Olga Gurkova LL.M.[1]
Jovan Ananiev, Ph.D.[2]

National Security v. Protection of Personal Data in the EU

ABSTRACT:

This paper aims to provide a short overview of the European legislation regarding the fundamental right to protection of personal data, established by the Charter of Fundamental Rights in EU and its interconnection with the national security. This paper concerns the freedoms and the question of the degree of privacy that we are willing to sacrifice in order to obtain a high level of national security. National security cannot be achieved in isolation from fundamental rights. In order to achieve national security while safeguarding fundamental rights, we must carefully consider whether too much freedom is being sacrificed to achieve a high degree of security.

Key words: personal data, national security, European Union, privacy, human security, private life.

Introduction

State security has been a dominant concern in the field of international relations since the emergence of the nation-state. The state was supposed to protect the individuals from threats regardless of the threat source. However, as in the period before the emergence of supranational and International organizations the state was the sole protector, the protection was sometimes followed by a high price on the safety of the individual.[3] Hence, we may ask ourselves which one is more valuable - the right to privacy and private life, on one hand, or the national security of the entire state and all of its citizens, on the other?

There is an extensive overlap between the areas of human rights and security which are mutually re-enforcing and indispensable for each other. For some, human rights actually define human security.[4] The essence of human security is respect for human rights and fundamental freedoms while ‘’upholding human rights is the way to achieve individual, national and international security.’’[5] However, it does not imply that the concepts of “state security” and “human security” are mutually exclusive or that they cannot coexist. As a matter of fact, there are several good arguments in favor of the

[1] Teaching Assistant at the University Goce Delcev – Shtip, Law Faculty.
[2] Associate Professor at the University Goce Delcev – Shtip, Law Faculty.
[3] L. C., Berg: ‘*’The European Union’s human security doctrine: a critical analysis,*’’ Naval postgraduate school, Monterey, California, March 2009, p.44.
[4] О. Ѓуркова,: „Приватноста и правото на заштита на лични податоци во судир со националната безбедност, to be published in *Правник,* 2012.
[5] S., Tadjbakhsh, A. M. Chenoy: ‘*’Human security: concepts and implications,’’* Taylor & Francis, 2007 - Political Science, p.123.

conclusion that "state security" and "human security" need each other. Human security strengthens the security of national populations which means that it is in the self-interest of the nation-state to protect the basic human rights. As Benjamin Franklin reflected, those who would give up essential liberty to increase their security deserve neither.[6] It seems obvious that a wise balance must be struck between state security and human security.

Many different theories, including Realism, Idealism and Constructivism have emerged with regard to the origins of these threats and the manners in which they should be perceived and dealt with. Their connecting point is one common factor – the absolute primacy of the nation state. The proponents of the human security theory fundamentally challenge this way of thinking.

The ubiquitous idea, introduced by the the new principles in the 1990s' is security in an "extended" sense. The extension takes four main forms. In its *first* form, the concept of security is extended from the security of nations to the security of groups and individuals: it is extended downwards from nations to individuals. In the *second*, it is extended from the security of nations to the security of the international system or to the supranational physical environment: it is extended upwards, from the nation to the biosphere. The extension, in both cases, is towards the types of entities whose security needs to be ensured. In the *third* operation, the concept of security is extended horizontally or toward the sorts of security which are in question. Different entities (such as individuals, nations, and "systems") cannot be expected to be secure or insecure in the same way; the concept of security is therefore extended from military to political, economic, social, environmental, or "human" security. In the *fourth* operation, the political responsibility for ensuring security (or invigorating all of these "concepts of security") is itself extended. It is diffused in all directions, beginning from the national states, upwards toward the international institutions, downwards to regional or local government and sideways to nongovernmental organizations, to public opinion and the press and to the abstract forces of the market.[7]

What is personal data?

We will turn now to the extensive concept of the definition of personal data. ''Personal data'' means data relating to a living individual which is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the data controller.[8] It covers any information that relates to an identifiable, living individual.

---

[6] It was written as a part of his proposal to the Pennsylvania Assembly, as published in *Memoirs of the Life and Writings of Benjamin Franklin (1818),* www.archive.org/details/templefranklin02franrich.

[7] E. Rothschild: United Nations Research Institute for Social Development, "*What is Security?"* Daedalus 124, no. 3 (1995) p. 55.

[8] Official web site of the Data Protection Commissioner: http://www.dataprotection.ie/viewdoc.asp?DocID=568 last entry on 03.10.2011.

A comparable definition to the previous one is contained in the EU Data Protection Directive (95/46/EC): *''personal data'' shall mean any information relating to an identified or identifiable natural person (''Data Subject").* An *identifiable person* is one which 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.

This definition is very broad, but its broadness is deliberate. In principle, it covers any information that relates to an identifiable, living individual. There are different ways in which an individual can be considered ''identifiable". A person's full name is an obvious identifier. But a person can also be identified from other information, including a combination of identification elements, such as physical characteristic, pseudonyms, profession, address, mobile phone number, place and date of birth etc.

More extensive definitions on personal data are provided in Opinion 4/2007 on the EU Article 29 and the Working Party on the concept of personal data adopted on June 20.[9] The Working Party's analysis has been based on the four main "building blocks" that can be distinguished in the definition of personal data": (1) Any information, (2) relating to, (3) an identified or identifiable (4) natural person." These elements are closely tangled among each other, in order to determine together whether a piece of information should be considered as "personal data."[10]

Protection of personal data in the EU

Security measures need to be reviewed on a regular basis, in order to ensure that they are up-to-date and effective. The 2000 Charter of fundamental rights in the EU[11] provided a highly innovative contribution to EU data protection, as it recognized in its article 8 the right to data protection as an autonomous right, instead of a simple dimension of the right to privacy. This Charter established the right to protection of personal data as an essential right, ensured by independent supervisory authorities.[12]

[9] Opinion 4/2007 on the concept of personal data, adopted on June 20. Official Journal No. L 281 of 23.11.1995, p. 31.

[10] The full text of the Opinion 4/2007 on the concept of personal data is available on the website: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[11] The Charter of fundamental rights in EU (2007/C 303/01) proclaimed by The European Parliament, the Council and the Commission, entry into force on the date of entry into force of the Treaty of Lisbon.

[12] See Article 8 (3) of the Charter of Fundamental Rights of the European Union: "Compliance with these rules shall be subject to control by an independent authority."

EU legislation for data protection

The primary legal instruments of the European Union are:

a) Treaty on European Union (Article 6 and Article 39);

b) Treaty on the Functioning of the European Union, (Article 16) and Title V - Area of Freedom, Security and Justice (articles 67 - 89);

c) Charter of Fundamental Rights, (Article 8);

d) Declaration No. 20 on Article 16 B of the Treaty on the Functioning of the European Union and;

e) Declaration No. 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

The Data protection instruments of the EU are:

a) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23/11/1995, p. 31.

b) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ No. L 350 of 30/12/2008, p. 60;

c) Regulation (EC) 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, OJ L 8 of 12/01/2001, p. 1.;

d) Decision No. 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, OJ No. L 183 of 12/07/2002, p. 1.

The structural design of the fundamental rights in the European Union has developed over time and continues to evolve. As we stated already, for the purpose of ever more efficient protection and promotion of fundamental rights, data protection has gained the status of a separate fundamental right in the EU in the text of the Charter of Fundamental Rights (Article 8) and it is now related to, but distinct from the right to respect for private and family life under Article 7. This evolution is clearly visible when the EU Charter and the 1950 European Convention of Human Rights of the Council of Europe (ECHR) are compared. Under Article 8 of the ECHR:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

This feature sets the EU Charter of Fundamental Rights apart from other key human rights documents which, for the most part, treat the protection of personal data as an extension of the right to privacy.

In comparison, Article 8 of the EU's Charter of Fundamental Rights acknowledges the centrality and importance that the right to data protection has acquired in our society, as shaped by technological

developments.[13] At the same time, data protection is also emerging as a key EU policy area and the EU has been the key driving force for the development of legislation in many Member States. The inclusion of data protection as an autonomous fundamental right demonstrates the EU's recognition of the importance of technological progress, as well as an attempt to make sure that fundamental rights are taken in consideration in this progress. The undeniable fact that our lives are now becoming a continuous exchange of information, as well as the fact that we live in a continuous stream of data, means that the data protection regime is gaining importance and that it is moving toward the center of the political and institutional system.

As we stated previously, the ECHR does not envisage an explicit and an autonomous right to data protection, but data protection emerges from the jurisprudence of the European Court of Human Rights in Strasbourg, as an aspect of privacy protection.

Historically, the EU has played a key role in driving the development and introduction of national data protection law in a number of legal systems in the EU, especially where such legislation did not exist previously. An important instrument in this respect is the Directive 95/46/EC of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive").

There was a lack of data protection in the former third pillar of the EU. The main challenge faced currently by the EU in the field of providing the effective and comprehensive data protection arises from the constitutional architecture of the former EU pillars. While data protection was highly developed in the former first pillar of the EU, the data protection regime in the former third pillar cannot be regarded as satisfactory. Yet, the former third pillar of the EU concerned areas such as the police cooperation, the fight against terrorism and the matters of criminal law where the need for data protection is especially important. The Lisbon Treaty facilitates closing of this gap. Declaration No 21 to the Lisbon Treaty provides specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters, as well as in the field of police cooperation. This may prove to be necessary because of the "specific nature" of these fields. The Lisbon Treaty and its abolition of the former pillar structure of the EU opened the opportunity for the EU to widen its data protection regime. Limitations on data protection for security or defense or other legitimate purposes remain possible according to the Article 52[14] of

[13] Conference Documents, FRA (EU Agency for fundamental rights): *Data Protection in the European Union: the role of National Data Protection Authorities and Strengthening the fundamental rights architecture in the EU II,* Luxembourg: Publications Office of the European Union, 2010, p.6.

[14] Article 52, Charter of Fundamental Rights of the European Union, Official Journal of the European Communities (2000/C 364/01): Scope of guaranteed rights:

1. Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and

the Charter of Fundamental rights of the EU. However, it is very important to point out that these limitations need to be provided in a lawful procedure and with respect to the essence of the right to protection of personal data, as well as with regard to the requirements of necessity and proportionality. From the fundamental rights perspective, complete and total exclusion of certain areas from the scope of data protection legislation is problematic and it must be avoided.

In order to provide a lawful protection of personal data, it was necessary to establish an independent supervisory body responsible for monitoring the application of Community acts relating to the protection of personal data in the Community institutions and bodies.[15] The European Parliament and the Council adopted Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies.[16] This regulation establishes an independent supervisory authority, the European Supervisor, responsible for monitoring the processing of personal data by the Community institutions and bodies. In addition, each institution has a Data Protection Officer which cooperates with the European Supervisor and informs him in particular about the processing operations involving sensitive data. The regulations and general conditions governing the performance of the European Supervisor are established in Decision No 1247/2002/EC from July 1, 2002. The European Supervisor is responsible for advising all Community institutions and bodies, either on his own initiative or in response to a consultation, on all matters concerning the processing of personal data. The European Supervisor is consulted by the Commission when it adopts legislative proposals relating to the protection of personal data. He is also informed by the Community institutions and bodies about the administrative measures involving processing of personal data. The special office of the Data Protection Commissioner is established under the 1988 Data Protection Act. The Data Protection Amendment Act, 2003 updated the legislation, implementing the provisions of EU Directive 95/46. The Acts set out the general principle that individuals should be in a position to control how data relating to them is used. The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts and enforcing the obligations upon

freedoms of others. 2. Rights recognized by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties. 3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

[15] Provided by Article 286 of the EC Treaty.

[16] 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, *Official Journal L 008 , 12/01/2001 P. 0001 – 0022.*

data controllers. The Commissioner is appointed by the Government and he is independent in the exercise of his or her functions. Individuals which feel that their rights are being infringed can complain to the Commissioner who will investigate the matter, and take whatever steps may be necessary to resolve it.[17]

Public safety, defense and state security v. protection of personal data

Data protection in relation to national security

The purpose of this section is to identify the main problem areas connected with the exclusion from the data protection regime in the activities related to national security. Article 13, section (1) of the Data Protection Directive[18] (relating to exemptions and restrictions) specifies that "*Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 section (1), art. 10, art. 11 section (1), art. 12 and art. 21 when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security"*.[19] The exceptions listed in Article 13, section (1), from a to c of the Data Protection Directive are interconnected. In various Member States (Luxembourg, Denmark, Ireland, Romania, Greece and Portugal) they are identified as the principal areas excluded from the domain of data protection law.[20] This derives from the wording of Article 13 of the Data Protection Directive. Namely, Article 13, section (1) of the Data Protection Directive provides for broad exemptions and restrictions concerning public security, defense, state security (including the economic well-being of the State when the processing operation

[17] Materials available on the official web site of the European Data Protection Supervisor (EDPS), http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Brochures/brochure_edps_en.pdf , last entry 20.12.2011.

[18] EU Directive 95/46/EC: The Data Protection Directive. See also: http://www.dataprotection.ie/viewdoc.asp?docid=93 , last entry 01.10.2011.

[19] Article 13
Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) The protection of the data subject of the rights and freedoms of others.

[20] Conference on Data protection in the age of SWIFT, PNR, Prüm and e-Justice, Trier, 31 May - 1 June 2010, conference documents, p. 44.

relates to State security matters) and the activities of the State in the area of criminal law. There is a lack of clarity regarding the extent of these exemptions and restrictions. In some Member States, these areas are altogether excluded from the scope of protection in data protection law. That leaves a considerably large area unregulated and potential serious consequences for fundamental rights protection may occur. However, there are three important issues considered in relation to this provision.

Firstly, the phrasing allows for "restriction" in relation to the security issues. This is not construed as equivalent to "exemption" from the scope of application of the Directive. The grammatical interpretation is not the only reason for stating that the range of activities of various branches of the executive do come within the scope of the Directive. Secondly, the first preamble recital of the Directive sets the European Convention on Human Rights as the background of the processing of personal data. Further, the third preamble recital explicitly states that the fundamental rights of individuals should be safeguarded. Thirdly, the essence of the overall structure of the Directive is not to carve out an unsupervised field in which States may operate outside the requirements of the law. On the contrary, in case of confrontation with national security issues, a proportionality test should be binding, balancing the fundamental rights against the other interests of the state, thereby not letting superseding or overruling the rights because of the state interests. And fourthly, the Directive needs to be interpreted in line with Article 8 of the EU Charter of Fundamental Rights, which, according to the new Article 6 of the Treaty of the EU has "the same legal value as the Treaties." Article 8 may only be limited under the conditions set in Article 52 of the Charter. According to Article 52 of the Charter, any limitation of the rights and freedoms recognized by the Charter "must be provided by law and respect the essence of those rights and freedoms". It is for these reasons that the option of national legislatures to provide blanket exemptions for certain branches of the executive (such as intelligence services or the Ministry of defense) does not fit with the normative framework of the Data Protection Directive.[21]

Conclusion: Is the state security more valuable than the protection of personal data?

When we analyze data protection and the principle of respecting the fundamental rights of citizens, a few questions come to mind. Does it seem logical to say that the "compressing" of the fundamental rights of citizens is worth the sacrifice, if the gain is to fight terrorism or other treats to the national security? Should citizens be willing to sacrifice their personal data for successful criminal investigations? Does the right to protection of personal data need to be in "stand by" mode when there is a serious threat to national security?

[21] *Data Protection in the European Union: the role of National Data Protection Authorities, European Union Agency for Fundamental Rights,* Luxembourg: Publications Office of the European Union, 2010, p.44.

Nowadays, the democratic societies find themselves threatened by highly sophisticated forms of espionage and terrorism. In order to protect its citizens, State authority must find alternative ways for an effective fight against terrorism. By doing so, the state jurisdiction "plays" in the yard of the fundamental right, especially with regard to the right to private life and the right to protection of personal data. Hence, state authorities must cooperate among themselves and with the state authorities from other countries in order to provide fast and solid communication and exchange of data in criminal investigations. This cooperation sometimes includes exchanging personal data that incorporate not only name, surname, but also academic degree, addresses (particularly mailing address), birth identification number/national identification number, date of birth, age, sex, education, marital status, data relating to identity documents, phone numbers and e-mail addresses, business name, registered office, place of business, identification number, payment data and payment history, numbers of SIM cards, telephone number, internet trafficking data etc.

Our general view is that the counter terrorism policies should be proportionate to the scale of the challenges and that they should focus on preventing future attacks. Where efficient law enforcement in the EU is facilitated through information exchange, it must also incorporate protection of the privacy of individuals and their fundamental right to protection of personal data. Justice seems to gain the second place, after the service of security. Thus, individuals' security and liberty remain absent from the overall objectives of the strategy. The concrete steps presented by the Commission Communication exclusively serve "internal security" purposes and interests, an approach that positions the rule of law and fundamental rights (aside from formalistic sentences and announcements) at the margins.[22]

There is a natural and logical convergence between security and data protection requirements. Improving information security at the European level is a key success factor in improving the security of data processing operations, and therefore, it will benefit data protection. We can highlight the importance of establishing adequate links between security and data protection. The improving of the national security and data protection at the European level is a key factor to achieve success in improving the security of data. This is possible only by establishing the right link between security and data protection. This is enabled by the introduction of the Stockholm Program[23] along with the legal framework for the European Union. Paragraph 1 of the Program reads: "all the opportunities given and offered by the Lisbon Treaty to strengthen the area of freedom,

[22] HOUSE OF LORDS, European Union Committee, 17th Report of Session 2010–12 - *The EU Internal Security Strategy,* Ordered to be printed 17 May 2011 and published 24 May 2011, Published by the Authority of the House of Lords London : The Stationery Office Limited, p. 14 of 90.

[23] Council of the EU, "The Stockholm Program – An open and secure Europe serving and protecting the citizens, endorsed by the European Council of Brussels in December 2009.

security and justice for better citizens of the Union should be used by the institutions of the Union".

Several Conventions, Declarations, Treaties etc. provide exemptions from the right to protection of personal data. Many of them overlap each other. For instance, Article 14 of the Treaty of Prüm provides that contracting Parties shall *"provide one another with personal data if any final conviction or other circumstances give reason to believe that the data subject…poses a threat to public order and security."* Currently, data protection in relation to matters which belonged to the first pillar prior to the entry into force of the Treaty of Lisbon are governed by the Data Protection Directive,[24] while third pillar measures[25] are governed by the Data Protection Framework Decision.[26] It is unsatisfactory to have two such documents. Additionally, some of the most important law enforcement measures which rely on the collection, retention and use of personal data which should be governed by either the Directive or the Framework Decision are governed by neither, but have their own data protection provisions.

Our general conclusion is that enhancing security while at the same time safeguarding fundamental rights may result from a careful consideration whether too much freedom is being sacrificed to achieve a high degree of security. Security cannot be achieved in isolation from the rest of the world and it is therefore important to ensure coherence and complementarity between the internal and external aspects of EU security. Where efficient law enforcement in the EU is facilitated through information exchange, it is also necessary to protect the privacy of individuals and their fundamental right to protection of personal data.

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 of 23 November 1995, p. 31).

[25] Provisions on police and judicial cooperation in criminal matters formed a part of Title VI TEU prior to its amendment by the Treaty of Lisbon.

[26] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350 of 30 December 2008, p. 60).

Bibliography:

- Charter Of Fundamental Rights Of The European Union, *Official Journal of the European Communities (2000/C 364/01).*
- Conference Documents, FRA (EU Agency for fundamental rights), *Data Protection in the European Union: the role of National Data Protection Authorities and Strengthening the fundamental rights architecture in the EU II,* Luxembourg: Publications Office of the European Union, 2010.
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters *(OJ L 350 of 30 December 2008).*
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ No. L 350 of 30/12/2008, p. 60.*
- Data protection Commissioner, official web site, http://www.dataprotection.ie/viewdoc.asp?docid=93 , last entry 01.10.2011.
- Decision No. 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, *OJ No. L 183 of 12/07/2002.*
- Declaration No. 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281 of 23/11/1995* .
- E. Guild, F. Geyer: *"Security Versus Justice?: Police and Judicial Cooperation in the European Union,"* Radbound University The Netherlands and Kingsley, UK, Ashgate Publishing, 2008, Hampshire, England.
- E. Rothschild, *"What is Security?"* Daedalus 124, no. 3 (1995).
- European Data protection Commissioner, official web site http://www.dataprotection.ie/viewdoc.asp?DocID=568 last entry on 03.10.2011.
- European Data Protection Supervisor, official web site: http://www.edps.europa.eu/EDPSWEB/

- Cameron, *"National security and the European Convention on Human Rights",* Martinus Nijhoff Publishers, 2000.
- L. C. Berg: *"The European Union's human security doctrine: a critical analysis",* Naval postgraduate school, Monterey, California, March 2009.
- M. Fletcher, R. Lööf, W. C. Gilmore: *"EU criminal law and justice",* Edward Elgar Publishing, 2008.
- *Memoirs of the Life and Writings of Benjamin Franklin (1818),* www.archive.org/details/templefranklin02franrich
- Opinion 4/2007 on the concept of personal data adopted on 20th June, *Official Journal No. L 281 of 23.11.1995,* the full text of the Opinion 4/2007 on the concept of personal data is available on the website http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
- Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM (2011) 32 final, Council Document 6007/11.
- Regulation (EC) 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, *OJ L 8 of 12/01/2001.*
- S. Tadjbakhsh, A. M. Chenoy, *"Human security: concepts and implications",* Taylor & Francis, 2007 - Political Science.
- *Schengen Information System II* (SIS II) (March 2007; 9th Report, Session 2006–07, HL Paper 49), Chapter 6.
- The Declaration No. 20 on Article 16 B of the Treaty on the Functioning of the European Union.
- The EU/US Passenger Name Record (PNR) Agreement (June 2007;21st Report, Session 2006–07, HL Paper 108) and The Passenger Name Record (PNR) Framework Decision (June 2008; 15th Report, Session 2007–08, HL Paper 106).
- The Treaty on European Union.
- The Treaty on the Functioning of the European Union and Title V - Area of Freedom, Security and Justice.
- *Data Protection in the European Union: the role of National Data Protection Authorities,* European Union Agency for Fundamental Rights, Luxembourg: Publications Office of the European Union, 2010.

- О. Ѓуркова: „Приватноста и заштитата на лични податоци во судир со нациналната безбедност“, to be published in *Правник* 2012.