Biometrics, e-identity and the balance between security and privacy- The case study of Passenger Name Record (PNR) system

## 1. Introduction

The implementations of biometrics entail either the establishment of identity or the tracing a persons identity. Biometric passports (iris, finger, face e.g) can be used in order to verify the passenger's identity. The published proposal of European Commission for a Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, specially combating terrorism, raises security and privacy issues, which become more complicated due to the use of the above e-passports.[1]

The proposed PNR record contains all information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person. PNR data are related to travel movements, usually flights, and includhe passport data, name, address, telephone numbers, travel agent, credit card number history of changes in the flight schedule, seat preferences and other information. The collection and analysis of PNR data allows the law enforcement authorities to identify high risk persons and to take appropriate measures.[2]

Aftermath of the September 11 attacks a new emergency political-law status of the society is established: the continuous state of "war" against the so-called unlawful combatants of the "enemy". Officially the enemy is the

[1] See T *E. Brouwer,* The EU Passenger Name Record System and Human Rights Transferring passenger data or passenger freedom? CEPS Working Document No. 320/September 2009, http://www.ceps.eu

[2] See .H. *Tielemans,/ K Van Quathem/ D.Fagan/ A. Weber,* Personal Data The Transfer Of Airline Passenger Data to the U.S.: An Analysis of the ECJ, http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/PublicationAttachment/37f11b14-ff49-4e95-a5ce-2ee016f94329/oid23778.pdf Decision

terrorists although the victims of the privacy invasions through the above new form of data-processing are the civilians. The problem is that some measures against terrorism, for example an excessive data-processing system as PNR, may seem reasonable in a situation of war although they would never be acceptable in a time of piece. However, there is a tension between addressing terrorism as a crime and addressing it as a war.

The combination of the above PNR date and the system based on biometric, i.e fingerprint or iris or recognition in passports provoke with both new challenges and thinking about the balance between security and privacy. The condition for giving a visa permission and the asylum policies are also relative matters. This paper attempts to clarify the main aspects of this subject and to bring into question the compatibility of the above biometric PNR data base with the proportionality principle, which is fundamental in the processing of personal data in accordance with the Directive 95/46.

## 2. The legal framework

The data-processing based on biometrics is covered both by the Directive 95/46 E.C (hence "the Dir.") and the art 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms (hence " ECHR"). According to art 2 par. a of the above Dir personal data' shall mean any information relating to an identified or identifiable natural person : 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. In accrordance with art 8 of ECHR Everyone has the right to respect for his private and family

life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and 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. Respect for private life also consists of a the right to establish professional or business relationship[3]. It is sure that also ublic information fall within the scope of private life where it is systematically collected and processed in files held by the authorities. The ECtHR has emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data,such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual"

The provisions of the above piece of legislation constitute a concrete framework based on the following structure: The rule is that the processing is lawful when the data are processed fairly and in an adequate, relevant and not excessive way in accordance with art. 5 of the Dir. Although a binding international agreement between the EU and the US on privacy and data protection, in the context of the exchange of information for law-enforcement purposes, remains of the utmost importance, the EU seems to realize the necessity of a core of privacy-island in the middle of the processing "ocean" .

The above propose Framework Decision provides for the transfer or the making available by air carriers of PNR data of passengers of international flights to the Member States, for the purpose of preventing, detecting,

[3]See the Niemietz v. Germany judgment of 16 December 1992 decided case of ECtHR, http://webcache.googleusercontent.com/search?q=cache:YYgLG8pY_e4J:www.bartosz-bilinski.pl/hr/case_of_niemietz.ppt+see+the+Niemietz+v.+Germany+judgment+of+16+December+1992&cd=1&hl=el&ct=clnk&gl=gr

investigating and prosecuting "terrorist offences or serious crime.[4] In accordance with art 5 of the Dir personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards". In the EU data protection legal framework the before mentioned provisions generate the purpose specification princinple. The purposes for which data are collected should be specified not later than at the time of data collection and the use of the data should be limited to the accomplishment of those purposes. The breach of that principle constitutes an unlawful processing of personal data.

In the explanatory report of the above proposal it is mentioned that the scope of the proposal is limited to those elements which require a harmonised EU approach.[5] However there is not a certain limitation about the extent of the collected data of so many people, who are not officially either suspect or accused for any crime. Proportionality is often raised in general terms, without further explanation. The most critical question which relatively arises is the meaning of the proportionality principle and which factors are taken into account.

The principle of proportionality is a very important factor in the legal review of biometric systems. The question that arises is related with the specific criteria and factors used for evaluating the proportionality of processing biometric information. The application of the proportionality principle requires a certain duration of processing and a limited area of felonies which can be investigated through the collection of PNR data. According with the above proposal the data is to be kept for 5 years, which constitutes rather a

[4] *F. Aarts/J. Schmaltz/ F. Vaandrager*, Inference and Abstraction of the Biometric Passport http://www.mbsd.cs.ru.nl/publications/papers/fvaan/passport/

[5] See at http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14584_en.htm

disproportionate invasion of privacy in order to fight uncertain threats, if somebody takes into consideration that these data can be used for other purposes beyond fighting terrorism or serious criminality. It should also be noted that the general invocation of terrorism or serious crimes does not fulfil the requirement of purpose specification. There should be further clarification of the reason for the processing of the data.

## 3. **The new legal notion of privacy in a postmordern context of continuous fight against terrorism and serious or organised crime**

The interaction of a person with others, even in a public context, may fall within the scope of private life in accordance with the case law of the ECtHR[6] The emergence of a surveillance society has modified the above public context in order to strike a new balance between security and (social) privacy. A postmodern approach to human rights attempts to set a new paradigm for protection of privacy based on a non exceptional but continuous state of war against terrorism and organised crime. The question that arises is about the new criteria of interpretation of proportionality principle in order to establish a new legal doctrine about the extension of measures restraining privacy.

The beforementioned biometric technology creates new ethical issues of the so- called surveillance society. One of them is the above mentioned impact on privacy. The thinking about proportionality of the related constraints in privacy is based on a reversed rule: the collection, storage and prcessing of PNR biometric data constitute a necessary measure to safeguard security under EU data protection law. Today the above processing is not the ultima ratio of data protection law based on fighting against criminals, however a proper process through which a structure of security can be ensured. That acknowledgment implies some thoughts about justification of the related impact on privacy. In other words the legally considered invasion of privacy

[6]See P.G. and J.H. v. the United Kingdom, no. 44787/98, §§ 56-57, ECHR 2001 IX)

can be acceptable when the relevant data processing is the necessary measure to protect society from terrorism or serious crime. The result is that there is a proper ratio between the two above components.

The enhancing of security in order to assist criminal law enforcement agencies through the above PNR system constitutes a new, postomodern, Panoptikon,[7] as it is described sociologically in terms found in the work of *Michel Foucault*[8]. The majority of the people can be considered as suspects of crime through the collection, storage and processing of the above PNR data used by law enforcement agencies based on the invalidation of the presumption of innonence, in a permanent state of exception. In this context the majority can be accounted as internal and unlawful combatants of the enemy in a war between a State and their citizens[9]. Thus, a legal framework based on the exceptional processing of personal data can not adjust to the new rule of collection, storage and processing in order to fight terrorism and serious crime.

## 4. Conclusions

The published proposal of European Commission for a Framework Decision on the use of (PNR) data for law enforcement purposes raises security and privacy issues in a postmodern era, which could entail a wide interpretation of a justification of the above data processing based on the continuous fight against terrorism and serious crime. The provisions of the EU data-protection law based on the exceptional processing of data cannot imply in the new environment in which the majority of the people are considered as suspect of crime.

[7] See *A. Albrechtslund*, The Postmodern Panopticon: Surveillance and Privacy in the Age of Ubiquitous Computing
[8] *M. Foucault*, Discipline and Punish: The Birth of the Prison, 1975
[9] See *N.Chomsky* http://www.counterpunch.org/chomskyterror.html, P.Swire http://www.counterpunch.org/swire1.html