Professional paper
UDC 004.6.056.5:004.738.5:339(4-67EU)

REINFORCING TRUST AND SECURITY IN DIGITAL SERVICES AND IN THE HANDLING OF PERSONAL DATA [*]

Anna Tikhomirova [**]

ABSTRACT

This paper analyses the chapter of EU Digital Single Market Strategy concerning data protection and as a result increasing of citizens trust in cybersecurity area. The author provides the present legal basis for the protection of personal data and justifies the relevance of considered issue. The paper considers the main rights and principles in cybersecurity sphere and some statistical data related with citizens trust and the need of data protection. Summarizing the information the author emphasizes pros and cons of EU data protection reform and some suggestions for improving the regulation of data protection.

Key words: EU digital market, EU digital market strategy, data protection, digital services

1. INTRODUCTION

Rapid technological developments in the last two decades have brought new challenges for the protection of personal data. The scale of data sharing and collection has grown exponentially, sometimes taking place on a global level, and individuals are increasingly making personal information publicly available.[1]

[*] The paper was submitted for publication as a result of attending study program at Faculty of Economics and Business, University of Zagreb. The study program was implemented within Tempus project 544117 InterEULawEast, scholarship mechanism (WP. 4).

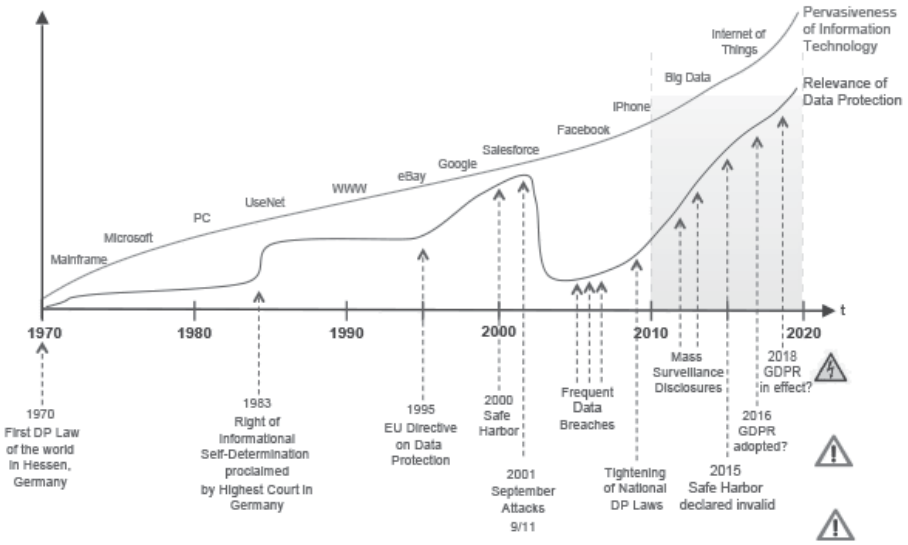
[**] Student of Tyumen State University, Institute of State and Law, Law department; yinxyang3@gmail.com.

[1] < http://www.consilium.europa.eu/en/policies/data-protection-reform/>, last access on 10/03/2016.

2. LEGAL BASIS

According to EU Data Protection Directive, *personal data* is "any information relating to an identified or identifiable natural 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" (Article 2a).[2]

The EU took a big step towards safeguarding a secure and open internet for Europe. Its five priorities – increasing cyber resilience; reducing cybercrime; developing the cyber defense policy; fostering EU industry; and promoting the core values internationally – remain essential.[3]



With a gradual emergence of different online sources the need of data protection increased as well as the regulation of it.[4] In nineteen seventy the first Data Protection law of the world was adopted. And by the end of 2015 a huge range of different sources using personal data and legal acts had been appeared.

[2] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, last access on 27/02/2016)

[3] <https://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-cybersecurity-strategy-28-may-2015_en>, last access on 3/03/2016.

[4] <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation>, last access on 10/03/2016.

Nowadays, there are several *main legal acts*, regulating the protection and handling of personal data:

- EU Data Protection Directive (also known as Directive 95/46/EC);
- European Cybersecurity Strategy (Cybersecurity Strategy of the European Union An Open Safe and Secure Cyberspace 7.2.2013 JOIN(2013) 1 final);
- European Agenda on Security (COM/2015/0185 final);
- the General Data Protection Regulation (COM/2012/11 final);
- e-Privacy Directive (**2002/58/EC**);
- Charter of Fundamental Rights of the EU (2000/C 364/01) (article 8).

The EU is committed to the highest standards of data protection, guaranteed by the Charter of Fundamental Rights. The modernization of EU data protection rules is a key enabler of the Digital Single Market as it will strengthen consumer trust in the digital economy.[5]

The Main Aims and Objectives of Digital Single Market Strategy at the sphere of personal data protection are:

- to prevent cyber threats and negative impact in the economy and fundamental rights;
- to develop industrial and technological resources for cybersecurity;
- to fulfill gaps in the fast moving area technologies and propose solutions for online network security;
- to adopt special rules applying to electronic communications services (the Network and Information Security Directive).

Directive 95/46/EC is a fundamental legal act that sets strict limits on the collection and use of personal data and demands that each Member State sets up an independent national body responsible for the supervision of any activity linked to the processing of personal data. It establishes main definitions in cybersecurity area.

In accordance with the Directive data processing is only *lawful* if:

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party; or

[5] <http://www.europa-nu.nl/id/vjtofdp38qwr/nieuws/questions_and_answers_digital_single?ctx=vh87km1jz6v2#p5>, last access on 8/03/2016.

- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or
- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

The *principles of data quality*, which must be implemented for all lawful data processing activities, are the following:

- personal data must be processed *fairly and lawfully*;
- special *categories* of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health etc.

The person whose data are processed, the data subject, can exercise the following rights:

- *the right to obtain information*;
- the data subject's *right of access*;
- the *right to object* to the processing of data.[6]

However, Directive 95/46/EC and other acts are not sufficient for comprehensive regulation in the 21th century.

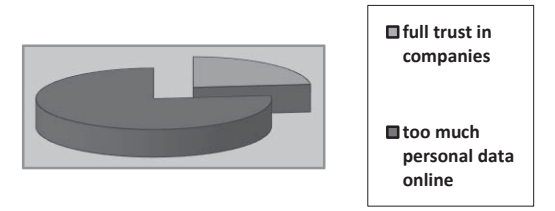
The European Commission put forward its EU Data Protection Reform in January 2012 to modernize the EU's 1995 data protection rules for strengthening online privacy rights and boost Europe's digital economy to make Europe fit for the digital age.

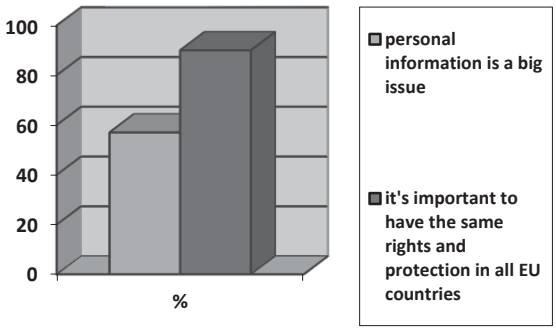
3. STATISTICS

According to the official information only 22% of Europeans have full trust in companies such as search engines, social networking sites and e-mail ser-

[6] < http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012>, last access on 13/03/2016.

vices and 72% of Internet users worry that they are being asked for too much personal data online.[7]





For 57% of Europeans disclosing personal information is a big issue and 90% of Europeans think it is important to have the same rights and protection in all EU countries.[8]

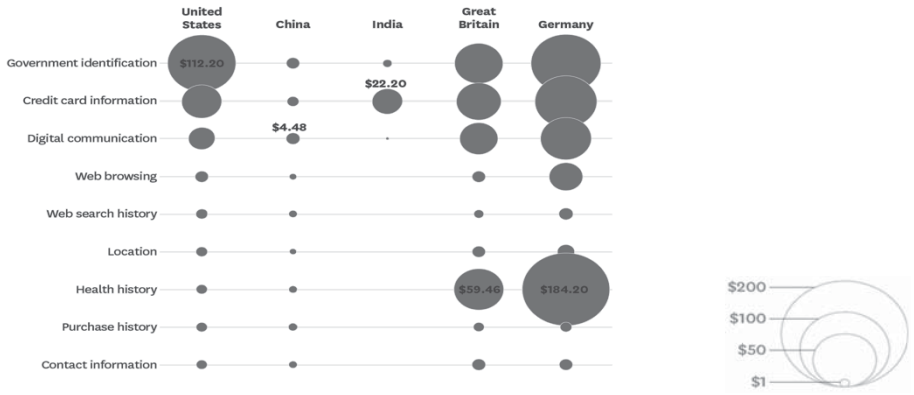
Analyzing the surveys of consumers in the US, China, India, Great Britain, and Germany reveal that they value some types of information much more highly than others.

As we can see people in the US, Great Britain and Germany would pay more (about one hundred dollars) to protect government identification data and credit card information (per person, US$, 2014). Moreover, citizens of Germany would pay one hundred eighty four dollars to secure their health history. And, on the contrary, people would pay less for the protection of web search history, location, purchase history and contact information. [9]

[7] <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX-%3A52015DC0192>, last access on 10/03/2016.

[8] <http://www.consilium.europa.eu/en/policies/data-protection-reform/>, last access on 10/03/2016.

[9] <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust/>, last access on 10/03/2016.



4. PRACTICE

The Weltimmo case (the Judgment of the Court of Justice of the EU (CJEU) (Case C-230/14) of 1 October 2015 was brought by the Hungarian data protection authority against property website Weltimmo, which operates a property advertising service in Hungary but is based in Slovakia. The advertising service was free of charge for the first month, and then subject to a fee. Several Hungarian advertisers e-mailed the Slovak company and requested deletion of their advertisement and their personal data following the expiry of the one-month free period. Weltimmo ignored such requests and transferred the advertisers' personal data who had failed to make payment to a debt collection agency.

Advertisers filed complaints with the Hungarian data protection authority, which imposed a fine of HUF 10 million (approximately €32,000) on Weltimmo, on the basis of breach of Hungarian data protection legislation.

The Hungarian data protection authority concluded that Hungarian (and not Slovak) law applied principally because: (i) Weltimmo collected the personal data in Hungary; and (ii) Weltimmo had a "Hungarian contact person" (a shareholder who was a Hungarian national residing in Hungary) who represented Weltimmo in Hungarian administrative proceedings.

The Hungarian Supreme Court hearing the case asked the CJEU whether the Hungarian data protection authority was competent to apply Hungarian data protection rules and impose fines.

In this case the CJEU interpreted the notion of establishment very broadly in this case. In its view, "establishment" is defined by: (i) the degree of stability of the arrangements; and (ii) the effective exercise of activities in that other Member State. The CJEU further stated that the concept of "establishment"

"extends to any real and effective activity – even a minimal one – exercised through stable arrangements". The notion of "in the context of the activities" was already broadly defined by the CJEU in its Google Spain judgement (C-131/12), to which reference is made in the Weltimmo judgement.

The Weltimmo judgment is potentially far-reaching and may make data protection compliance for some businesses offering services/products or otherwise operating across multiple Member States more difficult and burdensome. Companies which offer their services via the Internet in various jurisdictions should carefully consider whether to locate their staff and other facilities in the countries where they do not want to be deemed established, to avoid being subject to data protection compliance in several Member States. Internet businesses may find it more difficult to claim that local laws are not applicable to them outside the country of their "main" establishment.

In many respects, this judgment arguably brings forward certain proposed changes to the applicable law rules set out in the draft of General Data Protection Regulation, which would make any entity offering goods or services into the EU subject to EU data protection laws.[10]

This case underlines the importance of the adoption of one data protection act for all member states, because it'll simplify the functioning of businesses.

5. CONCLUSION

Over the recent years people have become much more concern about their personal data in different e-systems, on-line services and within the business processes. Digital single market strategy in the frame of personal data protection has substantial advantages for people and businesses and could get various economic benefits through the trust of users.

However, it still has some disadvantages, such as:

- an awareness of citizens about what kind of data a specific public authority processes;
- an inherent conflict between new privacy and security by design requirements in the proposed GDPR and the "once-only" principle, which can be solved by *adopting the system of certain technical requirements* for the processing of data.

[10] <http://www.allenovery.com/publications/en-gb/Pages/New-ground-breaking-CJEU-decision-on-applicable-data-protection-law.aspx>, last access on 10/03/2016.

Adoption and implementation of DGPR

- is the main goal for achieving a new level of data protection;
- will simplify secure of data, because of the existence of one act for all member states;

According to statistics people in EU worry about their personal data and free access to their information that's why right to be forgotten is one of the most important rights in new strategy.

In addition, there is a need for improving literacy in IT field by carrying out special lectures in different institution (schools, universities etc.).

LITREATURE

EU LEGISLATION

1. Digital Single Market Strategy COM/2015/0192 final, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192.
2. EU Data Protection Directive 95/46/EC, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.
3. Cybersecurity Strategy of the European Union An Open Safe and Secure Cyberspace 7.2.2013 JOIN (2013) 1 final, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:PDF.
4. European Agenda on Security COM/2015/0185 final, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC018.
5. General Data Protection Regulation COM/2012/11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
6. E-Privacy Directive 2002/58/EC, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.
7. Charter of Fundamental Rights of the EU 2000/C 364/01, available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

CASE LAW

1. Case C-230/14, Weltimmo s. r. o. v Nemzeti Adatvédelmi **és** Információszabadság Hatóság, available at http://curia.europa.eu/juris/document/document-jsf?text=&docid=168944&pageIndex=0&doclang=EN&mode=lst&dir=&occ=-first&part=1&cid=182564.

INTERNET SOURCES

1. <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation>
2. <http://www.europa-nu.nl/id/vjtofdp38qwr/nieuws/questions_and_answers_
3. digital_single?ctx=vh87km1jz6v2#p5>
4. <http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm>
5. http://www.allenovery.com/publications/en-gb/Pages/New-ground-breaking-CJEU-decision-on-applicable-data-protection-law.aspx
6. <https://edri.org/files/DSM_Analysis_EDRi_20150617.pdf>