-D images that can be rotated on the screening monitor, enabling them to identify any possible explosives and weapons. Concerning the Walk-Through Metal Detector Alarm Resolution WTMD, it uses the Backscatter x-rays, which offers a more effective and unambiguous alarm resolution strategy than a pat- down inspection. Last novelty - the Threat Image Projection TIP which is a computer software program displaying fictitious images of threat items in the actual image of passenger bags, or that projects entirely fictitious bags, with or without threat items, on to the x-ray monitor. TIP had been installed only in several airports in the USA, in other cases some deployed x-ray machines are still not TIP- ready and cannot accept installation.

Talking about the screening issue before 9/11, firstly, there were no strict methods used in order to screen passengers and their belongings. Rapid turnover among screeners and rapid screening of passengers had caused various tragic consequences, one of those examples could be 9/11 itself. After those attacks, significant attention was paid to the sufficiency of the screeners training.

Belgium, Canada, France, the Netherlands and the United Kingdom were those countries to make a significant improvement in screeners training. In these countries screeners’ qualifications are more extensive. In contrast to the previous 9/11 regulations of USA, Belgium required screeners to be citizens; France required screeners to be citizens of a EU country, the Netherlands- screeners do not have to be citizens, but they must have been residents of the country for 5 years. After 9/11 USA legislation stipulated that the screeners must be also US citizens. Training time also differed from USA and mentioned EU countries. While USA required 12 hours of training, Belgium, France and Netherlands required 40 to 60 hours training for screeners (before 9/11). Finally these countries from the beginning have placed responsibility for screening with airport authorities or the government instead of air carriers. Considering about the prior 9/11 legal situation of USA, aviation security was the responsibility of the air carriers and airports, Government and FAA performed a supervisory role.

After 9/11 the legal duty of such responsibility fell solely under the Government umbrella – aviation security became Federal responsibility managed by the TSA, Department of Transportation (ATSA Appendix C). Analyzing this fact it is obvious, that in such cases airports and governments put more effort to assure that screening is completed professionally.

Lastly, after 9/11 only the higher education holders had the possibility to be trained as screeners. 2002 USA Pilot Programme provided that screening personnel could consist of retired law enforcement officers[33]. So the New York City Police Department retires around 4000 officers each year the age of 40 or 50 – ensuring candidates for screening sector in airports. Concluding it is prominent to say, that screening process improved (e.g. lower screening turnover, better technologies, such as Backscatter X-rays, Trace-detection portals or "puffers", Quadrupole Resonance Scanning, or Polygraphs[34], several screening levels) and more attention was paid for screeners' training after 9/11. This could be the core point to ensure that perpetrators are kept from breaching security checkpoints and gaining access to secure airport areas or to aircraft.

Aviation security matters were examined initially in this thesis because of necessity to create legal framework and practical efficiency overlook for following analysis of privacy rights and PNR data legal dilemma. While this chapter focused on aviation security under G8, ICAO, EU and USA positions, it does not purport to be a comprehensive analysis of the sector. It rather highlighted EU and US initiatives relating airline passenger data exchange. Privacy rights and PNR data transfer are crucial to be analyzed within aviation sector because in 21st century freedom of movement and traveling *per se* are closely related to the air transportation.

---

[33] Civil Aviation Security Financing Study, US aviation security // http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_7.pdf [retrieved May 29, 2008]

[34] **Backscatter X-rays** can trace the contours of a person's body and reveal any hidden objects, such as non-metallic weapons, plastic explosives or drugs. Some critics argue these devices reveal too much and are an invasion of privacy, though filters can be added to protect a passengers' modesty.

Trace-detection portals or "puffers" can be used to detect explosive residue on a passenger by blowing small bursts of air at the person being screened. These puffs are designed to dislodge molecules from a person's body or clothing, and the air is sucked into a filter and analyzed fro suspicious substances. The same method may be used on baggage.

Quadrupole Resonance Scanning – a scanner bombards a passenger's suitcase with radio waves and examines the wavelengths of the energy emitted by the contents of the bag.

Polygraphs – or "lie detectors" are being used since 2006 for passenger screening. Passengers enter a booth, place one hand on a sensor and answer a series of questions on a touch screen. The sensor measures the blood pressure, pulse, sweat level analyzing them to determine if the person is lying. Definitions // http://www.cfr.org/publication/11397/targets_for_terrorists.html [retrieved May 11, 2008]

2. PRIVACY AND SECURITY DICHOTOMY

2.1. International legal regulation of the right to private life and privacy

Privacy is a fundamental right which appears so essential to the very human nature and so necessary for the constitution of the social and political bond, that it is absolutely compulsory to recognize that it enjoys a special legal quality and must be given a prominent status[35].

Universal Declaration of Human Rights 1948[36], Article 12 provides that "No one shall be subjected to arbitrary interference with his privacy…" Also Article 13 states that "Everyone whose rights and freedoms <…> are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity". Moreover, Article 8.2 provides exceptions when right to private life can be interfered by public authority in accordance with the law and if it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The International Covenant on Civil and Political Rights[37], in Article 17 guarantees the right to privacy in similar terms that no one shall be subject to arbitrary or unlawful interference with his privacy, nor to unlawful acts on his honor and reputation. Consequently from such provision everyone has the right to the protection of the law against such interference or attacks. The right to privacy is also protected in the Convention on the Rights of the Child[38] (Article 16) and in two regional treaties, the

[35] Protecting privacy/ Edited by Basil S. Markesinis. – The Clifford Chance Lectures Volume Four; Oxford University Press, 1999. – 74 p. – ISBN 0-19-826885-8

[36] Universal Declaration of Human Rights (1948). Articles 8, 12 and 13 // http://www.unhchr.ch/udhr/lang/eng.htm [retrieved November 29, 2008]

[37] The International Covenant on Civil and Political Rights (1966). Article 17 // http://www.unhchr.ch/html/menu3/b/a_cescr.htm [retrieved November 28, 2008]

[38] Convention on the Rights of the Child (1989). Article 16// http://www.unhchr.ch/html/menu3/b/k2crc.htm [retrieved November 28, 2008]

1969 American Convention on Human Rights[39] (Article 11.2 largely repeats Article 17 of the ICCPR) and the European Convention on Human Rights[40] of 1950 (Article 8 differs in terms stating that everyone has the right to respect for his private and family right…) Also, within the EU scope an important document concerning privacy is Charter of Fundamental Rights[41] (2000) with its Article 7 reiterated the definition of privacy given by the 1950 ECHR. Its Article 8 "Protection of personal data" explicitly defined fundamental right of data privacy: "everyone has the right to the protection of personal data concerning him or her" and the process of such data should be done in accord to the law, with the consent of the data subject and granting him/her a right to access to the data concerned.

In all mentioned legal documents, except EU Charter of Fundamental Rights 2000, there were no clearly expressed right to privacy on matters of personal data/ PNR data. But this right has to be understood as an implicit right flowing from the mentioned articles. Whether information is gathered and held by public authorities or private parties, everyone should have the right to ascertain whether information concerning them is stored, and if so, what information it is and for what purpose. Moreover it is necessary to ascertain who is controlling the access to their personal data; who is correcting inaccurate information or is eliminating it if unlawfully maintained[42].

In present century protecting privacy gets extremely essential target, because borderless world assures the flow of information in rapid and uncontrollable terms. Term *"borderless world"* is used because of EU Shengen set provisions; because of globalization and the outsourcing of economic actors entrains an ever growing exchange of personal data and because of the Internet. Also security pressure in the name of legitimate fight against terrorism opens the access to a significant number of data to an increasing number of public authorities. And finally because of the digital society (biometrics, networks) accompany everyone at each stage of life. In all these mentioned cases it is visible rather vague line between privacy and publicity.

---

[39] American Convention on Human Rights (1969) // http://www.oas.org/juridico/English/treaties/b-32.html [retrieved November 28, 2008]

[40] European Convention on Human Rights (1950)// http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf [retrieved November 28, 2008]

[41] The Charter of Fundamental Rights of the EU of 2000 did not have a binding power on the member states but had more symbolic nature, combining EU's fundamental principles of human rights. In December 2007 the Treaty of Lisbon gave this Charter a legally binding feature, enabling the Union to ensure that human rights, including the right to privacy, would be enforced in the framework of both the Council of Europe and the EU. OJ C 364, 18.12.2000, P 1-22.

[42] See Marks S., Clapham A. International human rights lexicon. – Oxford university press, 2005. – 264-265 p. – ISBN 0-19-876413-8

For many centuries it has been the practice of governments to collect and store information about individuals living within their jurisdictions. Personal information is to be considered as extremely sensitive, because it relates to matters as a person's financial status, medical or mental history, employment record and etc.

Since the first Data Protection Act in 1970 of the State of Hesse in West Germany, the rest of international community focused also on passing similar legislation concerning personal data protection. In 1981 Council of Europe passed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[43], which was the first legally binding international instrument with worldwide significance on data protection. With the aim to extend the safeguards for everyone's rights and fundamental freedoms, particularly the right to respect for privacy, taking into account of the increasing flow across frontiers of personal data (preamble of the 1981 Convention). Article 7 states that it is necessary to take security measures "for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alterations or dissemination". There should be specific security measures for different files taking into account its degree of vulnerability. But still it has no difference whether personal data is used within national State's jurisdiction or in international arena, same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their privacy rights and interests (information flow regardless frontiers also refers to article 10 of ECHR[44]; article 19 of ICCPR).

According to the Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETC No 108)[45], in practice protection of persons grows weaker when the geographic area is widened. Also having regard to the rapid evolution of information handling techniques and the development of international data traffic, it is necessary to have international agreements and created mechanisms between states to enable them to keep each other informed and to consult each other on matters of data protection.

EU and USA perspectives on data protection and privacy are different. This causes legal problems for EU to transfer PNR data to the US. Firstly, US prefer a "sectoral" approach to data protection legislation, relying on a combination of legislation, regulation and self-regulation, rather

[43] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)// http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm [retrieved December 5, 2008].

[44] See footnote 40.

[45] See footnote 43.

than overarching governmental regulations. According to former US President Bill Clinton and former Vice President Al Gore recommendations of 1 July, 1997 "Framework for Global Electronic Commerce"[46], private sector should lead and all companies should implement self-regulation in reaction to issues brought on by Internet technology. Moreover, where government involvement is needed, its aim should be to support and enforce a predictable, minimalist and simple legal environment for electronic commerce. So relating to the data privacy, accordingly to Clinton-Gore recommendation consumers have to be informed which personal information is being compiled about them and recommended that they would provide with limit use of that personal data.

However, above mentioned recommendation stated that existing European data privacy laws are to be voided, since they may hinder the development of electronic commerce. US consider that EU privacy legislation can arise when certain sectors and circumstances require. And also argue, in its part II section 5 "Privacy"[47] that "the United States will continue policy discussions with the EU nations and the EC to increase understanding about the US approach to privacy and to assure that the criteria they use for evaluating adequacy are sufficiently flexible to accommodate our approach". Till present situation, the US has not issued single, overarching privacy law comparable to the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Also it is known why Europeans have legal concerns of adequate protection of personal data and its decent storage. During World War II fascist and post-War Communist regimes Europeans faced danger associated with uncontrolled use of personal information and were rather suspicious and fearful for unchecked used of personal information. The disclosure of race or ethnicity led to secret denunciations and seizures that sent friends and neighbors to work/concentration camps. These faced atrocities were directly related to privacy and the release of personal information inconceivable to most Americans. Relating to such severe historical experiences Europeans have the right to demand of high standards for their personal information protection. Bus as it will be seen from following chapters, US still can not grant adequate level of protection of such information. Additionally US intention to strike a balance between creating adequate level of data protection and to maintain security mostly fails, because of too much attention to the letter. This US "security above all" system can be seen from the following exemplary case.

---

[46] Framework for Global Electronic Commerce by President W. J. Clinton and Vice President A. Gore Jr. P. 14 (1997) // http://isis.ku.dk/kurser/blob.aspx?feltid=196532 [retrieved October 20, 2008]

[47] Ibid P. 12- 14.

According to BBC news[48], the passenger, a Chinese man, was detained in San Francisco airport after security officials spotted him wearing electrically warmed shoes. Those shoes contained batteries, wires and a heating device designed to keep his feet warm. Since the man could not speak English he was unable to explain this kind of personal possession and its necessity. Consequently bomb squad officials blew up the shoes in a remote corner of the airport without any precise examination of the situation. This conduct embodies violation of persons' right to private life. Everybody has the right to possess goods, which are necessary and available or accessible for him/her. But in contrary, law demands equilibrium of rights and duties of individual. An individual never has absolute control over own privacy. If individuals do have the freedom to organize life as they please, this will only remain self-evident up to the point that it causes social or inter-subjective friction. At that point, the rights, freedoms and interest of other, as well as the prerogatives of the authorities, come into play. The friction and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance.[49] Interference into right to privacy (restriction) can be justified only if it meets with 3 criteria: legitimacy, reasonability and proportionality. Interference has to be based on legal grounds; its objective must be legitimate. Article 52 of the EU Charter of Fundamental Rights requires that any restriction to the right to respect for private life be in accordance with the law. Also the conditions under which the restriction is imposed must be reasonable and crucial for achieving certain public aim (under the subject of this thesis, it is the task to examine whether collecting and transferring PNR data from EU to US indeed helps to ensure aviation security and combat terrorism or it is solely ineffective measure violating privacy rights). Finally, the means chosen must be proportionate to the end pursued so that they can be considered necessary and genuine. A disproportionate infringement of the right to respect for private life and privacy is not allowed, even for the sake of achieving highly desirable objectives, such as overall security[50]. So only interference which is necessary to achieve a legitimate objective is proportionate.

Additionally to above mentioned 3 criteria (when interference into right to privacy can be justified) Rousseau's classic example of the republican stand has to be mentioned. Philosopher claimed

---

[48] See footnote 9.

[49] Privacy and the Criminal law/ Edited by Eric Claes, Antony Duff and Serge Gutwirth. – Intersentia, 2006. – 74-75 p. – ISBN 9050955452. See also Walters G. J. Human rights in an information age/ A philosophical analysis. – Toronto, Buffalo, London: University of Toronto press, 2001, p. 134. – ISBN 0-8020-8550-4

[50] European Union agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes (2208) // http://fra.europa.eu/fra/material/pub/discussion/FRA_opinion_PNR_en.pdf; [retrieved October 28, 2008]

the need for the citizen to participate in the public sphere to achieve "true freedom" (correlatively having rights) and warned that private concerns (correlatively absolute rights without interference or restrictions) threaten the functioning of good government. "The rise of self-interest would mean the end of the state", claimed Rousseau[51]. Moreover self-interest would lead to total destruction of society and there would be no possibility to implement control mechanism in order to preserve aviation security or security in general.

Consequently right to privacy can not be absolute[52]. In researched case about electrically warmed shoes this meant that individual by possessing some goods had a legal obligation not to pose any risk or threat to society. But here was indeed no balance. Firstly while checking the watch list of potential terrorists - detained Chinese man was not on it. Secondly, the man was not provided any Chinese- English interpreter to explain about his unusual shoes; on the other hand security officials had a legal obligation to investigate his health condition, maybe shoes were necessary to avoid any possible risk to his health, caused by getting his feet frozen. Lastly, the passenger still had the right to posses these electrically warmed shoes – security officials supposed to offer him to put these shoes into check-in baggage[53]. Without such proposal bomb squad officials blew up the shoes. This action was taken without clear identification of any potential threat, only mentioning by San Francisco airport spokesman M. McCarron that "it turns out it was some kind of heated shoe of some type – I don't know what that means-but they have run the passenger's name through records and it comes up clean right now".

This case clearly shows the disbalance between aviation security and its used precautionary measures and preservation of human rights - precisely persons' right to privacy. And this statement can not be denied upon the fact, that San Francisco airport had previously faced a similar case of detected explosive shoes, or recall the Paris, Charles De Gaulle International Airport precedent with Richard Reid[54]. Every case should be solved on individual ground, not correlating with any previous, even if it

---

[51] See footnote 49.

[52] Walters G. J. Human rights in an information age/ A philosophical analysis. – Toronto, Buffalo, London: University of Toronto press, 2001, p. 134. – ISBN 0-8020-8550-4

[53] Ideas generated through the interview with Lithuanian Civil Aviation administration officers.

[54] **Richard Colvin Reid**, the terrorist on the US watch list, who attempted to destroy a commercial Boeing 767 Paris, France - Miami, USA by detonating plastic explosives hidden in his shoes (the same kind Boeings were used as weapons of mass destruction in the terrorist attacks of 11 September, because they are known to be easily controlled and has huge patrol storage while on flight). This incident was the ground for new rule in the airports' check point to require passengers to take

is related to security issues. Concluding in this case taken measures were neither reasonable, nor proportional, nor based on any certain legal norm.

2.2. Legal focus on privacy rights: Directive 95/46/EC and EC Regulation 45/2001

Directive 95/46/EC[55] 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 defines personal data as "any information relating to an identified or identifiable person- data subject; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[56]". This concept in later chapters of the thesis will be analyzed together with PNR data, recognizing those two data elements so relevant to the thesis: personal data is for examining privacy rights and PNR data is for concretizing legal dilemma in aviation security and human rights sphere.

Continuing to the Directive, it embodies main data protection principle: Member States are required to provide that a transfer of personal data to third country may only take place IF the third country in question ensures an adequate level of data protection. Also it must be guaranteed that Member State's laws, which comply with the other provisions of this Directive, are respected prior to the transfer. 56-57 recitals of the Directive 95/46/EC emphasize that (56) *whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection <…> (57) whereas <…> the transfer of personal data to a third country which does not ensure an adequate level of protection* must be prohibited.

An exceptional clause is granted in the Article 26 (2) where Member States can authorize a transfer of personal data to third countries which do not ensure an adequate level of protection. Such action is permitted only under appropriate contractual clauses also by the Commission Decision

---

off their shoes. **CNN news**. Suspect in shoe bombing case indicted (January, 17, 2002) // http://edition.cnn.com/2002/LAW/01/16/reid.charges/?related%20%0D%0D [retrieved October 19. 2008]

[55] OJ L 281, 23.11.1995 P 0031-0050

[56] Ibid. Article 2

2001/497/EC[57], which provides cases when such transfer is necessary: safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others[58]. Correlatively with Directive 95/46/EC thesis mentions also Organization of Economic Co-operation and Development Guidelines which aims also to harmonize national privacy legislation and at the same time to prevent interruptions in international flows of data[59]. EU Member States and US are Contracting Parties to this Organization, so those Guidelines are to be binding. Consequently transfer of personal data to third countries can be affected only in full compliance of the mentioned Directive 95/46/EC provisions.

Its 5 key principles[60]:

1. Legitimate purpose: Data must be processed for a specific purpose and subsequently used or further communicated only if not incompatible with the purpose of the transfer. Article 6.1b defines that EU Member States shall provide that personal data is collected for specified, explicit and legitimate purposes. Other kind of data usage (for historical, statistical or scientific purposes) shall not be understood as incompatible with the purposes IF Member States provide appropriate safeguards. Legitimate use of personal data guarantees safe air transportation and reduces threats to aviation security. Supporting this principle of Directive 95/46/EC, it is crucial to mention OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. As EU is a Member to this Organization, it has adopted those guidelines and incorporated it in its privacy laws. Article 7 of the OECDG defines there should be limits to the collection of personal data and it should be obtained by lawful and fair means[61].
2. Data quality/ proportionality: Personal data should be accurate and kept up to date, also adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed. This provision is repeated in OECDG Article 8. All inaccurate or incomplete data should be erased or rectified (Article 6.1c, d). Within proportionality element, Article 6.1e provides that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected

[57] OJ L 181, 04.07.2001 P 0019-0031

[58] Ibid. Appendix 2.

[59] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)// http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [retrieved October 17, 2008]

[60] See footnotes 55 and 57.

[61] See footnote 59.

or for which they are further processed". Also again added the necessity for appropriate protection mechanisms if data is stored for longer periods. Article 8.5 emphasizes extra restrictions to data collectors to provide "suitable specific safeguards" for extremely sensitive data, which still has to be provided (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs etc). Again this proves that the US on one hand is expecting PNR data to be transferred from EU for aviation security reasons; on the other hand it is not providing specific and extremely competitive protection mechanism. This fact is questionable, why US is delaying to eliminate loopholes in its privacy laws in order to be compatible with EU ones. Even though US is binding with OECDG on the protection of privacy and transborder flows of personal data. There would be no PNR data dilemma if US have complied with its legal privacy commitments.

3. Transparency: In article 10 and 11 of the Directive[62] it is provided the obligation to Member States to inform the data subject when his personal data are being processed to guarantee fair processing in respect of this subject. Those mentioned articles should be analyzed closely with the Article 7 of the Directive, which provides with special circumstances when personal data can be processed (e.g. when data subject unambiguously gave his consent, when processing is necessary to comply with a legal obligation to which the controller is subject, when it is related to vital interest of the data subject and etc.) Finally under the Directive it is unquestionable right for data subject to have possibility to access all data processed about him and the right to rectification of the data where they are shown to be inaccurate (article 12). Correlatively with OECDG Article 13 it is defined that individual has the right to obtain from a data controller any data relating to him and be informed what data has been collected.
4. Security mechanism: for this thesis Article 17 is of great significance and must be noticed. Article 17.1 defines that *the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network...* (Correlatively with OECDG Article 11 and 16) This article is the leading one while arguing any passed agreements between EU and US on PNR data transfer[63]. Once again, US do not ensure a level of security

[62] See footnote 55.

[63] See Chapter 3.3

appropriate to the risks which might occur while processing and using such data[64]. Article 17 has to be viewed together with the Article 28. Assuring security to the personal data, supervisory authority has to be provided- such independent body that will monitor the data protection level, give advices to the state organs about administrative measures and regulations, also that supervisory authority should start legal proceedings when data protection regulation has been violated. Article 28.4 provides that "Each supervisory authority shall hear claims lodged by any person<…> concerning the protection of his rights and freedoms in regard to the processing of personal data…" Accordingly to this, Directive 95/46/EC permits individual complaints about violations to the supervisory authority or in a court of law. This provision is totally positive in the sphere of person's right to privacy; it guarantees persons right to make claims for the breach of his private life elements: personal information and his other records. Moreover under the Article 29, European Commission has competence to set up "Working party on the Protection of Individuals with regard to the Processing of Personal Data", commonly known as the "Article 29 Working Party"[65]. Acting on advisory status and independently (Article 29.1) it shall give the Commission an opinion on the level of protection in the Community and in third countries (Article 30.1b). In the following section 5 it will be provided in details about the "Article 29 Working Party" achievements.

5. Transfer of personal data to third countries issue. The term *"third countries"* are to be understood as countries outside the European Union. The US mainly is in favor of this term for current analysis. Personal data processing, according to the Article 25 of the Directive 95/46/EC, "may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection". This includes safe data transfer operations, safe maintenance and strict supervision of such data from unauthorized subjects. Thus, although Article 25 lays down the basic rule, Article 26 contains derogations, allowing controllers to transfer the personal data notwithstanding lack of adequate protection. Such transfers still can be made if one of conditions applies: e.g. where data subject has given consent or where the transfer is related to a contract involving the controller. Transfers may also be allowed where sufficient safeguards are adduced by the controller or on the basis of

[64] Statement based on http://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf [retrieved October 20, 2008]

[65] OJ L 281, 23.11.1995 P 0031-0050 and OJ L 201, 31.7.2002, P. 37- 47 Article 15.

approved contractual terms[66]. Apart of all mentioned above there occurs several questionable situations, related to the US. Firstly, provisions in US laws[67] that CBP and TSA can share PNR data with other federal agencies related to the countering terrorism functions. US provisions pose risk for data misuse meaning that the US can unilaterally decide over the PNR data transfers within its agencies, so use uncontrollable. Secondly, in the matters of how the PNR should circulate EP criticized the US "pull" system[68], which consisted in granting CBP full access to the European databases to collect PNR. This could definitely have endangered EU citizens' privacy rights, because in such case the US has uncontrollable capacity to access any possible data. For this reason European Parliament favored a "push" system, where the air carriers would send the PNR data to the US upon request, which would reduce the control and access of the US government. It has to be pointed out that from a data protection point of view a "push" system is the only acceptable way of transferring personal data with less possible violations of right to privacy.

Consequently cross-border exchange of personal information, particularly between the US and Europe, has posed difficult questions about the meaning and scope of the EU Directive. How these countries should understand term "adequate protection", and would companies based in US, Latin America, China etc. be able to satisfy the adequate protection criterion through contractual agreements with their European counterparts?[69] Those and many other similar questions were opened for "Article 29 Working Party".

In close subordination to the Directive 95/46/EC and OECDG it is prominent to mention Regulation EC No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[70]. Even though it is applied for EU institutions and bodies and does not include the US institutions, it is still useful to include this Regulation in the thesis, because it closely correlates with the Directive 95/46/EC and improves data protection legal

---

[66] See Data Protection law/ Second edition by David Bainbridge. - Saxon Graphics Ltd, Derby, 2005. – 20 p. – ISBN 185811-342-3

[67] Aviation and Transportation Security Act 19 November, 2001.
http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf

[68] See PNR data Agreements in Chapter 3.3.

[69] See Walters G. J. Human rights in an information age/ A philosophical analysis. – Toronto, Buffalo, London: University of Toronto press, 2001, p. 121-125. – ISBN 0-8020-8550-4

[70] OJ L 8 12.1.2001 P 0001-0022

considerations. Regulation provides several novelties to European data protection mechanism (not mentioned in Directive 95/46/EC). Article 41 of the Regulation EC No 45/2001 creates the European Data Protection Supervisor- an independent supervisory authority[71], which is responsible for ensuring respect of fundamental rights and freedoms of natural persons and in particular their right to privacy. Also, EDPS has crucial role to monitor and ensure the application of the provisions of the Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by EU institutions or bodies with the exception of the Court of Justice of the European Communities acting in its judicial capacity. Also meaning that in correlation with above analyzed "Article 29 Working Party" EDPS has authority to deal with PNR data issues between EU and US.

Another element to improve Directive 95/46/EC effectiveness by Regulation EC No 45/2001 was provided in Article 32.2 which gave legal ground to every data subject to lodge a complaint with the EDPS if his or her rights under Article 286 of the Treaty on EU[72] have been infringed as a result of the processing of his or her personal data. European Court of Justice has jurisdiction to hear all disputes related to such complains, including claims for damages. Article 32.4 also adds that subject who has suffered damage because of unlawful processing operation or any action incompatible with Regulation EC No 45/2001 shall have the right to have the damage made good in accordance with Article 288 of the EU Treaty.

Concluding in European privacy legislation Directive 95/46/EC has substantial meaning, because it sets up main rules how personal data should be treated and protected. With 5 key principles of the Directive and additionally issued EC Regulation No 45/2001 EU has created high level of data protection mechanisms, which should ensure that no violations can be done to right to privacy.

2.3. Safe harbor principles

"Article 29 Working Party" and US Department of Commerce proposed "Safe Harbor" plan to bring US companies up to a minimum level of compliance with the EU Directive 95/46/EC. The issuance of European Council Decision of 27 July 2000[73] had to prove the legitimacy of "Safe Harbor" provided principle of ***adequate protection*** in accordance with the mentioned EU Directive (Article 25.6). Recital 5 of the Decision defined that adequate level of protection for the transfer of data from

[71] Ibid Article 41, 44 and 46.

[72] OJ C 321E, 29.12.2006, P 0001-0331.

[73] OJ L 215, 25.8.2000. P 0007 –00 47

the Community to the US should be attained if organizations comply with the safe harbor privacy principles for the protection of personal data transferred from EU to the US. Talking about Safe harbor principles[74] it provides for US and EU companies cheaper and simpler means for complying with the adequacy requirements of the Directive.

US companies could opt into the program as long as they adhere to the Directive 95/46/EC and to 7 Safe Harbor principles outlined: 1) Notice – persons have to know the purpose for which the company collects and uses their data; 2) Choice – or the option to choose whether or how their personal information will be disclosed to a third party, this principle stipulates an "opt-out" policy and in case of sensitive information – an "opt-in" policy.3) Onward Transfer – data transfers can be concluded only following the adequate data protection principle; 4) Security- those measures have to be taken by organizations creating, maintaining, using or disseminating personal data, to say- it has to be made reasonable effort to prevent any possible harm for collected information. 5) Data integrity – data must be relevant and reliable for the purpose it was collected for. 6) Access – Individuals must be able to correct, amend, or delete any personal information if it is inaccurate. But this right of access is not absolute. Obligation of an organization to provide access to PNR data is subject to the principle of proportionality or reasonableness and has to be tempered in certain cases. 7) Enforcement – this mechanism must be effective in order to ensure its compliance. In general, enforcement will take place in the US in accordance with US law and will be carried out primarily by the private sector and where necessary by government enforcement of federal and state unfair and deceptive statutes, giving a participating organization's commitment to the Safe Harbor the force of law.

Transatlantic willingness to diminish privacy laws difference and aim to improve cooperation on PNR data transfer led to adoption of the Safe Harbor principles. This legal act can be considered as one of many trials to solve US EU dilemma on privacy and security. Arguments whether it is effective or not flows from the fact that decisions by organizations to qualify for the safe harbor are entirely voluntary and organizations may qualify for it in different ways. Consequently this options allows privacy laws to be treated differently also.

[74] Ibid.

3. PNR DATA. EU-USA LEGAL DILEMMA

3.1. PNR data as an object of aviation security

The terrorist attacks of 11 September in New York and Washington DC have led to major changes in the way security matters are handled throughout the Western world, and especially in the United States. According to scholars US taken security measures were draconian comparing of those from other countries[75]. Clearly the tragedy recalled the need to monitor and control internal flights, and international flights into, out of and over the US has required the collection and analysis on those passengers data on aircraft.[76] Passenger name record data[77] is an extensive data set held in airline computers when a travel reservation is made. Legal subjects for accessing PNR data are the US Bureau of Customs and Border Protection within the jurisdiction of DHS and TSA. The debate concerning PNR started in 2001, due to the US Aviation and Transportation Security Act[78], which was enacted the same year on November 19. This Act required that every air carrier make PNR data available to the above mentioned authorities 72 hours prior to each plane's takeoff. Such ATSA legal provision visually can be seen in the Figure 1, which shows categories of systems on a chronological axis. PNR

[75] Oxford Journals, International Journal of Refugee Law, Volume 18, Nr 2. 2006. P 313-332// http://ijrl.oxfordjournals.org/cgi/content/full/18/2/313?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=1&title=PRIVACY+VS.+SECURITY&andorexacttitle=or&andorexacttitleabs=and&andorexactfulltext=and&searchid=1&FIRSTINDEX=0&sortspec=relevance&resourcetype=HWCIT [retrieved October 7, 2008].

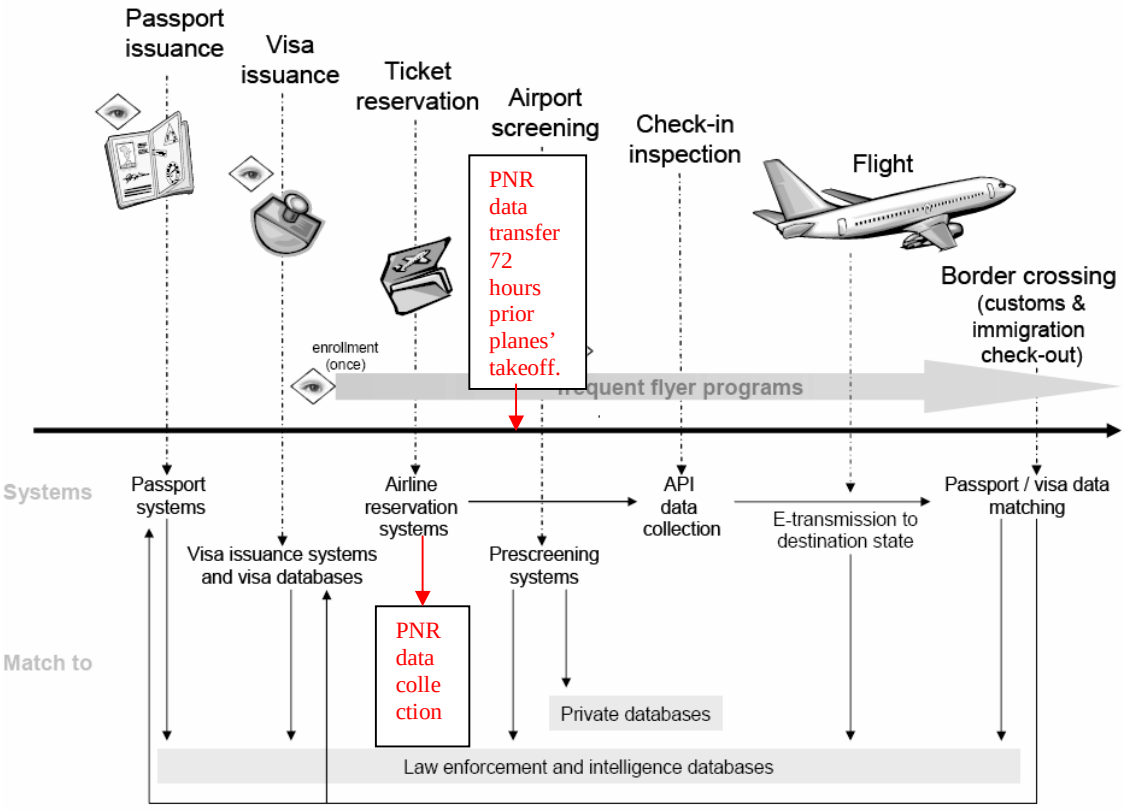
[76] The US Government and other governments have been using passenger lists to screen travelers and persons already on watch list or passenger of potential risks before they depart for long ago. Since 9/11 the focus has shifted to find potential terrorist who are so far unidentified by using more of the detailed information collected by airlines and travel agencies when person books a flight. These data contain information as travel itineraries and payment details, - this can be analyzed in conjunction with current intelligence to identify high- risk travelers before they board their planes. The problems arise when more information is collected than is needed for purpose of aviation security, standards of accuracy slip and the information is shared with those not responsible for counter- terrorism and is used for other purposes// http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf [retrieved October 18, 2008].

[77] See also "What's in a Passenger Name Record (PNR)?"// http://hasbrouck.org/articles/PNR.html [retrieved October 18, 2008].

[78] See footnote 4. Section 115. 1-5

data is collected at the ticket reservation moment (marked “PNR data collection”) and is transferred to US 3 days prior to foreseen flight (marked “PNR data transfer”).

Figure 1. **Categories of systems on a chronological axis**



Source: OECD : Background material on biometrics and enhanced network systems for the security of international travel (2004)// http://www.oecd.org/dataoecd/16/18/34661198.pdf [retrieved October 2, 2008]

Continuing the examination of ATSA, section 115.3 provides that carriers shall make PNR information available to the Customs Service upon request. Not complying with such requirements US declared to impose negative measures[79]. Consequently to this regulation PNR data legal dilemma began between EU and US.

Researching PNR elements it can be noted that required data gives information about passenger’s **history, conduct and behavior**. This system divides people into two categories – more

[79] See footnote 64, P 1.

trusted and less trusted. According to Bruce Schneier, also the third category appears between those two: untrustworthy people whom there is no reason to mistrust. And from such category all this potential threat can arise, meaning that some people going to commit a terror attack might have no previous link to terrorism[80]. So PNR data would not be effective to ensure aviation security.

Other disputable aspect of PNR is the amount of its elements. PNR can contain as 60 data fields or separate pieces of information such as: address, email address and contact telephone; travel agency and agent, form of payment, seat number and seat information; frequent flyer information, general remarks etc. This may lead to inaccuracies. So it remains unclear why PNR data should include all above mentioned elements. This information can not be useful at all times: e.g. when potential terrorist is using his uncles' credit card, while on board he changes his seat, or in opposite – a decent citizen by mistake occupies a seat of a suspected criminal etc. Contrary, Jonathan Faull[81] stated that the more PNR Americans have the lower is risk of making mistakes while identifying potential criminals. Those controversial opinions makes PNR data dilemma of even greater extent.

Talking about the degree to which the collection, retention and transfer of PNR data is acceptable all depends generally on value in combating terrorism and other serious cross-border crime. It is important to evaluate, how much use it will be got for each amount of personal information, and if some parts of gathered information have no influence to reduce terrorism, then it is no need to demand for it. In all cases gathering personal information is intrusion into persons' private life so it is suggestible to require as less personal information as possible. Another element to be mentioned is the importance of PNR data to be accurately collected and correctly analyzed. Inaccurate PNR data can provide a false identification and attribute to an individual conduct and behavior which is not his. E.g. Osama bin Laden is worldwide known terrorist, who presumably can pose high risk for aviation and for national security of any state. But his brother Yeslam bin Ladin (who changed his surname from bin Laden for security purpose not to be combined with his terrorist brother, never involved in terrorist activities, and long ago not in contact with Osama bin Laden[82]) can always expect double check on his PNR, and face many inconvenient situations while in airport.

---

[80] Schneier B. Our data, ourselves//http://www.schneier.com/essay-207.html [retrieved November 10, 2008]

[81] The head of the Commission Directorate General on Justice, Freedom and Security (JLS). See EU Committee 21st Report of Sessions 2006-2007 // http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf [retrieved November 10, 2008]

[82] Bin Laden family// http://en.wikipedia.org/wiki/Bin_Laden_family [retrieved October 18, 2008]

Also, there are several persons named Richard Reid. Only one is a dangerous terrorist included on the US watch list and who has already been sentenced to life imprisonment[83]. Another exact name holder is the US Entertainment journalist[84]. Lack of attention on PNR data subsequent elements but name can violate rights not only on privacy but also right to free movement.

The last example to be mentioned is Senator Edward Kennedy, who was once forbidden to land in the US because he shared a name with an individual on a watch list. Security rules did not allow him to be told at airport why he was being denied a ticket, but being a US senator helped the problem to be resolved easy[85]. An ordinary person would have faced more problems: would be taken aside, kept in detention until the investigation of true identity is over. This arbitrary detention is obvious violation of human rights, which can appear from incorrect PNR data analysis. As it correlates with the above mentioned, PNR data incorrect analysis and the watch list itself pose great danger. In legal ambit these errors are called Type I or *false positives*[86] errors, occurring when a system erroneously signals a match: someone with no affiliation to terrorists is flagged by the Secure Flight system and either subjected to additional screening measures, detained, and/or denied aircraft boarding.

3.2. Is equilibrium possible between security and privacy within PNR data scope?

When there is a major difference in the legal philosophy of personal data between the US and Europe it is fundamental difficulty in the negotiations to be concluded[87]. The first one is not constrained by comprehensive privacy legislation and relies on a mix of legislation, regulation and self regulation. Also it puts priorities on security of the citizens and the territory to the first place to the detriment of civil liberties. By ATSA Section 115.3 US stressed that security is a crucial element, but

[83] See Footnote 54.

[84] Journalist Richard Reid// http://today.ninemsn.com.au/article.aspx?id=182006 [retrieved October, 19, 2008]

[85] Watch-list "Justice" by John R. Lott and Sonya D. Jones as published in the Washington Times, 2005// http://209.85.135.104/search?q=cache:OZcVLrE1A98J:www.gunowners.org/op0514.htm+Senator+Edward+Kennedy+SHARES+THE+SAME+NAME+ON+THE+WATCHLIST&hl=lt&ct=clnk&cd=10&gl=lt [retrieved October 18, 2008]

[86] Congressional Research Service Report: Homeland Security: Air Passenger Prescreening and Counterterrorism (2005) P. 18// http://www.au.af.mil/au/awc/awcgate/crs/rl32802.pdf [retrieved October 12, 2008]

[87] Statement of Mr. Alex Turk, the Chairman of Europol's Joint Supervisory Body (JSB) (2002). Nolan S., EU Security versus Civil Liberties: the case of PNR data transfer, BISA Annual Conference, Cork 2006, P 2// http://www.bisa.ac.uk/2006/pps/nolan.pdf [retrieved October 25, 2008].

have not included any reference how to balance this provision with privacy rights and especially rights of foreign citizens.

Considering about EU it focuses more on balancing between security and privacy, emphasizing greater importance to civil liberties. Moreover, EU acts according to privacy rights legislation and harmonized privacy laws. On the other hand as it will be noticed from later chapters, EU got assimilated in some part to the US "security above all" approach, because it was unable to conclude effective PNR data Agreements, which would have adequately safeguarded privacy rights[88]. Thus both of them have the same target - combating terrorism while improving transatlantic cooperation in security sector. Even though of such target and willingness to diminish uncertainty among themselves by several Agreements and Safe Harbor principles, EU and US face difficulties.

Examining other reasons why EU and US came up with PNR data transfer legislation, it can be stated, that the US used political and economic pressure while promoting the adoption of a policy reflecting American interests. The US warned EU in case of non compliance it would use economic sanctions against the EU and may abort air transportation contracts, this way breaching persons' right to freedom of movement[89].

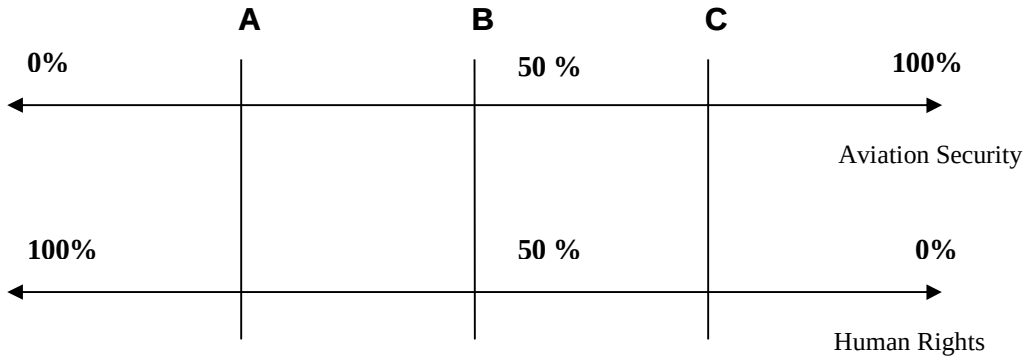
After all mentioned above the main point can be debated: is it possible to balance between security and privacy, having both security AND privacy, diminishing the security OR privacy dilemma within the scope of PNR data transfer necessity?

To examine this dilemma I have consulted with Lithuanian Civil Aviation Administration Officers: the Chief of Aviation Security department Juozas Žėkas, Chief Assistant of Passengers screening department Ričardas Martinaitis and Chief of Aviation Security department within Civil Aviation Administration Tomas Montvila. They provided a scheme, obviously showing three grand phases of possible security and privacy correlation. See the Figure 2 below:

[88] See Chapter 3.3/ 3.5.

[89] Privacy International and ACLU call for repeal of EU-US agreement on data transfers// http://209.85.135.104/search?q=cache:0FJLP4MsI1oJ:www.privacyinternational.org/article.shtml%3Fcmd%255B347%255D%3Dx-347-548477+US+POSES+RISK+FOR+EU+WHILE+PNR+DATA+PROTECTION&hl=lt&ct=clnk&cd=1&gl=lt; [retrieved October 26, 2008].

Figure 2. **Aviation security and Human rights correlation**



Brief explanation. Phase A – treating human rights at maximum level (close to 100%, but never absolute 100%) always results minimum level of aviation security (or security in general). In this phase human rights (right to privacy) are more important than security[90]. Consequently, this phase is of potential danger if combined with 0% of security model so purely never occurs. For this thesis phase A is not relevant.

B - This is the essential phase. Balance between human rights and security issues. Both human rights and security should lead. Designing security into systems from the beginning would give decent level of security human beings need while preserving civil liberties. While focusing on PNR data collection and transfer between EU and US, it is imperative to adopt proper legislation and ensure valid practice on adequate safeguards of PNR data. This private information should have real safeguards and not solely legal provisions on how PNR data has to be treated and protected[91]. E.g. it is better to have intelligence agents squatting on the ground in the Middle East arguing the Koran, and not sitting in Washington arguing about wiretapping laws or restricting fundamental rights in order to ensure own security. Privacy and security should be improved in parallel[92].

C – Aviation security is on maximum scale while human rights decreased till minimum. Obviously, this situation can be possible in military concerned country. According to Amnesty

[90] High Commissioner for Human Rights Louise Arbour statement// http://www.amnestyusa.org/document.php?id=ENGIOR400192008; [retrieved October 26, 2008].

[91] See Chapter 3.6.

[92] See generally Waldron J. "Security and liberty: The image of Balance" / The Journal of Political Philosophy: Volume 11, No.2, 2003, 191-210 p. // http://www3.interscience.wiley.com/cgi-bin/fulltext/118847768/PDFSTART [retrieved October 26, 2008]

International's brief survey on September, 2008 there is no doubts that following 11 September, 2001 attacks in the US and later attacks in London and Madrid, a wide range of counter-terrorism laws, policies and practices have eroded human rights. In order to create "security above all" system human rights were heavily restricted. Even if it was legal (because implemented under legal provisions) and reasonable, but it was not proportional. Governments claimed that security can be achieved by violating the rights of others.

Examining EU and US positions on security and privacy balance level, looking within PNR data scope, it will be initially overviewed statistical reports. According to the Rasmussen Reports of January 18, 2008, 51% of Americans said that security is more important than privacy. 29% of respondents disagreed stating that privacy is more important than security. 20% were not sure[93]. This report has proved that Americans are indeed influenced by the Bush administration's "security above all" vision. Moreover US intelligence authorities have a notorious saying – privacy and security are a zero-sum game[94]. This means, that in order to maintain secure and strong state (+1) it is necessary to intervene into privacy field (-1). The sum is 1+ (-1) = 0. On the other hand it is easy to understand – they- Americans faced severe occurrences of 9/11. Consequently from such statistics it can be noted that US policy is relevant to phase C. Lithuanian Civil Aviation Administrator Officers are also of such position, that in order to have effective aviation security system privacy rights have to be interfered. Even thought legal intervention is allowed it supposed to cause as less damage as possible to fundamental rights.

Also according to Eurobarometer survey on the privacy issue by European Commission of April 22, 2008[95] respondents from 27 EU countries were interviewed. A fight against international terrorism was an acceptable reason to restrict data protection rights (understanding this as security more important than privacy). 80% agreed that it should be possible to monitor passenger flight details, 70%- even telephone calls if these actions served to combat terrorism. Other respondents stated that this should be done within clearly defined limits: 30% of respondents stressed that only suspects should be monitored, while between 19% and 30% of respondents wanted even stricter safeguards, involving the judiciary. Even though this statistics show that Europeans also think that security is important, but

[93] Rasmussen Reports// http://www.rasmussenreports.com/public_content/politics/current_events/general_current_events/51_say_security_more_important_than_privacy [retrieved October 26, 2008]

[94] Wright L. The Spymaster. Can Mike McConnell fix America's intelligence community? (2008) // http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright[retrieved October 26, 2008]

[95] Eurobarometer // http://www.libertysecurity.org/article2006.html; [retrieved October 26, 2008].

nonetheless they point out the importance of privacy. At this point EU security and privacy policy is relevant to dichotomy of B and C. In this thesis it is presumed that EU is of such policy to embrace security AND privacy equilibrium, so adopting policies which restricts civil liberties the least.

Indeed, collecting PNR data and transfer it to the US in order to enhance security would not harm privacy if the data collected is protected by appropriate safeguards. Security and privacy are not inversely correlated, because e.g. as more PNR data is collected and wrongly interpreted or misused, as great danger will be caused both to security and to privacy. Meanwhile enforcing proper safety measures would give effect both to security and to privacy. Bruce Schneier, former US Government Secure Flight Working group on privacy and security specialist in contrary to US Intelligence stresses that privacy and security have to be displayed at a close link and balance must be ensured[96].

3.3. International agreements on PNR data: 2004, 2006, 2007

3.3.1. 2004 Interim PNR Agreement

Outside the Safe Harbor principles, air passenger data transfer caused widespread public concern over its privacy implications and so accelerated European Union to enter into negotiations with the USA. In May 2004 the CBP released its declaration of Undertakings[97] ensuring adequate protection for PNR data transferred from the Community concerning flights to or from the US. European Commission Decision 2004/535/EC[98] on adequacy allowed CBP officially adopt those undertakings. Consequently to these primary legal concerns European Community and the US reached the Agreement on the processing and transfer of PNR data by air carriers to the United States DHS and CBP. The conclusion of this Agreement was authorized by Council Decision 2004/496/EC[99] on the

[96] See Schneier B. Protecting privacy and Liberty-Crypto-Gram Newsletter (2001)// http://www.schneier.com/crypto-gram-0109a.html#8; [retrieved October 26, 2008]. See also Waldron J. Security and liberty: The image of Balance / The Journal of Political Philosophy: Volume 11, No.2, 2003, 191-210 p. // http://www3.interscience.wiley.com/cgi-bin/fulltext/118847768/PDFSTART; [retrieved October 26, 2008].

[97] Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection, 69 Fed. Reg. 41543 (July 9, 2004) See OJ L 235, 6.7.2004 P.0011-0022

[98] OJ L 235, 6.7.2004 P 0011-0022 Based upon Article 25(2) of Directive 95/46/EC and included US 48 Undertakings.

[99] OJ L 183, 20.5.2004 P. 0084-0085

adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the US CBP (with explanatory elements and 48 Undertakings).

The main purpose of this 2004 Agreement was to collect PNR data in order to prevent and combat terrorism, transnational and other serious crime. The purpose for which the data will be used should be limited to fighting acts of terrorism without expanding their scope to unspecified "other serious criminal offences". It supposed to be exhaustive list of cases, when PNR data is being collected and for what reason. Wide nature of the provision leaves open for too many exceptions that can be used under the exclusive discretion of the US authorities. Consequently this discretion makes possibility to intervene in any possible sphere of persons' private life with excuses of combating terrorism.

Before completing negotiations, US sought to include 38 PNR data elements. The "Article 29 Working Party" under its Opinion 4/2003[100] accepted only 20 (including **No Show** history – where the passenger buys a ticket but does not travel; and **Go Show** – the purchase of a ticket at the airport at the last minute. The latter is an important element to be stored for PNR, because having in mind the last minute purchase *per se* and wide range of reasons why passenger buys a ticket so late). US later dropped the number of data elements to 34[101], referred in the 16 undertaking of the 2004/535/EC Decision[102]. As a matter of fact not including those which Working Party had thought as acceptable, meanwhile included 18 others "well beyond what could be considered adequate, relevant and not excessive" (such as OSI – Other Service Related Information, SSI/SSR – Special Service Information/ Special Service Requests). Recently mentioned elements belongs to the very sensitive PNR data field (e.g. passengers request for "halal food" clearly makes relevance that this is an Arabic person, according to Islam culture willing to consume only *permissible* food on board).[103]

According to the American Civil Liberties Union (ACLU) scholar Dr. Gus Hosein most controversial are elements 26 and 27, - the OSI information and the SSI/SSR information. From his statement it is clear that OSI and SSI/SSR is behavioral data and the US Government particularly seeks for this information and not because it is necessary to identify an individual, it is because the US wants to draw conclusions based on this data. Meaning that 26 and 27 elements were used in addition to get information about individuals' personality and behavior. Consequently under such requirements of

---

[100] Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data (2003)// http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_en.pdf [retrieved October 26, 2008]

[101] See ANNEX I.

[102] OJ L 235, 6.7.2004, P 11

[103] House of Lords: The EU/US PNR Agreement. Report 2006-2007, P 15// http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf; [retrieved October 19, 2008].

PNR data passengers could feel like *"supervised objects"* and the entire flight can be defined as strict observation of their particular movements and conversations. This obvious interference into right to private life and privacy can be examined together with another example, which also gives reference that individuals may feel like "*supervised objects"*. That is biometrics system, which is used in both EU and the US airports in order to identify individual while e.g. comparing fingerprints and prevent any possible threat to aviation security. E.g. fingerprints information and passengers' identities are being stored in central data base. Each time passenger is leaving to the US his/hers fingerprints are being checked. In some philosophical view it may seem that all passengers are treated as potential terrorists. Anyway traveler's identity must be checked, not in regard of "checking for the potential threat of terrorism", but for maintaining rules of safe air navigation and legality on board[104].

2004 Agreement provided treatment of sensitive data. In the Undertakings 9-10 it is defined, that "CBP will not use "sensitive" data[105] <…> and implement, with the least possible delay, an automated system which filters and deletes certain "sensitive" PNR codes and terms which CBP has identified in consultation with the European Commission". The US was bound with obligation to delete and not use "sensitive" data until such automated filers will be implemented. This filtering mechanism resembles together with the methods in general how the PNR can be accessed. Undertakings 13-14 embodies the "pull" system mode, meaning that CBP receive PNR data directly from the air carrier's reservation system for purposes of identifying potential subjects for border examination, whose travel includes a flight into or out of the US. As it will be observed in later Agreements, the same problematic system remains, and it was grave even in 2007 Agreement, which repeated intentions to implement "push" system: "DHS will immediately transition to a "push" system for the transmission of data <…>no later that 1 January 2008…" [106]. The "push" system is considered by the EU to be less intrusive from a data privacy perspective, and this system does not confer on airlines any discretion to decide when, how or what data to push, however. This decision is conferred on DHS by US laws.

Continuing to the 2004 Agreement another important element on PNR data is retention period. 16 undertaking states that such data will be retained for three years and six months; later it will be transferred by CBP to a deleted record file and retained there for 8 years more before being destroyed.

---

[104] Secured and sorted Mobilities: Examples from the airport, P 507// http://www.surveillance-and-society.org/articles1(4)/sorted.pdf [retrieved October 24, 2008]

[105] Data concerning racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning the health etc.

[106] 2007 PNR Agreement Section 2.

This is too wide provision. There should be no exceptions for saving data from deletion longer than necessary.

Very doubtful is Undertaking 35: *No statement in these undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any US legislation which materially affects the statements made in these Undertakings.* This generally means that changes in US law which require PNR data to be used for other purposes will override the Undertakings. Obviously US puts priority to its own legislation and leaves great doubts to EU, whether the agreement on PNR data issues has any importance to the US or it is concluding the agreement just in order to have future amendments for own benefits. The point of argument is that US has no strict legislation on issues concerned PNR data protection, supporting this argument on the facts flowing from previously analyzed Clinton-Gore Recommendations. Moreover, analyzing Constitutional provisions of both continents it is visible, that US has totally different point of view on right of privacy than EU countries (this statement was analyzed previously in chapter 2). On my opinion, Council should have not permitted this provision in its Decision, and it should have been corrected this way: CBP shall process PNR data received and treat data subjects concerned by such processing in accordance with *applicable European Union laws and its Member States constitutional requirements, without unlawful discrimination comparing to its national laws.* In this case the PNR data would be protected in an adequate level, as it is required in Directive 95/36/EC.

Finally, the illegality of 2004 Agreement can be proved under the fact that in September 2004, the European Parliament appealed to the European Court of Justice for the annulment of it, together with the annulment of the Adequacy Decision[107], arguing that they breached fundamental principles of Directive 95/46/EC also breached fundamental rights and principle of proportionality. EP did not agree with the Commission that the US authorities provided adequate privacy safeguards and above all Commission had no legal capacity to negotiate international agreements on behalf of EU.

Also European Parliament stressed 4 other arguments. First one, that the CBP is not understood as third country within the meaning of Article 25 of Directive 95/46/EC and has direct access to PNR data, not provided for by the directive. Second one – *the principles of the basic directive are infringed as regards the processing of sensitive data, the right of access and related rights, that is not guaranteed and the authorization transfer to other US authorities and other countries is incompatible with Directive 95/46.* The third argument based on the infringement of fundamental rights (right to

[107] OJ L 235, 6.7.2004 P11

private life and right of protection of personal data) laid down in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[108]. Last one is rather essential- that the decision infringed the principle of proportionality, in amount that PNR data can be transferred and kept by the US authorities for too long. As a consequence, ECJ ruled in joint cases C-317/04 and C-318/04 that Agreement cannot have been validly adopted on the basis of article 95 EC, read in conjunction with article 25 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement on such data so it has to be annulled[109].

Responding to such annulment US only stated its regret that the European Parliament narrowly decided to refer the PNR accord to the European Court of Justice, because they believed "the PNR deal with the Commission <…> [was] a good one…"[110]

2004 Agreement was only an initial on the EU- US cooperation on PNR data related issues. Consequently 2004 Agreement did not impose adequate protection for privacy rights, especially with such defined "pull" system, unclear PNR data retention periods, defined too wide scopes of PNR usages and information sharing with third US authorities.

3.3.2. 2006 Interim PNR Agreement

In 6 October 2006 second interim Agreement between the European Union (in previous Agreement the party was stated as European Community) and the US on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security was reached[111].

Most significant point- that interim agreement enables PNR data in the reservation systems of air carriers to continue to be transferred to the US in the same way as under previous 2004 Agreement. The US Administration may access electronically PNR data from air carriers' reservation/departure control systems located within the territory of the EU Member States, respecting specifically Article 6

[108] European Convention for the Protection of Human Rights and Fundamental Freedoms// http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf [retrieved October 22, 2008].

[109] OJ L 235, 6.7.2004 P 11

[110] U.S. Mission Defends U.S –EU Air Passenger Data Accord (2004)// http://useu.usmission.gov/Dossiers/Data_Privacy/Apr2204_Kessler_PNR.asp [retrieved October 22, 2008].

[111] OJ L 298, 27.10.2006 P 29. Set to expire July 31, 2007.

which states that "…DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union concerning passenger flights in foreign air transportation to or from the United States".

New flexibility appears in case of sharing PNR data with other counter-terrorism agencies within the US Government. It is necessary to analyze this novelty in the Agreement together with the Intelligence Reform and Terrorism Prevention Act of 2004[112]. It required the President to establish a new Information Sharing Environment (ISE) (Section 1016.4b.A.) that facilitates the sharing of terrorism information. Under this enactment President issued the Executive Order 13388[113] of 25 October 2005 requiring DHS and other agencies "promptly to give access <…> to terrorism information to the head of each other agency that has counterterrorism functions" (Section 2a.). Section 1b is of doubtful nature especially for the European citizens on the PNR data issues. It is stated that those agencies, sharing information among them shall "protect the freedom, information privacy, and other legal rights of Americans…" This is another example that under US law foreigners are not protected, and so is not their PNR data. It means that when EU is transferring PNR data of its citizens, not only DHS is receiving it, but also other agencies related to counterterrorism functions. This poses a risk of misuse of PNR data.

Consequently Europeans are not protected from their data violations under any of the US national laws. Meanwhile the US had agreed on the terms with EU that the latter ensures "air carriers operating passenger flight in foreign air transportation to or from the US process PNR data contained in their automated reservation systems as required by DHS" (Article 1 of the 2006 Interim Agreement on PNR data). As an obvious beneficiary of this Agreement is again - the US.

Article 2 presents the methodology used for PNR data transfer. "Pull" system is still valid: "DHS will electronically access the PNR data from air carriers' reservation system located within the territory of the Member States <…>until there is a satisfactory system in place allowing for transmission of such data by the air carriers".

This temporal agreement did not provided stable legal atmosphere between EU and US. According to the EDPS Peter Hustinx in one way or another privacy right of air passengers between EU and US will remain to be threatened by the information sharing deals[114].

---

[112] See footnote 31.

[113] Executive Order 13388: Federal register Vol. 70, No.207 (October 27, 2005)// http://edocket.access.gpo.gov/2005/pdf/05-21571.pdf [retrieved October 22, 2008]

[114] See generally footnote 103.

3.3.3. 2007 PNR Agreement

In July 2007 new 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 US Department of Homeland Security was reached[115]. This was the most significant agreement, which recognized information sharing as an essential component in the fight against terrorism and transnational crime and that the use of PNR data is an important tool for achieving this[116]. Including that "US and European privacy law and policy share a common basis and that any differences in the implementation of these principles should not present an obstacle to cooperation…" Also it was repeated as in previous agreements regard to the Article 6 paragraph 2 of the Treaty on European Union on respect for fundamental rights, and particularly to the right to the protection of personal data.

Paragraph 6 is of great significance, because it deems for DHS to ensure an adequate level of protection for PNR data transferred from the European Union.

Analyzing explanatory US letter to EU of the 2007 Agreement[117], several important elements are being presented. Firstly, US sharply draws the *scope* of PNR data usage, stating that DHS uses EU PNR for purpose of preventing and combating terrorism, related crimes, other serious crimes/ organized crimes of transnational nature and also flight from warrants or custody for above described crimes. Additionally PNR may be used for the protection of **vital interests** of the data subject or other persons, also in any criminal judicial proceedings or as otherwise required by law. As it was mentioned in the previous analysis of the 2006 Agreement, the latter provision "other vital interests" is posing a great risk for PNR data to be used too wide. It would be reasonable to add certain statement like "PNR may be used for other vital interest, **which were debated and agreed upon together with EU**". This way the US DHS would not have capacity to act unilaterally. If EU would accept the matter under the "vital interest" status, then US could use PNR data in the permitted field. I would grant this decisive capacity to EU because shared PNR data is of its nationals and it has stronger legal obligation to protect it from misuse.

---

[115] OJ L 204, 4.8.2007, P.0018-0025

[116] Preamble of 2007 PNR Agreement.

[117] Explanatory US letter to EU of the 2007 Agreement//
http://register.consilium.europa.eu/pdf/en/07/st11/st11595.en07.pdf [retrieved October 22, 2008]

Second element described in the US letter[118] involves sensitive information sharing issues. It provides: "DHS threats EU PNR data as sensitive and confidential in accordance with US laws, and its discretion, provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions <…> Access shall be strictly and carefully limited…" It has to be understood in terms of ***bona fide,*** EU after transferred the PNR data, can presume, that its nationals' personal information will not be exchanged with unauthorized agencies, and that US deals with the PNR data as it was agreed upon. Thirdly, there is a novelty in the PNR data list – instead of previously required 34 data types now only 19 is available for the transfer[119]. The US Freedom of Information Act[120] grants to any person, no matter of what nationality, the right to request for personally identifiable information contained in PNR. Request can be submitted to FOIA, PA Unit, Office of Field Operations, U.S. Custom and Borders Protection, Room 55-C, 1300 Pennsylvania Avenue, NW Washington, DC 20229[121]

Very doubtful element is 17- general remarks (excluding sensitive information). This content should be further specified not leaving US discretion to decide unilaterally what information each time they may need. According to the case Rotaru vs. Romania judgment of 4 May 2000, collecting any personal data is already intervention into right to privacy. Any measures giving the authorities a power to interfere with the right to respect for private life by collecting and further processing personal data should contain explicit, detailed provisions concerning the persons authorized to consult such files, the nature of files, the procedure to be followed or the use that may be made of the information thus obtained[122].

Such open-ended formulations are incompatible with general requirements that PNR data to be collected for specified and explicit purposes and also that such data collected and transmitted for the purpose of combating terrorism and organized crime should be necessary, proportionate and not excessive.

Only an interference which is necessary to achieve a legitimate objective is proportionate. Any element in PNR data should be clearly defined together with the objective served by such collection

---

[118] Ibid.

[119] See Annex 2.

[120] US Freedom of Information Act // http://www.usdoj.gov/oip/amended-foia-redlined.pdf; [retrieved October 24, 2008].

[121] European Union Joint Press Release (2007) // http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/95438.pdf [retrieved October 24, 2008]

[122] ECJ case: Rotaru vs. Romania// http://www.echr.coe.int/Eng/press/2000/May/Rotaru.eng.htm [retrieved October 24, 2008]

and processing of personal data. This method would guarantee that proportionality is taken into account from the outset.

Talking about PNR data retention, the explanatory report emphasizes, that DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non operational status. In this status PNR data is retained for eight years and may be accessed only with approval of senior DHS official. This long retention period was agreed upon because of strong pressure by the US Government[123]. Consequently, US also expects that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions[124].

Another significant element of 2007 Agreement was outlined in Article 2, which emphasizes the transition from "pull" to "push" system: "DHS will immediately transition to a push system for the transmission of data by such air carriers no later than January 1, 2008…" According to mentioned US explanatory report, DHS is prepared to move as expeditiously as possible to a "push" system. The responsibility for initiating a transition to this system rests with the carriers, who must make resources available to migrate their systems and work with DHS to comply with technical requirements. And it is obvious, that willing to abort "pull" system European air carriers should implement technical requirements faster and this way reduce US capacity to intervene into European PNR data base unilaterally. This is the negativity of "pull" system. But this legal commitment on transition to a "push" system again is not clear, because it does not confer on airlines any discretion to decide when, how or what data to push. That decision is conferred on DHS by US laws[125].

From all the mentioned above it is prominent that any Agreement concluded gives the US jurisdiction to act unilaterally and change any aspects not in accord with American laws. Consequently this proves that EU has to adjust itself to the US positions. Making comparison study of 2007 PNR Agreement with EDPS Opinion of 2008 it is clear that "push' system still is not embodied. Recital 96 of the Opinion provides that air carriers established outside the EU are required to push data as long as they have technical instruments to do that. If not, they have to permit the extraction of data through the pull method. Consequently this demonstrates that pull system is still valid. This poses risk for private data misuse and raise difficulties to control of the compliance of PNR data transfer with data protection rules.

---

[123] OJ C 110 1.5.2008 P 0001-0015 Recital 103

[124] See footnote 117.

[125] Ibid. P 7

Finally, 2007 Agreement with its explanatory report provide that PNR data shall be transmitted 72 hours before a scheduled departure of the flight. Also, DHS may require PNR prior to 72 hours before the scheduled departure of the flight, when there is an indication that early access is necessary to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with the purposes defined in recital I[126].

To conclude the analysis of 2007 Agreement it is necessary to state, that EU, no matter what, is greatly dedicated to accept any requirements by US. All the criticized provisions in this thesis can make presumption that 2007 Agreement still was not the best outcome of the PNR data negotiations and legal concerns on EU citizens' privacy rights. Moreover, EU Council Presidency and the Commission in its letter to U.S[127] declare that "EU will take all necessary steps to discourage international organizations or third countries interfering with any transfers of EU PNR to the United States. The EU and its Member States will also encourage their competent authorities to provide analytical information flowing from PNR data to DHS and other US authorities concerned". Consequently from such reply letter EU confirms to be considered the adequate level of PNR data protection in the US and is ensuring to improve cooperation in aviation security while informing passengers about how governments use their information.

In February 2008, Jonathan Faull, the head of the EU's Commission of Home Affairs complained about the US bilateral policy concerning PNR. That time US signed memorandum of understanding with the Czech Republic (also the UK, Estonia, Germany and Greece) in exchange of VISA waiver scheme, without contacting with Brussels. Those tensions were caused by a lesser level of data protection in the US especially since foreigners do not benefit from the US Privacy Act of 1974. As it was mentioned before, Privacy Act protects the interest of US citizens, and for EU citizens this law does not apply.

Evaluating the role of the Commission while concluding PNR data Agreements, there can be noted several critical aspects of PNR law making. Firstly Commission did not give proper regard to data protection principles in negotiating away many of the key tenets. As it was stated in the Directive 95/46/EC Article 26, the transfer of PNR data to third countries is possible only if adequate protection is guaranteed to such data. EU declared US privacy protections as adequate, despite the fact that US clearly did not meet the criteria for such a finding. Commission took unacceptable risk while still permitting such transfer.

---

[126] Ibid P 1.

[127] Ibid P 10.

Secondly, EU has not assured adequate protection requirements by such actions mentioned above, nor did provided with clear purpose limitation, retention period or exhaustive cases when sharing of PNR is possible with other agencies (although EU legal regime only permitted data transfer for combating terrorism, the European Commission allowed the US to use information for expanded cases- other organized crimes, vital interest etc.) EU took the risk that PNR retained in dormant US archive for 8 years will be deleted after.

Thirdly EU did not demand to amend US privacy laws in order to be better adjusted with similar privacy laws of Europe. It gave US predominant position for unilaterally changing provisions of the PNR Agreements, getting too many excuses. EU did not draw sufficient attention to the inequality of the US law as it applies only to foreign carriers, not US airlines operating abroad. It may leave gaps in the counterterrorism field, posing risk that potential terrorists can freely enter into EU, because of lack of PNR Agreement from US carriers.

Finally, the PNR data Agreements with US are not the last challenge for European citizens' privacy rights. Commission foresees possibility to transfer PNR with other allies in the fight against terrorism, meaning that European citizens' PNR data will be shared not solely with US, (relevant Agreements are being concluded with Canada, Australia, also for future negotiations are set Russia, India, Turkey, Tunisia, Malaysia and Thailand[128]). Such multilateral legislation called as global surveillance infrastructure on PNR data transfers may grant bigger dilemma. Worldwide stream of multilateral data sharing can endanger fundamental rights and especially right to privacy. And in this case US with ACLU, Privacy International are also aware of such risk.

3.4. European Parliament joint Resolution

In 2007 European Parliament passed harsh resolution on the processing and transfer of PNR[129] to the US. European Parliament concerned firstly at the persistent lack of legal certainty as regards the consequences and scope of the obligation, especially about the DHS's handling, collection, use and storage of PNR data that's is not founded on a proper agreement, but only on non-binding assurances

[128] ASEAN-EU. Joint Declaration on Co-operation to Combat Terrorism. Brussels: 14th ASEAN-EU Ministerial Meeting, 2003. January 27-28.

[129] EP Joint Resolution on EU-US PNR Agreement//http://quintessenz.org/doqs/000100003894/2007_07_11_EU-parl_PNR_joint%20resolution.pdf [retrieved October 20, 2008]

that can be unilaterally changed by the DHS at any moment. The fact was deplored in the mentioned resolution that:

- The length of PNR data retention will be extended from 3,5 years to 15 years (consisting of a seven year "active" and an eight year "dormant" period), as well as this being retroactively applied to data collected under the previous PNR agreements;
- After 15 years there is no guarantee that the data will be definitely deleted; (!)

Reduction in data fields from 34 to 19 is largely fake due to the merging and renaming of data instead of ACTUAL deletions.

This Joint Resolution has caused many critics. Firstly, included into the art 4 there is a regret of the fact that "…PNR data is not founded on a proper agreement, but only on non-binding assurances that can be unilaterally changed by DHS at any given moment and that do not convey any rights or benefits on any person or party". This means that by any changed circumstance, DHS could use PNR data for other "unspecified additional purposes", and this way violate the person's right to privacy (e.g. information regarding ethnic origin, political opinion, private life of the individual could easily be accessed, having in mind that PNR data is being kept from 3.5 to 15 years, or for 7 years in "active analytical databases" leading to a big risk of massive profiling, contrary to EU principles - Article 11, 13, 14). Secondly, having in mind the mentioned factor, the agreement states in its Article 7, that it must be comprehensive, annual reviews by DHS and the EU, including "…an assessment of the effectiveness of the measures in terms of greater security…" USA has to assure the effective protection of PNR data, but as it is obvious from the Article 10bis, there is a regret, that "the agreement does not foresee precise criteria for the definition of the protection of personal data offered by DHS as adequate according to EU standards."

3.5. Recent PNR data legislation: EDPS opinion 2008 C 110/01 and EP Resolution of 20 November 2008

As 2007 PNR data Agreement lacked effective safeguard mechanism of PNR data transferred from EU to the US, EDPS (established by the EC Regulation No 45/2001[130]) proposed new schemes on the EU US PNR system to the Commission. Following the Opinion of the EDPS on the draft Proposal

[130] OJ L 8, 12.1.2001 P 0001-0022

for a Council Framework Decision on the use of PNR data for law enforcement purposes[131] it was intended to harmonise Member States' provisions on obligations to transmit PNR data for air carriers operating flights to or from their territory for preventing and fighting terrorism and other organized crime. Crucial element of the Opinion identifying purpose of PNR gathering is stated in recital 13, which defines that main target, is to "carry out risk assessment of persons, obtain intelligence and make association between known and unknown people". Meaning it is important to identify persons who are or may be involved in terrorism activities, as well as their associates. Consequently PNR data do not have an identification purpose, it contributes mainly to carry out risk assessments of the persons, obtaining intelligence and making associations between known and unknown people.

By this Opinion thesis receives broader ample of the PNR data collection purposes. Moreover, it gives new justifications for PNR data retention. According to recital 16 of the Opinion it is obvious that in order to identify risk posing persons, it is necessary to analyze patterns of certain behaviour so this requires to keep PNR data for a sufficiently long period as to fulfill the purpose of developing risk indicators and establishing patterns of travel. The added value of PNR data is justified by the EC precisely because of the proactive nature of the system it intends to establish- a system which seeks to develop "profiles" and associate individuals to be linked to terrorists, who might follow the same travel routes or have the same travel patterns or history.

But revising all suggestions EDPS stated that those measures are rather intrusive into privacy rights and proposed techniques for assessing behavioural patterns need to be amended[132]. EDPS Opinion embodies new statement for balancing privacy and security elements. Recital 36 of the Opinion declares that the fight against terrorism and organized crimes can certainly be a legitimate ground to apply exceptions to the fundamental rights to privacy and data protection but as far as this intrusion is supported by undeniable and proportional elements.

Continuing on the problematic PNR data transfer methods EDPS considers only "push" system to be effective safeguard for privacy rights (as it was mentioned above, it still permits "pull" system). Opinion embodies that within effective "push" system data should be filtered at the very primary step of processing, without exclusions that non necessary data will be deleted immediately by third party[133].

Last element to be discussed is PNR data retention, according to EDPS, 15 years retention period is too excessive. Even if it indicates the need to establish patterns of travel and behaviour, the

[131] OJ C 110, 1.5.2008 P 0001- 0014

[132] Ibid, Recital 29.

[133] Ibid, Recital 98.

efficiency is questionable and can not be justified. There is no reasonability to retain data of all passengers in total absence of suspicion for 15 years whether in analytical or dormant database.

Having regard to this EDPS Opinion, European Parliament adopted resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes[134]. It was stated that personal data shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes; moreover derogations from this principle are permitted only in accordance with law and constitute a necessary measure in a democratic society for suppression of criminal offences. Accordingly if there is event of any extension of the proposal's scope, the Commission and the Council should clarify the necessity and establish appropriate legal basis for such specific purpose[135]. Examining sensitive PNR data, EP puts emphasis that such data may be used only on a case-by-case basis and under regular investigations or prosecution, having obtained the warrant (Recital 26). Regarding retention period, EP Resolution stresses that Commission had failed to justify the proposed retention period of 3.5 years and included strict provision that data transfers should be made using PUSH method alone restricting third countries to gain access to PNR data in EU reservation systems (Recital 27-28). Also another positive outcome of the Resolution was provision of exhaustive list of cases when PNR data can be accessed. Finally EP Resolution limited transfer of PNR data to third countries if they do not provide adequate level of such data protection or appropriate safeguards to it.

Summing up it is obvious that recent PNR data legislation paid attention to loopholes made in previous 3 PNR data Agreements and intends to correct mentioned errors in order to preserve privacy rights at the same time maintaining secure air transportation.

---

[134] Council framework decision on the use of the PNR for law enforcement purposes (2008)// http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P6-TA-2008-0561%200%20DOC%20XML%20V0//EN&language=EN [retrieved October 29, 2008]

[135] Ibid. Recitals 19-24

3.6. Proposals how to amend open-ended provisions in PNR data agreements

After examining 3 PNR data Agreements it is noticeable main legal loophole leading to further inaccuracies and uncertainties for PNR data to be properly collected, stored, transferred and safeguarded. That is open-ended and imprecise formulations, which may allow the US to interpret PNR Agreements wider than necessary.

PNR data processing operations and other provisions should be defined and specified precisely in order to ensure that data processing operations are foreseeable by data subjects and are not violating right to respect of privacy elements. This requirement of precision constitutes guarantee against arbitrariness in the imposition of restrictive measures and so there can not be any secret surveillance basing on these open-ended formulations. Within the scope of thesis topic, passengers flying to the US should be appropriately informed about what PNR data are collected about them. Any secret surveillance on behavioural patterns while on board or in airports can not be justified. Under the case law of the European Court of Human Rights[136], such interference in the private life of individuals cannot be presumed to be necessary in a democratic society. But in order for systems of secret surveillance to be compatible with Article 8 of the Convention, it has to contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society and in particular with rule of law, which implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision. It must be carried out by the judiciary, since such control affords the best guarantees of independence, impartiality and a proper procedure. Consequently US should neither expect to require specific PNR data under open-ended provisions nor require for specific behavioural data observed on board or in airports (PNR data 17, 18 elements)

Several proposals to amend provisions of PNR data Agreements are done with accord to the Article 29 Data Protection Working Party (01646/07/EN WP 138) Opinion 5/2007[137].See the table below:

[136] See ECHR cases Klass vs. Germany, Annan vs. Switzerland, Rotaru vs. Romania, Malone vs. United Kingdom, Kruslin vs. France, Kopp vs. Switzerland.

[137] Opinion 5/2007 on the follow-up 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

Table 1. **Open-ended provisions in 3 PNR data agreements**

Field with open-ended provisions	2004 PNR Agreement	2006 PNR Agreement	2007 PNR Agreement
1. PURPOSE LIMITATION	PNR data collected for preventing and combating: terrorism and related crimes; other serious crimes, including organized crimes, also flight from warrants or custody.	Ibid.	Ibid. additionally PNR data may be used where necessary for the protection of the vital interests of the data subject or in any criminal judicial proceedings as required by law.
2. PNR DATA ELEMENTS	34 elements. Nr.19- General Remarks Nr.26- OSI; Nr.27- SSI/SSR; Nr.33- Any collected APIS information.	Ibid.	19 elements. Nr.7- All available contact information; Nr.12- Split divided information; Nr.15- All baggage information; Nr.17- General remarks with OSI, SSI/SSR; Nr.18- Any collected APIS information.
3. METHODS OF ACCESS	CBP will "pull" PNR data from air carrier reservation system, until air carriers are able to implement a satisfactory "push" system.	Ibid.	Transition to "push" system no later than by 1 July, 2008. As it was seen from chapter 3.III.5 there is still not such system adopted for all EU air carriers.
4. PNR DATA RETENTION	3.5 years. After this PNR is transferred by CBP to a deleted record file and retained there for 8 years more before being destroyed. And there is no legal ground to assume that after 8 years it is surely deleted.	Ibid.	7 years in analytical database, then moved to a dormant, low-operational status for 8 years and may be accessed only by DHS approval. Meaning that it is still can be accessed.
5. PNR DATA SHARING	No other foreign, federal, State of local agency has direct electronic access to PNR. BUT- CBP will provide PNR data to other governmental authorities, including foreign governmental authorities with counter-terrorism or law enforcement functions.	Executive Order 13388, it was established ISE: promptly access to terrorism information to head of each other agency that has counterterrorism function.	Ibid.

Firstly, considering about PNR data collection purpose limitation (while preventing and combating terrorism), there should be no blanket expressions such as "serious crime", "other related crimes" or "other vital interests". It is suggestible to draw up a comprehensive list of crimes (on the other hand a list of specific offences may be difficult to name because of a changing picture of criminal activity, but at least the list can be done presumably). Also explicit and certain provisions should be included in required PNR elements, without "general remarks". Open-ended provisions run the risk that

Security concluded in July 2007. Adopted 17 August, 2007// http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf [retrieved October 22, 2008]

any change in US legislation might unilaterally affect the level of data protection as it is foreseen in PNR Agreements.

Secondly, method of PNR data transfer remains questionable: transmission from "pull" to "push" system supposed to be done no later than by 1 July, 2008. As it was stressed in the EDPS Opinion 2008 C 110/01 and EP Resolution of 20 November 2008 it remains problematic to achieve this transmission.

Thirdly, concerning about data retention period it is necessary to diminish division into active and dormant periods. As long as PNR data is accessible, in limited or restricted cases, they remain available in a database and can be accessed and processed by DHS. Also, no operational evidence has been provided that such data retention period is necessary (as required by Article 8 of the ECHR). For contemporary situation on PNR data retention and transfer to the US Lithuania has no final decision. Articles from www.delfi.lt prove that PNR dilemma is not resolved yet[138].

Fourthly, open-ended provision on what institutions can access PNR data is of great potential to violate individuals' right to privacy. PNR data Agreements provide information sharing environment and justifies PNR data to be access by other governmental authorities with counterterrorism functions. This provides US with ample opportunities to spread PNR data within any authority more or less having functions of counterterrorism.

Concluding it has to be stress the dissatisfaction of the "29 Article Working Party" that EU-US negotiations have not achieved proportional protection of PNR data, and mostly served the US side. 2007 Agreement "does not strike the right balance to uphold the fundamental rights of citizens as regards data protection"[139] EU failure to conclude effective agreements for preserving own citizens privacy rights on adequate level is unjustifiable. This fosters to state that EU got affected by US "security above all" system and might comply with further US global surveillance ideas.

Trying to find justification for such dissatisfaction, it can be stated, even if PNR data Agreements were not of maximum concern about privacy rights, they held important aim- collect personal information for counterterrorism matters. Threat was reduced indeed: running PNR data against alert systems in order to identify known terrorist and criminals gave results. Once a known terrorist was identified, PNR could be used to identify another passenger connected to the letter. This is being done by comparing PNR data of the known terrorist/criminal to those of the passengers who

[138] Samoškaitė E., Skrisi vienąkart, o duomenis saugos 8 metus? (2008 10 21)// www.delfi.lt [retrieved October 21, 2008]

[139] See footnote 137. P 3.

share the same address, credit card number, contact details. This exercise is very useful in obtaining evidence by association and in identifying previously unsuspected passengers.

Moreover, by running PNR data against a combination of characteristics and behavioural patterns it became simpler to identify high-risk passengers. Also, running PNR data against risk intelligence allowed to identify also travel agencies in a certain country which has connections with a specific terrorist organization or criminal group. In such cases PNR data helps identify which passengers have bought tickets from such suspected agency[140]. Finally, because of PNR data files it is double security guaranteed upon the arrival. Each "high-risk" passenger or potential terrorist have to be questioned once again by security officers and in combination with other specific information denied an entry in the territory of the destination country. PNR data when used in conjunction with data from other sources significantly assist in the identification of terrorist, whether before a planned attack or after such an attack.

Critically, by PNR data collection CBP and other authorities gain access to private information of passengers flying from EU to US. As it was mentioned above PNR serves to ensure aviation security and prevent possible threats. But I agree with Bruce Schneier, who mentioned that only two things have made airline travel safer since 9/11: reinforcement of cockpit doors, and passengers who know that they may have to fight back. All other taken measures including CAPPS II, Secure Flight and Trusted Traveler, also PNR data collection - is "security theater". B. Scheier notes that it would be a lot safer if airports implemented enhanced baggage security - both ensuring that passenger's bags don't fly unless passenger himself/herself is on board, and explosives screening for all baggage - as well as background checks and increased screening for airport employees[141]. Real security arises from old fashioned investigative work: putting people in charge of investigating potential plots and letting them direct the computers, instead of putting the computers in charge and letting them decide who should be investigated[142]. Solely by granting main function to computer algorithms and PNR data matches will not help to fight the terror. By PNR data collection and transfer legal consequences are more negative than positive. Grave intrusions into privacy rights can not be justified by US goal to

[140]Commission Staff Working Document (2007)// http://209.85.129.132/search?q=cache:MYlCogQarEAJ:eur-lex.europa.eu/Notice.do%3Fmode%3Ddbl%26lang%3Den%26ihmlang%3Den%26lng1%3Den,lt%26lng2%3Dbg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,%26val%3D459467:cs%26page%3D+how+PNR+data+collection+helps+to+combat+terorrism&hl=lt&ct=clnk&cd=1&gl=lt [retrieved December 5, 2008]

[141] Schneier B. Airline security a Waste of cash//http://www.schneier.com/essay-096.html [retrieved November 10, 2008]

[142] Schneier B. How to not catch terrorist//http://www.schneier.com/essay-163.html [retrieved November 10, 2008]

ensure security in any possible and available manners. And as B. Schneier concluded "**Who controls our data controls our lives** and sells our most intimate information. But the long-term effects of this on society are toxic; we give up control of ourselves"[143].

Considering all mentioned factors I conclude the task risen in the introduction of this thesis that collecting PNR data is not the crucial method for ensuring aviation security and it can not be understood as solely effective measure to combat terrorism. Moreover by PNR data collection no balance is possible between privacy and security[144].

[143] Schneier B. Our data, ourselves//http://www.schneier.com/essay-219.html [retrieved November 10, 2008]

[144] See footnote 64.

CONCLUSION

Secure civil aviation system is a critical component of entire nations' overall security, physical infrastructure and economic foundation. The terrorist attack of 9/11 turned American airliners into weapons of mass destruction and demonstrated significant, longstanding vulnerabilities in aviation security. Additionally because of international dimension, the phenomena of terrorism and organized crime can only be effectively dealt with through international legal cooperation.

By various aviation security initiatives of G8, ICAO, EU and US air transportation security was a subject of extreme improvement, emphasizing necessity to make great changes in airports and on board. US practice to concentrate on passenger and baggage screening was essential one to guarantee that neither prohibited goods can be imported to security restriction zones or on board nor perpetrators reached those zones.

According to US security and privacy scholar, former Secure Flight Working Party specialist Bruce Shneier, such technological improvements assist to raise aviation security, and there should be no necessity to quarrel about intervention to privacy rights or require for PNR data within international flow. Privacy rights and PNR data transfer are crucial to be analyzed within aviation sector because in 21st century freedom of movement and traveling *per se* are closely related to the air transportation.

Thesis found that an individual does never have absolute right to privacy, and for security reasons this fundamental right sometimes can be intervened. But there has to be decent equilibrium. Interference into right to privacy (restriction) can be justified only if it meets with 3 criteria: legitimacy, reasonability and proportionality. Considering these criteria within private data conception it is crucial, especially in this "borderless world" of technologies, to assure that adequate protection is ensured if data is a subject of international transfer. This is clearly embodied in EU Directive 95/46/EC, wherein Member States are required to provide that a transfer of personal data to third country may only take place IF the third country ensures an adequate level of data protection. Further transatlantic willingness to diminish privacy laws difference and aim to improve cooperation on PNR data transfer led to adoption of the Safe Harbor principles. This legal act can be considered as one of many trials to solve US EU dilemma on privacy and security.

Considering about bilateral commitments on security and privacy legal dilemma (which arose from ATSA requirement to transfer personal data to CBP) under 2004 PNR agreement EU irresponsibly granted that US is capable to ensure adequate level of data protection, but ECJ judgment

annulled such negotiations. Further concluded PNR agreements in 2006 and 2007 were of poor legal value to EU also. Main problem is the open-ended provisions on PNR data, which might allow US to act unilaterally and expand the scope of such provisions. There should be eliminated such wide scope norms. Also, reducing PNR data elements from 34 (in 2004, 2006 Agreements) till 19 (in 2007 Agreement) is a legal trick, because observing list of 19 PNR data elements it can be seen that "general remarks" or "OSI/SSI/SSR information allow US to demand any data, so amended list in 2007 Agreement is of no benefit ensuring privacy to EU citizens.

Moreover, it is necessary to diminish data retention period into active and dormant operational status, because this allows PNR data to be retained as long as CBP finds it necessary. Finally creating PNR data sharing environment within authorities, of counterterrorism functions in the US it gets extremely difficult for EU to implement monitoring mechanism and control where, how, who and when PNR data is used.

Critically, PNR data collection being useful to identify potential criminals who already have ties with terrorism network but is not crucial measure to ensure aviation security. 3 PNR data agreements had little input for safeguarding EU citizens' privacy rights but on the other hand were essential for US. Consequently by inability to stand against economic sanctions and other threats from US, EU complies with any provisions. EU failure to strike for right balance between security and privacy and inability to conclude effective agreements for preserving own citizens privacy rights on adequate level is unjustifiable. This fosters to state that EU got affected by US "security above all" system and might comply with further US global surveillance ideas.

Summing up EU- US legal dilemma can not be solved if one or another contracting party will not realize that by PNR data collection, transfer, retention and by illegal intrusions to privacy rights aviation security can not be ensured. PNR data and aviation security are closely resembled issues, but it is unjustifiable to gain one meanwhile canceling the other. The hypothesis was proved.

BIBLIOGRAPHY

Literature:

1. **Data Protection law**/ Second edition by David Bainbridge. - Saxon Graphics Ltd, Derby, 2005. – 20 p. – ISBN 185811-342-3
2. **Marks S., Clapham A.** International human rights lexicon. – Oxford university press, 2005. – 264-265 p. – ISBN 0-19-876413-8
3. **Pečkaitis J. S., Mačerinskienė I**. Magistro baigiamojo darbo rengimo tvarka: mokomasis leidinys. – Vilnius: Mykolo Romerio universiteto Leidybos centras, 2008, p 4-78. - ISBN 978-9955-19-083-7
4. **Privacy and the Criminal law**/ Edited by Eric Claes, Antony Duff and Serge Gutwirth. – Intersentia, 2006. – 74-75 p. – ISBN 9050955452
5. **Protecting privacy**/ Edited by Basil S. Markesinis. – The Clifford Chance Lectures Volume Four; Oxford University Press, 1999. – 74 p. – ISBN 0-19-826885-8
6. **Silverman D**. Doing qualitative research. A Practical Handbook (second edition) - London, Thousand Oaks, New Delhi: Sage Publications, 2005. – 99 p. – ISBN 1-4129-0197-9. – ISBN 1-4129-0196-0
7. **Shawcross, Beaumont**, Air Law - Contemporary Tables and Index // Butterworths, 2007. Division II, P. 12-20.
8. **Walters G. J.** Human rights in an information age/ A philosophical analysis. – Toronto, Buffalo, London: University of Toronto press, 2001, p. 121-134. – ISBN 0-8020-8550-4
9. **Weber L**. International Civil Aviation Organization. An Introduction. Kluwer Law International, 2007. P. 11.

European Union Legislation:

1. OJ L 281, 23.11.1995 P. 0031-0050
2. OJ L 215, 25.8.2000 P. 0007-0047
3. OJ L 8, 12.1.2001 P. 0001-0022
4. OJ L 181, 04.07.2001 P. 0019-0031
5. OJ L 201, 31.7.2002, P. 0037- 0047

6. O J L 335, 30.12.2002 P. 0001-0022
7. OJ L 89, 5.4.2003 P. 0009-0010
8. OJ L 183, 20.5.2004 P. 0084-0085
9. OJ L 229 29.6.2004 P.0003-0004
10. OJ L 235, 6.7.2004 P. 0011-0022
11. OJ L 298, 27.10.2006 P. 0029
12. OJ C 321E, 29.12.2006, P. 0001-0331
13. OJ L 204, 4.8.2007, P.0018-0025
14. OJ C 110 1.5.2008 P. 0001-0015
15. **Council framework decision on the use of the PNR for law enforcement purposes** (2008) // http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P6-TA-2008-0561%200%20DOC%20XML%20V0//EN&language=EN [retrieved October 29, 2008]
16. **EU Council on the Processing and transfer of passenger name record data by air carriers to the US DHS- PNR** (2007) // www.cyberlaw.pro/docs/pnragreement.pdf [retrieved October 23, 2008]
17. **Memorandum of Cooperation between the International Civil Aviation Organization and the EC regarding security audits and inspections and related matters** (2008)// http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008PC0335(01):EN:HTML [retrieved October 7, 2008]

USA Legislation:

1. **Aviation and Transportation Security Act** (19 November, 200) // http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf [retrieved April 28, 2008]
2. **Freedom of Information Act** (amended in 2007) // http://www.usdoj.gov/oip/amended-foia-redlined.pdf [retrieved November 17, 2008]
3. **Intelligence Reform and Terrorism Prevention Act** (17 December, 2004) // http://www.nctc.gov/docs/pl108_458.pdf [retrieved November 17, 2008]
4. **Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection**, 69 Fed. Reg. 41543 (July 9, 2004) found in OJ L 235, 6.7.2004 P.0011-0022
5. **The Presidential Executive Order 13388**: Federal register Vol. 70, No.207 (27 October, 2005) // http://edocket.access.gpo.gov/2005/pdf/05-21571.pdf [retrieved November 17, 2008]

ICAO Regulations:

1. ICAO Journal, The magazine of the International Civil Aviation Organization VOL. 56, No.5 June 2001. Page 9-10, 26.
2. ICAO Journal, The magazine of the International Civil Aviation Organization. VOL.56, No 9. November/December 2001. Page 10
3. ICAO Journal, The magazine of the International Civil Aviation Organization. VOL.57, No 2. March 2002. Page 5, 27.
4. ICAO Journal, The magazine of the International Civil Aviation Organization. VOL.58, No.7. September 2003. Page 5-6
5. Aviation Security and Facilitation Branch // http://www.icao.int/atb/sfbranch/index.asp? [retrieved April 8, 2008]

Treaties/ Declarations:

1. **American Convention on Human Rights** (1969) // http://www.oas.org/juridico/English/treaties/b-32.html [retrieved November 28, 2008]
2. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (1981) // http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm [retrieved December 5, 2008]
3. **Convention on the Rights of the Child** (1989) // http://www.unhchr.ch/html/menu3/b/k2crc.htm [retrieved November 28, 2008]
4. **European Convention on Human Rights** (1950) // http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf [retrieved November 28, 2008]
5. **International Covenant on Civil and Political Rights** (1966) // http://www.unhchr.ch/html/menu3/b/a_cescr.htm [retrieved November 28, 2008]
6. **The Charter of Fundamental Rights of the EU** (2000) // OJ C 364, 18.12.2000, P 1-22
7. **The Chicago Convention** (1944) // http://www.icao.int/cgi/goto_m.pl?/icaonet/dcs/7300.html; [retrieved May 20, 2008]
8. **Universal Declaration of Human Rights** (1948) // http://www.unhchr.ch/udhr/lang/eng.htm [retrieved November 29, 2008]

Case law:

1. Rotaru vs. Romania, ECHR Judgment 2004 05 04
2. Klaas vs. Germany, ECHR Judgment 1993 09 22
3. Amann vs. Switzerland, ECHR Judgment 2000 02 16
4. Malone vs. United Kingdom, ECHR Judgment 1984 08 02
5. Kruslin vs. France, ECHR Judgment 1990 04 24

Publications and Reports:

1. **Adey P.** Secured and sorted mobilities: examples from the airport// http://www.surveillance-and-society.org/articles1(4)/sorted.pdf [retrieved May 8, 2008]
2. **Amnesty International**: Security and human rights. Counter-terrorism and the United Nations // http://www.amnesty.org/en/library/asset/IOR40/019/2008/en/7c2b7a4d-7a71-11dd-8e5e-43ea85d15a69/ior400192008en.pdf [retrieved May 10, 2008]
3. **Article 29 Working Party Opinion 4/2003** on the Level of Protection ensured in the US for the Transfer of Passengers' Data (2003) // http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_en.pdf [retrieved October 22, 2008]
4. **Article 29 Working Party Opinion 5/2007** on the follow-up agreement between EU-US on the processing and transfer of PNR data by air carriers to the US Department of Homeland Security (2007) // http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf
5. **Article 29 Working Party Workshop.** EU approach towards a new passenger data agreement (2007) // http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2007_03_26_pnr_workshop_report_en.pdf [retrieved October 29, 2008]
6. **BNET business network.** Know nothing: US intelligence failures stem from too much information, not enough understanding. http://findarticles.com/p/articles/mi_m1282/is_n14_v50/ai_21102283 [retrieved March 3, 2008]
7. **Bureau of Customs and Border Protection, Department of Homeland Security.** Comments of the Identity project, World privacy forum and John Gilmore // http://hasbrouck.org/IDP/IDP-APIS-comments.pdf [retrieved October 10, 2008]

8. **Chertoff M.** Information sharing critical to airline safety (2006) // http://www.america.gov/st/washfile-english/2006/September/20060901110957EAifaS0.8765222.html [retrieved October 1. 2008]
9. **Civil Aviation Security Financing Study**. US aviation security (2004) // http://ec.europa.eu/transport/air_portal/security/studies/doc/2004_aviation_security_s_7.pdf [retrieved October 2, 2008]
10. **Congressional Research Service Report**: Homeland Security: Air Passenger Prescreening and Counterterrorism (2005) P. 18// http://www.au.af.mil/au/awc/awcgate/crs/rl32802.pdf [retrieved October 12, 2008]
11. **Communication from the Commission to the Council and the Parliament**. Transfer of Air passenger name record (PNR) Data: a global EU approach (2003) // http://www.statewatch.org/news/2003/dec/apis_en.pdf [retrieved October 10, 2008]
12. **EU agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes** (2008) // http://fra.europa.eu/fra/material/pub/discussion/FRA_opinion_PNR_en.pdf; [retrieved October 28, 2008]
13. **EU Commission Directorate General on Justice, Freedom and Security (JLS). EU Committee 21st Report of Sessions 2006-2007** // http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf [retrieved November 10, 2008]
14. **EU Joint press release.** Agreement with the United States on the continued use of passenger name record (PNR) data (2006) // http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/er/91183.pdf [retrieved October 7, 2008]
15. **EU Joint Press Release.** The EU and the United States reach agreement on Passenger Name Record (PNR) data (2007) // http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/misc/95438.pdf [retrieved October 9, 2008]
16. **Explanatory US letter to EU of the 2007 Agreement** // http://register.consilium.europa.eu/pdf/en/07/st11/st11595.en07.pdf [retrieved October 22, 2008]
17. **Framework for Global Electronic Commerce by President W. J. Clinton and Vice President A. Gore Jr.** (1997) // http://isis.ku.dk/kurser/blob.aspx?feltid=196532 [retrieved October, 2008]

18. **Green. C.T.** Bush administration to make hacking a terrorist offence (2001) // http://www.theregister.co.uk/2001/09/25/bush_admin_to_make_hacking/ [retrieved March 7, 2008]
19. **High Commissioner for Human Rights Louise Arbour** // http://www.amnestyusa.org/document.php?id=ENGIOR400192008 [retrieved October 26, 2008]
20. **House of Lords:** House of Lords: The EU/US PNR Agreement. Report 2006-2007, P 15// http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf [retrieved October 19, 2008]
21. **Hustinx P.** Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection/ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf [retrieved November 1, 2008]
22. **Kaplan E.** Targets for Terrorists: Post 9/11 Aviation security (2006) // http://www.cfr.org/publication/11397/targets_for_terrorists.html [retrieved December 5, 2008]
23. **Kessler J.** The United States Mission to the European Union. U.S. Mission defends US-EU air passenger data accord (2004) // http://useu.usmission.gov/Dossiers/Data_Privacy/Apr2204_Kessler_PNR.asp [retrieved October 9, 2008]
24. **Nolan S.** Research study: EU security versus civil liberties. The case of PNR data transfer // http://www.bisa.ac.uk/2006/pps/nolan.pdf [retrieved October 5, 2008]
25. **Opinion of the European Agency for Fundamental Rights on the Proposal for a Council framework decision on the use of PNR data for law enforcement purposes//** http://fra.europa.eu/fra/material/pub/discussion/FRA_opinion_PNR_en.pdf [retrieved November 10, 2008]
26. **Poole R. W. Jr.** Improving Airport Passenger Screening (2002) // http://www.reason.org/ps298.pdf [retrieved October 5, 2008]
27. **Poole R. W. Jr., Passantino G**. A Risk – Based Airport Security Policy (2003) // http://www.reason.org/ps308.pdf [retrieved October 5, 2008]
28. **Poole R. W. Jr.** Airport Security: Time for a New Model (2006) // http://www.reason.org/ps340.pdf [retrieved October 5, 2008]
29. **Privacy International report.** Transferring Privacy: the transfer of passenger records and the abdication of privacy protection (2004) //

http://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf [retrieved November 10, 2008]

30. **Privacy International.** Leading surveillance societies in the EU and the World (2007) // http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 [retrieved November 29, 2008]
31. **Privacy International and ACLU call for repeal of EU-US agreement on data transfers (2007)** // http://209.85.135.104/search?q=cache:0FJLP4MsI1oJ:www.privacyinternational.org/article.shtml%3Fcmd%255B347%255D%3Dx-347-548477+US+POSES+RISK+FOR+EU+WHILE+PNR+DATA+PROTECTION&hl=lt&ct=clnk&cd=1&gl=lt [retrieved November 10, 2008]
32. **Quinn S.** Air data deal: forum brief (2004) // http://www.eupolitix.com/latestnews/news-article/newsarticle/air-data-deal-forum-brief/ [retrieved October 1, 2008]
33. **Sharon N.** EU Security versus Civil Liberties: the case of PNR data transfer, BISA Annual Conference (2006)// http://www.bisa.ac.uk/2006/pps/nolan.pdf [retrieved October 25, 2008]
34. **Schneier B.** Backscatter X-Ray Machines and your Privacy// http://www.schneier.com/blog/archives/2006/12/backscatter_xra.html [retrieved October 19, 2008]
35. **Shneier B.** The eternal value of Privacy. http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886 [retrieved June 26, 2008]
36. **Schneier B.** Airline security a Waste of cash. http://www.schneier.com/essay-096.html [retrieved November 10, 2008]
37. **Schneier B.** Your Vanishing Privacy. http://www.schneier.com/essay-109.html [retrieved November 10, 2008]
38. **Schneier B.** Risk of Third-Party data. http://www.schneier.com/essay-128.html [retrieved November 10, 2008]
39. **Schneier B.** How to not catch terrorist. http://www.schneier.com/essay-163.html [retrieved November 10, 2008]
40. **Schneier B.** Security at what cost? http://www.schneier.com/essay-207.html [retrieved November 10, 2008]
41. **Schneier B.** Our data, Ourselves. http://www.schneier.com/essay-219.html [retrieved November 10, 2008]

42. **Schneier B.** Crypto-Gram newsletter: protecting privacy and liberty. http://www.schneier.com/crypto-gram-0109a.html#8 [retrieved November 1, 2008]
43. **The aftermath of 11 September 2001: Liberty vs. Security before the Supreme Court of Canada.** Oxford Journals, International Journal of Refugee Law, Volume 18, Nr 2. 2006. P 313-332// http://ijrl.oxfordjournals.org/cgi/content/full/18/2/313?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=1&title=PRIVACY+VS.+SECURITY&andorexacttitle=or&andorexacttitleabs=and&andorexactfulltext=and&searchid=1&FIRSTINDEX=0&sortspec=relevance&resourcetype=HWCIT [retrieved October 7, 2008]
44. **United Nations Human Rights Committee, General Comment** No 27 (1999)// http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/6c76e1b8ee1710e380256824005a10a9?Opendocument [retrieved October 24, 2008]
45. **UN Report on Counter-terrorism technical assistance programmes-ICAO //** http://www.un.org/sc/ctc/directory/doa/ICAO.html [retrieved May 20,2008]
46. **U.S. Mission Defends US –EU Air Passenger Data Accord** (2004) // http://useu.usmission.gov/Dossiers/Data_Privacy/Apr2204_Kessler_PNR.asp [retrieved October 22, 2008]
47. **USA Government Accountability Office Report.** Terrorist Acts demonstrate urgent need to improve security at the Nation's airports (2001) // http://www.gao.gov/new.items/d011162t.pdf [retrieved October 2, 2008]
48. **USA Government Accountability Office Report.** Aviation Security (March 2005) // http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf [retrieved October 2, 2008]
49. **USA Government Accountability Office Report.** Secure Flight Development and Testing Under Way, but risks should be managed as system is further developed (2005) // http://www.gao.gov/new.items/d05356.pdf [retrieved October 2, 2008]
50. **Waldron J.** Security and liberty: The image of Balance / The Journal of Political Philosophy: Volume 11, No.2, 2003, 191-210 p. // http://www3.interscience.wiley.com/cgi-bin/fulltext/118847768/PDFSTART [retrieved October 26, 2008]
51. **Wright L.** Spymaster: Can Mike McConnell fix America's intelligence community? // http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright?currentPage=all [retrieved October 15, 2008]

Additional literature:

1. **Benjamin Franklin**. Important quotes from history (1759)// http://www.theamericanpatriotsite.com/pages.asp?pageid=51523 [retrieved October 24, 2008]
2. **BBC news.** Shoes trigger airport security alert (April, 11, 2002) // http://news.bbc.co.uk/2/hi/americas/1922748.stm [retrieved October 19, 2008]
3. **Bin Laden family**// http://en.wikipedia.org/wiki/Bin_Laden_family [retrieved October 18, 2008]
4. **CNN news.** Suspect in shoe bombing case indicted (January, 17, 2002) // http://edition.cnn.com/2002/LAW/01/16/reid.charges/?related%20%0D%0D [retrieved October 19. 2008]
5. **Eurobarometer** // http://www.libertysecurity.org/article2006.html [retrieved October 26, 2008]
6. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** (1980)// http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [retrieved October 17, 2008]
7. **Rasmussen Reports** (2008) // http://www.rasmussenreports.com/public_content/politics/current_events/general_current_events/51_say_security_more_important_than_privacy; [retrieved October 26, 2008]
8. **Samoskaite E.** Skrisi vienąkart, o duomenis saugos 8 metus? (2008 10 21)// www.delfi.lt [retrieved October 21, 2008]
9. **Washington Times.** Watch-list Justice (2005) // http://209.85.135.104/search?q=cache:OZcVLrE1A98J:www.gunowners.org/op0514.htm+Senator+Edward+Kennedy+SHARES+THE+SAME+NAME+ON+THE+WATCHLIST&hl=lt&ct=clnk&cd=10&gl=lt [retrieved October 18, 2008]
10. **What is in a Passenger Name Record (PNR)?** // http://hasbrouck.org/articles/PNR.html [retrieved October 18, 2008]

Janulaitytė G. Aviation security after 9/11 and human rights / Joint international law master thesis. Professor doc. dr. J. Žilinskas. – Vilnius: Mykolas Romeris university, Faculty of law, 2008. -

ANOTATION

Master thesis researches and examines the legality and effectiveness of PNR data transfer from EU to US in order to ensure aviation security and diminish potential terror threat after 9/11. Also it is being debated about privacy vs. security balance dilemma, which appeared because of privacy rights regulation disparity between EU and US. Additionally crucial proposals are being instructed how to solve this dilemma while abolishing open-ended provisions of PNR Agreements. The first part of master thesis reviews in theoretic aspect the importance of aviation security and its correlation with human rights. As air transportation remains a driver embodying freedom of movement it is essential to ensure its security but without detriment of civil liberties. The second part analyzes international and regional laws providing right to privacy, right to protection of personal data within necessity to ensure aviation security. Any intervention to privacy sphere is justifiable only by legitimate, reasonable and proportional means. The third part of this thesis evaluates the importance of PNR data protection, examines and criticizes EU-US PNR data bilateral agreements and proposes how to amend its' open-ended provisions. Finally in this part reader will be provided with the answer, why US having "security above all" approach should not require such drastic measures for intervening into personal privacy field in order to combat terrorism. Concluding thesis stresses out that by signing such inappropriate Agreements for itself and greatly affected by US pressure EU took unreasonable and disproportional risk to ensure transatlantic aviation security while intervening into privacy rights of own citizens.

Key words: PNR data, privacy vs. security, legal dilemma, combating terrorism, bilateral agreements, open-ended provisions.

Janulaitytė G. Aviacijos saugumas po rugsėjo 11-osios ir žmogaus teisės / Jungtinės tarptautinės teisės magistro baigiamasis darbas. Vadovas doc. dr. J. Žilinskas. – Vilnius: Mykolo Romerio universitetas, Teisės fakultetas, 2008. -

ANOTACIJA

Magistro baigiamajame darbe išanalizuoti ir įvertinti keleivio duomenų įrašo persiuntimo teisėtumo ir efektyvumo klausimai, iš Europos Sąjungos į Jungtines Amerikos Valstijas, siekiant užtikrinti aviacijos saugumą bei užkirsti kelią potencialiems teroro atvejams po rugsėjo 11-osios. Nagrinėjama privatumo vs. saugumo balanso dilema, atsiradusi dėl skirtingo ES ir JAV teisės į privatų gyvenimą teisinio reguliavimo, ir pateikiami pasiūlymai, kaip spręsti šią problemą šalinant pasirašytų dvišalių susitarimų nuostatų nekonkretumą. Pirmojoje darbo dalyje teoriniu aspektu aptariama civilinės aviacijos saugumo svarba ir jos ryšys su žmogaus teisėmis. Kadangi oro transportas išlieka vienas pagrindinių asmens judėjimo laisvės įprasminimo garantas, norint užtikrinti jo saugumą nedera pažeidinėti svarbiausių asmens teisių bei laisvių. Antrojoje dalyje nagrinėjami tarptautiniai ir regioniniai teisės šaltiniai, reglamentuojantys teisę į privatumą, asmeninės informacijos apsaugą ir kaip šios nuostatos turėtų atsispindėti užtikrinant aviacijos saugumą. Bet kokia intervencija į šias teises turi būti grindžiama legitimumo, pagrįstumo ir proporcionalumo principais. Trečiojoje dalyje aptariama keleivio duomenų įrašo apsaugos svarba, ES ir JAV dvišalių susitarimų dėl KDĮ persiuntimo efektyvumas ir kritika, pateikiami pasiūlymai dėl šių susitarimų pataisų, taip pat atsakoma į klausimą, kodėl JAV būdama „saugumas virš visko“ pozicijos neturėtų reikalauti tokių drastiškų asmens teisės į privatumą įsikišimo priemonių, norėdama pagerinti ir sustiprinti aviacijos saugumą kovoje su terorizmu. Magistro baigiamasis darbas užbaigiamas išvadomis, jog EU, pasirašydama jai nepalankius susitarimus ir pasiduodama JAV spaudimui, rizikuoja asmenų privačios informacijos saugumu ir visgi negarantuoja, jog tokiu būdu sumažės potencialių teroro išpuolių vykdant transatlantinius skrydžius.

Pagrindiniai žodžiai: asmens duomenų įrašas, aviacijos saugumas, privatumas vs. saugumas, teisinė dilema, kova su terorizmu, dvišaliai susitarimai.

SUMMARY

Janulaitytė G. Aviation security after 9/11 and human rights / Joint international law master thesis. Supervisor assoc. prof. dr. J. Žilinskas. – Vilnius: Mykolas Romeris university, Faculty of law, 2008. –

Master thesis researches and examines the legality and effectiveness of PNR data transfer from EU to US in order to ensure aviation security and diminish potential terror threat after 9/11. Also it is being debated about privacy vs. security balance dilemma, which appeared because of privacy rights regulation disparity between EU and US. Accordingly this thesis is essential in present because neither this legal dilemma has been solved yet nor adequate protection to PNR data guaranteed. That is why it is crucial to research new methods how effectively ensure aviation security without violating privacy rights. PNR data is an object of this thesis; relevantly to that thesis examines the necessity of equilibrium between right to privacy and guaranteed security, evaluates the input of 3 PNR data Agreements for obtaining aviation security and reduces potential terror threats, and proposes how to change its open-ended provisions. Hypothesis of this thesis is that EU US legal dilemma for ensuring aviation security can hardly be solved only by collection and transfer of PNR data. This measure can be used as additional and supportive but in narrower scale.

By using empirical phenomenological method and qualitative research I will reveal my critics and suggestions, based on gotten knowledge from wide ample of literature: 3 PNR data Agreements, EU and US legislation, International Conventions, statistical, interview sources from Lithuanian Civil Aviation Administration officers and etc. Diversity of opinions and literature leaves opportunity to make own conclusions and this way permits this thesis to be original and scientifically useful.

By such research thesis reveals that PNR data Agreements were beneficial only to US which pose the risk to EU citizens' privacy rights. Moreover, open-ended provisions of such Agreements allows to US act unilaterally and use collected PNR data uncontrollable. Making conclusions it is clear that by collecting PNR data aviation security is secured but not as effective as using other technical precautionary measures. Meaning that such unreasonable and disproportional way to fight terrorism mainly violates human right to privacy. The results of master thesis may intend to cause public awareness that collection of personal information in the airports and while booking the flight may leave consequences. Accordingly this research might serve travelers (mainly those who constantly travel to the US and do not know exactly about PNR data collection and interference into their privacy rights),

EU law makers who should consider upcoming PNR data Agreements more attentitive and should not leave possibility to the US be a dominant Contracting party. Finally this thesis will be useful for such audience, who is interested in international law and precisely EU- US cooperation on privacy rights matters. Presumably it will leave a lasting value for future researches on counterterrorism measures within aviation security and privacy rights scope.

Master thesis consists of 3 main parts: the first one reviews importance of aviation security as a mean to have freedom of movement, second one analyses privacy and security balance necessity within legitimate, reasonable and proportional dimension and last part examines and criticizes 3 PNR data Agreements, which were more negative to EU than positive in order to have safe transatlantic aviation.

Janulaitytė G. Aviacijos saugumas po rugsėjo 11-osios ir žmogaus teisės / Jungtinės tarptautinės teisės magistro baigiamasis darbas. Vadovas doc. dr. J. Žilinskas. – Vilnius: Mykolo Romerio universitetas, Teisės fakultetas, 2008. -

SANTRAUKA

Magistro baigiamajame darbe išanalizuoti ir įvertinti keleivio duomenų įrašo persiuntimo teisėtumo ir efektyvumo klausimai, iš Europos Sąjungos į Jungtines Amerikos Valstijas, siekiant užtikrinti aviacijos saugumą bei užkirsti kelią potencialiems teroro atvejams po rugsėjo 11-osios. Nagrinėjama privatumo vs. saugumo balanso dilema, atsiradusi dėl skirtingo ES ir JAV teisės į privatų gyvenimą teisinio reguliavimo, ir pateikiami pasiūlymai, kaip spręsti šią problemą šalinant pasirašytų dvišalių susitarimų nuostatų nekonkretumą. Remiantis tuo, kas paminėta, magistro baigiamasis darbas yra aktualus todėl, kad nei teisinė dilema, kilusi tarp ES ir JAV nėra išspręsta, nei užtikrintas tinkamas asmens duomenų įrašo apsaugos mechanizmas. Todėl svarbu vertinti, kokius naujus bei efektyvesnius metodus valstybės turi įdiegti, norėdamos turėti saugią aviaciją ir nepažeistas asmens teises į privatumą.

Keleivių duomenų įrašas yra magistrinio baigiamojo darbo objektas, per kurį bus vertinama privatumo *per se* ir užtikrinamo saugumo pusiausvyros reikiamybė, analizuojamas 3 ES-JAV dvišalių susitarimų indėlis užtikrinant aviacijos saugumą ir sumažinant potencialius teroro išpuolius bei pateikiami pasiūlymai, kaip pakeisti nekonkrečias tų susitarimų nuostatas, kurios suteikia JAV pranašumą.

Magistrinio darbo hipotezė yra susijusi su tuo, jog ES-JAV teisinę dilemą sudėtinga spręsti dėl netinkamų priemonių pasirinkimo. Tai yra, norint turėti saugią aviaciją neužtenka reikalauti tik keleivio duomenų įrašų, privaloma sukoncentruoti saugumo pajėgas tiek pačiame oro uoste, steriliose jo zonose, tiek ir užtikrinti keleivių bei jų bagažo patikrą. Keleivio duomenų įrašo persiuntimas ir kaupimas yra vienas iš potencialiausių būdų pažeisti asmens teisę į privatumą/ asmeninę informaciją. Todėl ši priemonė turėtų būti reglamentuojama tik kaip papildoma ir tik labai siauru mastu.

Naudojantis empiriniais fenomenologiniais tyrimo metodais bei kokybine analize magistro baigiamasis darbas pateiks kritiką bei pasiūlymus. Visa tai bus objektyvi ir patikima analizė, nes atlikta išanalizavus įvairią literatūrą- tarptautines konvencijas, susijusias su žmogaus teise į privatumą, privatų gyvenimą bei asmeninę informaciją, ES-JAV 3 dvišales sutartis dėl keleivio duomenų įrašo perdavimo,

kitus ES bei JAV teisės aktus, Centrinės Žvalgybos Valdybos ataskaitas, Amerikos „Saugaus Skrydžio“ darbo grupės specialisto Bruce Schneier tyriamuosius straipsnius apie aviacijos saugumą ir asmens teises, statistinius Eurobarometro ir RasmussenRaports duomenis, bei naudingą informaciją, gautą konsultuojantis su Lietuvos Civilinės Administracijos pareigūnais.

Literatūra pateikia skirtingas pozicijas, priklausomai nuo to, kurio subjekto šalininkai rašo atsiliepimus. Tačiau galutinės išvados darbe padarytos remiantis 3 dvišalių susitarimų teisinėmis ydomis, bei minėtojo JAV speicialisto praktinėmis analizėmis. Be to, nuomonių unikalumas ir skirtumai suteikia galimybę padaryti savas išvadas, dėl kurių magistro baigiamasis darbas tampa originalus bei novatoriškas.

Atlikus minėtą analizę stebėtina, jog dvišaliai susitarimai yra naudingi tik JAV, kuri kelią pastebimą grėsmę asmens privačios informacijos saugumui. Taip pat, nekonkrečios susitarimų nuostatos suteikia JAV galimybę vienašališkai interpretuoti jų reikšmę ir nekontroliuojamai disponuoti ES keleivio duomenų irašais su kitomis JAV institucijomis, vykdančiomis kovą su terorizmu.

Reziumuojant galima teigti, jog keleivio duomenų įrašo persiuntimas ir analizavimas JAV negali garantuoti visapusiško aviacijos saugumo, privaloma imtis kitų efektyvesnių ir netaip žmogaus teises pažeidžiančių priemonių (pvz. patobulinta griežtesnė keleivių bei bagažo patikra, naujos saugos instrukcijos lėktuve, lakūnų kabinos apsauga ir t.t.) ES prisiimdama įsipareigojimus pagal ydingą 2007 dvišalį susitarimą nenumatė, jog jis nėra pagrįstas, ir proporcionalus siekiamam tikslui kovoti su terorizmu ir apsaugoti civilinę aviaciją nuo grėsmių. Tokios išvados turėtų atkreipti visuomenės dėmesį ir būti aktualios ypač tiems asmenims, kurie dažnai keliauja į JAV, taip pat į šio magistro baigiamojo darbo išvadas turėtų atkreipti dėmesį ES teisės aktų kūrėjai, kuriems derėtų atidžiau ir griežčiau vertinti būsimus ES-JAV susitarimus dėl keleivio duomenų įrašo perdavimų bei nenusileisti JAV spaudimui derybose pasirašant teisės aktus, reglamentuojančius teisę į tinkamą asmeninės informacijos apsaugą. Taip pat šio darbo analizė būtų naudinga ir tiems subjektams, kurie domisi tarptautine teise ir ES- JAV bendradarbiavimu užtikrinant aviacijos saugumą po Rugsėjo 11-osios tragedijos. Tikėtina, jog ši analizė turės išliekamąją vertę ir ja galės pasinaudoti kiti tyrėjai, bandantys atrasti efektyvesnius būdus užtikrinti aviacijos saugumą nepažeidžiant žmogaus teisių ir laisvių.

Magistro baigaimasis darbas susideda iš trejų dėstomųjų dalių: pirmoji dalis analizuoja aviacijos saugumo svarbą ir pabrėžia, jog oro transportas išlieka vienas pagrindinių asmens judėjimo laisvės įprasminimo garantas, tačiau norint užtikrinti jo saugumą nedera pažeidinėti svarbiausių asmens teisių bei laisvių. Antrojoje dalyje nagrinėjami tarptautiniai ir regioniniai teisės šaltiniai, reglamentuojantys teisę į privatumą, asmeninės informacijos apsaugą ir kaip šios nuostatos turėtų atsispindėti užtikrinant aviacijos saugumą. Bet kokia intervencija į šias teises turi būti grindžiama

legitimumo, pagrįstumo ir proporcionalumo principais. Trečiojoje dalyje aptariama keleivio duomenų įrašo apsaugos svarba, ES ir JAV dvišalių susitarimų efektyvumas ir kritika, pateikiami pasiūlymai dėl šių susitarimų pataisų taip pat atsakoma į klausimą, kodėl JAV būdama „saugumas virš visko“ pozicijos neturėtų reikalauti tokių drastiškų asmens teisės į privatumą įsikišimo priemonių, norėdama pagerinti ir sustiprinti aviacijos saugumą kovoje su terorizmu. Magistro baigiamasis darbas užbaigiamas išvadomis, jog EU, pasirašydama jai nepalankius susitarimus ir pasiduodama JAV spaudimui, rizikuoja asmenų privačios informacijos saugumu ir visgi negarantuoja, jog tokiu būdu sumažės potencialių teroro išpuolių vykdant transatlantinius skrydžius.

ANNEXES

ANNEX 1

Types of PNR collected under the interim Agreements of 2004 and 2006 (34):

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address (es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/divided PNR information
17. E-mail address
18. Ticketing field information
19. General remarks

20 Ticket number

21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information (Other Service Related information)

27. SSI/SSR information (Special Service Information/ Special Service Requests)
28. Received from information
29. All historical changes to the PNR
30. Number of travelers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS (Advanced Passenger Information System) information
34. ATFQ (Automatic Ticketing Fare Quote) fields

Source: http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf [retrieved October 23, 2008]

ANNEX 2

Types of PNR collected under the 2007 EU-US Agreement (19):

1. PNR record locator code
2. Date of reservation/ issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flier and benefit information (e.g. free tickets, upgrades, etc.)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information): Although this data element puts together the previous data elements: address (6), billing address (8), contact telephone numbers (9) and email address (17), it cannot be excluded that additional information will be provided as well.
8. All available payment/billing information
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
15. All Baggage information: Seat information, including seat number
16. General remarks including OSI, SSI and SSR information
17. Any collected APIS information
18. All historical changes to the PNR listed in the numbers 1-18.

Source: EU Council (2007) // www.cyberlaw.pro/docs/pnragreement.pdf [retrieved October 23, 2008]