ACTA TECHNICA CORVINIENSIS
– Bulletin of Engineering
Tome IX [2016] , Fascicule 1 [January – March]
ISSN: 2067 – 3809

Anna Barbara SZABÓ

THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA FROM THE PERSPECTIVE OF DATA PRIVACY

[1.] Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, HUNGARY

Abstract: While the data protection policies of the United States of America (USA) tend to differ state-by-state, the European Union is aiming to create and apply a unified legal system in all of its 28 member states, which during their accession process; all European Union candidate states must integrate into their legal system. In the USA, there is often a greater emphasis on the liberty of speech and the freedom of press, than the right to informational self-determination. This complicates those legal proceedings, which are commenced by a European state against contents, which are hosted on websites by an American hosting company. Furthermore, the USA, in the name of fight against terrorism, – often unwarrantedly and improperly by European Union legal standards – is collecting data during international trading and personal transportation, which violates the human rights accepted by the European Union. Due to the actuality of the topic, I shall compare the data privacy regulations of the European Union and the USA.
Keywords: data privacy, regulation, European Union, the USA, trans-Atlantic relationship

HISTORICAL OVERVIEW

There is a perceptible difference between the evolution of the legal systems of the two powers: in Europe, the typical predominance of the continental legal system prevails, with its codification, and the preponderance of the written law against jurisprudence. Meanwhile in the USA the common law, known as the Anglo-Saxon law is dominant, which prefers jurisprudence-making precedents, which allow different interpretation of the law in different legal cases even in the same state. [1]

The professional literature classifies the European data privacy protection as a third generation system, which initial purpose was to lessen the dependency of the citizens towards the state in regards of obtaining public information. Second generational data privacy regulations have brought the emergence of the right of informational self-determination, while the third generational legislation was shaped by developments of the business world and the advancements in technology. As civilization progressed, the demand for a transparent state, the right to have access to and disseminate public information and for the freedom of information came to prominence, besides the protection of personal information. This has also brought about the need for transparency in the use of public funds at state- and other public bodies. The aforementioned factors have considerably supported the democratic operation of the state. The appearance of the data of public interest helps it by way of the folk control democratic function, it encourages administrative organs' efficiency, the citizens to give birth the participation of truth, the corruption and state abuses in public affairs appearance, which one yielded the right of the expressions of an opinion. [2]

The protection of information in the European Union is determined by a data protection directive of the OECD (Organisation for Economic Co-operation and Development), based on international consensus, which came into force in 1980. An essential purpose of this directive is to enable the smooth operation of economic relations whilst protecting private information. The principles laid down by the OECD have influenced the creation of the Council of Europe's agreement, titled “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, which was approved in 1981. [3]

In 2001, the office of the European Data Protection Supervisor's was created, in order to ensure that all the institutions and bodies of the European Union have the appropriate respect to the citizen’s private life during the processing of personal data. [4]

In contrast, the citizens’ right for the protection of their private information is significantly weaker than in Europe, despite Samuel Warren's and Louis Brandeis' study, published in 1890, which found that

the advancement of technology can be intrusive to one's privacy. This necessitated the creation of a new system for the protection of one's right to informational self-determination. This system has matured by the 1970s, when it was decided – citing fundamental rights –, that the citizens should be protected against large state records. Hereafter I shall present the most significant milestones of this process, based on a study, by András Molnár. [6] [7]

In 1928 in the case of Olmstead vs. the United States, with a majority decision the Supreme Court held that telephone intercepts without a court order do not violate basic constitutional rights, because physically, the constitution regards the protection of privacy only within the house. It was because of this decision, that Louis Brandeis had formulated the "right to be let alone". The "right of privacy", only as an umbrella term was relatively lately introduced to the basic constitutional legal concepts in the 1960s, but still, it is not explicitly mentioned in the Constitution of the United States.

William Prosser, as a professor of law classifies the right to privacy into the legal system of compensation, where he views the public disclosure of private facts as a violation of the right to privacy, which results to a disadvantage for those affected, regardless of veracity. He defines the action of libel as a separate category, as well as the possession of image, name and other identifiers. Later, Gary Bostwick established the principle, that third parties should have access only to a certain protected zones to information about the individual.

In 1977, a judgment, made by the Supreme Court in regards to the Whalen vs. Roe case has established, that the interests, which are affected by issues related to the private sector are made up by several separate interests, which include information on the individual and its right to remain a secret. [8]

In a study by David Solove in 2006, he views the unauthorized collection of information, the abuse of information, which have been legally obtained and the publication of such information to the general public unconstitutional.

In summary, the U.S. does not apply a standard law for data privacy, because it is possible to interpret it differently from one Member State to another. In despite of some courts having declared the protection of data privacy as a basic right, there is no single official supervision. Another vulnerability presents itself as only American residents, and those with valid residence permit are subject to the Privacy Act (the federal data protection law).

RELATIONSHIP BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA

As the development of the information society continues, privacy and the right to informational self-determination can succeed less and less. In regards to data, lesser-developed countries are becoming increasingly vulnerable against more developed countries, which by the exploitation of the technological rift are carrying out unreported data mining. One way to reduce such dependency is to legitimize data collection between countries by mutual agreements and the establishment of proper safeguards. The legal harmonization of the OECD and EU satisfies this principle.

The "Safe Harbor" was created to facilitate the transmission of data to the United States. The assurance of the protection of private data during its processing is the most cardinal requirement of transmitting data to a third country. According to the Committee of the European Union, data transfer to the U.S. is considered to have an accepted level of safety, when the recipient U.S. Company is on the Safe Harbor list. The Safe Harbor list contains those Companies, which have agreed to meet the Safe Harbor data protection directives, set forth by the government of the United States.

The legal basis for all these are the 2000/520/EK (July 26th 2000) resolution of the European Committee based on the 95/46/EK directive of the European Parliament and the Safe Harbor act for providing adequate data protection, issued by the U.S. Department of Commerce, which contains all the data protection directives, that a U.S. based Company should meet. [9]

In the context of the Stockholm-program, the European Parliament has asked the European Commission to make a proposal for negotiations with the USA regarding data protection aimed at law enforcement and data exchange. The task force, based on the 29th article chaired by Jacob Kohnstamm has found that the passenger name records (PNR) of the U.S. collects such vast amounts of personal data of citizens travelling from the EU, which clearly is beyond the principles of necessity and proportionality. It states, that the fight against crime and terrorism does not justify the mass surveillance and tracking of passengers. Such police-like methods in EU member states are only feasible in special cases and within constitutional boundaries. The task force has also stated that it has not been presented with any statistics, which compares the number of criminals caught with the assistance of the PNR system with the number of surveyed passengers, which would justify the need for such surveillance. Thus, the task force recommends narrowing the range of personal data managed by the PNR system. In agreement with the European Data Protection Supervisor, the task force considers the recording of special data by the U.S. Department of Homeland Security unacceptable. Furthermore, it considers the 15-year long preservation of such data disproportionate, considering that according to the

EU Charter of Fundamental Rights such data needs to be anonymized or deleted six month after use.
The European Data Protection Supervisor supports the logging and documentation of each access to PNR data, so proper use by the U.S. Department of Homeland Security can be verified. [10] [11]
The trans-Atlantic partnership plays a significant role in the foreign politics of the EU, which aims to develop a trans-Atlantic market by 2015. In the framework of a trans-Atlantic partnership the European Union expects its partners to accept the values which it represents. Such values are democracy, human rights and the rule of law, sustainable economy and sustainable growth. The protection of these values must be assured even during the defense from global threats, such as terrorism. Despite the USA and EU being the world's largest bilateral trading partners, which causes economic dependence, nevertheless some acts of the U.S. – of which the European Parliament has on several occasion called on the U.S. Government to cease – often contradict the values represented by the European Union. Such acts are the penalties by death still accepted by a number of U.S. States, the maintenance of the Guantanamo Bay detention center and the unilateral visa requirement against some EU member states. The records of persons, suspected to be involved in terrorism and proven innocent are not being deleted from the database, furthermore the U.S. keeps records of their namesakes and last, but certainly not least – the controversial data mining done by the U.S. National Security Agency. For example: NSA confessed it, that Angela Merkel and the Greek government tapped his members' telephone, and more hundred users Google and Yahoo's drawer;[1] between 2004-2012 French economic leaders' interception[2], CIA to which the door was showed because of spying chief from Germany.[3] The possibility that BND is German intelligence service arose on the other hand data it tracked recruited and European leaders for NSA.[4] The USA's senate accepted it meanwhile USA Freedom Act-ot, which differs from European Union norms likewise. [12]
Concept definition differences may cause a problem the uniform data protection in questions. Since it is English language areas Data Protection, you are Data the personal data understand his protection by Security. The information security, you are INFOSEC expression generally the electronic information it is used for protection. NATO in a standard Security of masks the administrative safety under Information. [13]

SUMMARY

The difference between the two powers goes beyond its historical roots. Despite that the United States itself is composed of numerous member states as well, its foreign policy does not view the European Union as a singular entity, and continues to show differences in treatment while dealing with EU member states.
The interpretation of data privacy and informational right to self-determination in the U.S. differs significantly from that of the EU. On the long term, the problems mentioned earlier can endanger the trans-Atlantic relationship. Related negotiations drag on exceptionally currently with the partnership, currently inside European Union debates it is accompanied by them.

References:

[1.] Katalin Gönczi Katalin - Pál Dr. Horváth Pál - István Stipta - János Zlinszky: Egyetemes jogtörténet (Nemzedékek Tudása Tankönyvkiadó, 2002.,ISBN: 9789631945720)
[2.] András Jóri: Adatvédelmi kézikönyv, OSIRIS KIADÓ KFT., 2005.
[3.] Gazdasági Együttműködési és Fejlesztési Szervezet (OECD), általános tájékoztató (Downloads:http://oecd.kormany.hu/az-oecd-rol, 11.09. 2013.)
[4.] Az Európai és a Tanács 95/46/EK irányelve (10. 24. 1995) (Downloads:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML, 11.09. 2013.)
[5.] Az Európai Adatvédelmi Biztos, általános tájékoztató (Downloads: http://europa.eu/about-eu/institutions-bodies/edps/index_hu.htm,11.09. 2013.)
[6.] Adatvédelmi Biztos honlapja, általános tájékoztató (Downloads: http://abi.atlatszo.hu/index201.php?menu=usa, 11.26. 2013.)
[7.] András Molnár: A magánszférához való jog az Amerikai Legfelsőbb Bíróság joggyakorlatában (Downloads: http://dieip.hu/wp-content/uploads/2011-2-11.pdf, 11. 25. 2013.)
[8.] Tamás Győrfi: Az amerikai alkotmányjog szabadság-fogalma (Downloads: http://jesz.ajk.elte.hu/gyorfi4.html,.11.25. 2013)
[9.] Adatvédelmi Biztos honlapja, általános tájékoztató (Downloads: http://abi.atlatszo.hu/index201.php?menu=safe harbour, 11.26. 2013.)

[1] referring to: http://mno.hu/hirtvarchiv/beismerte-az-nsa-hogy-lehallgattak-merkelt-1192975; (07.09. 2015.)
[2] referring to: http://444.hu/2015/06/29/az-nsa-nem-csak-a-francia-elnokoket-de-a-francia-gazdasagi-vezetoket-is-lehallgatta/, (07.09. 2015.)
[3] referring to: http://hu.euronews.com/2014/07/11/parbeszedet-kezdemenyez-a-berlini-kemugy-miatt-az-amerikai-kulugyminiszterium/, (07.09. 2015.)
[4] referring to: http://444.hu/2015/05/29/belgium-vizsgalatot-indit-a-titkos-adatgyujtes-miatt/, (07.092015..)

[10.] A stockholmi program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa 2010/C 115/01 (Downloads http://eur-lex.europa.eu/Notice.do?mode=dbl&ihmlang=en&lng1=en,hu&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=513011:cs, 12.01. 2013.)
[11.] 29. cikk szerinti adatvédelmi munkacsoport, 00664/11/HU WP 181, 10/2011 sz. vélemény „az utas-nyilvántartási adatállomány (PNR) felhasználásáról a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntető eljárás alá vonása érdekében" című, európai parlamenti és tanácsi irányelvre irányuló javaslatról, 2011. április 5. (Downloads: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_hu.pdf, 12.01. 2013.)
[12.] Az Európai Unió Hivatalos lapja: P6_TA(2006)0238 EU–USA transzatlanti partnerségi megállapodás, C298 E/226, 2006. 12.18.(Downloads: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:298E:0235:0235:HU:PDF, 11.26. 2013.)
[13.] Security within the North Atlantic Treaty Organisation (NATO)-C-M(2002)49 (Donhttp://www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf, 11.26.2013)

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING

ISSN:2067-3809