Bartosz Marcinkowski

Can the United States provide a higher standard of personal data protection than the EU?

Some comments on selected state regulations[1]

The view established in EU Member States assumes that the level of personal data protection in EU Member States (and the EU as such) is much higher than that provided by the US legal system. This assumption will (presumably) find its validation in relation to the US federal law. However, many of the solutions found at the state level in the US are only now being introduced into the EU system (and that of the EU Member States). The article highlights that such established views (or stereotypes) can be unfounded (and may lead to even more unsubstantiated conclusions).

1 The importance of transatlantic relations and the challenges of the digital economy

In the globalizing world, with the growing role of China and the Pacific-region states, the significance of complex, mutual economic, political, scientific, cultural and social relations between the European Union and the United States is not to be underestimated. The importance of these relations is reflected in the value of trade between the EU and the US, estimated at the beginning of the 21st century at about USD 120 billion per year; this estimate does not take into account non-quantifiable benefits from scientific and cultural exchange. The United States has been and continues to be the biggest importer of EU goods and services.[2] Today, the "fuel" driving the world's economy are data, including in particular personal data, containing information on specific individuals. It is said that data are the "new coal" of modern economy.[3] This digital economy is the result, among other things, of the unprecedented development of technologies for processing and exchanging data on a massive scale[4]. Polish researcher Marek Safjan points out that we are experiencing "an explosion of, until recently, unheard of possibilities of data collection and processing".[5] An illustration of this progress is, *inter alia*, the universality and ease of access to the Internet and its features.[6]

Given the importance of transatlantic relations, as briefly presented here, the elimination of barriers overly or unduly hindering relations between the EU and the US on various levels should

1 The author of this article would like to thank Professor Marie-Theres Tinnefeld (Munich University of Applied Sciences) and Professor Irena Lipowicz (Cardinal Stefan Wyszyński University in Warsaw). This article could not have been written without their support and encouragement.

2 R. Bendini: The European Union and its trade partners, fact sheets on the European Union, July 2015 (http://www.europarl.europa.eu/ftu/pdf/pl/FTU_6.2.1.pdf). See also: M. Krzysztofek: Personal data protection in the European Union after the reform. Commentary on the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Warsaw, 2016, p. 238.

Bartosz Marcinkowski

PhD candidate at the Cardinal Stefan Wyszyński University in Warsaw, Partner at DZP law firm in Warsaw

E-Mail: bmmarcinkowski@gmail.com

3 C. Schwab: The Fourth Industrial Revolution. What It Means and How to Respond, [in:] Foreign Affairs Anthology Series, 12 December 2015 (//www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution).

4 Point 4 of the preamble to Data Privacy Directive 95/46/EC and Explanatory Memorandum – Proposal for a General Data Protection Regulation, COM (2012) 11 final, p. 2.

5 M. Safjan: Personal data protection-informational autonomy boundaries, [in:] Personal Data Protection, M. Wyrzykowski, ed. Warsaw, Poland, 1999, p. 9.

6 For example: T. Craig, M. Ludloff: Privacy and Big Data, Sebastopol, CA, 2011, p. 3. See. also Y.A. de Montjoye, C.A. Hidalgo, M. Verleysen, V.D. Blondel: Unique in the Crowd: The privacy of the bounds of human mobility, Nature.com Scientific Reports 25 March 2013 (http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html#ref20) and P.P. Swire: The Second Wave of Global Privacy Protection. Symposium Introduction, [in:] Ohio State Law Journal 74/2013, pp. 842-852, and the United States of America, Federal Trade Commission: Complaint on Facebook, Inc., (0923184) (http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf). On the legal aspects of social networking sites see P. Fajgielski: The processing of personal data on social networking sites – selected legal aspects, [in:] Electronic media. Contemporary legal issues K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016, pp. 152 ff.

be one of the ways of stopping the declining trends observable in relation to the global position of Europe and North America.[7]

The said barrier can arise as a result of, in particular, any potential excessive limits on personal data transfers from EU Member States to the United States. In American literature such restrictions are referred to as non-tariff barriers to trade.[8]

The concept of "adequate level of personal data protection" occurs in the law of the European Union as a fundamental measure of data security in a third country, such as the United States.[9] Only assessing "the adequacy of the level of protection" allows for a legal transfer of personal data to a third country. However, the legal regulations in place do not define the said notion.

At the same time, a common view in the European Union is that the United States does not ensure an adequate level of protection of personal data. Emphatic expression of this view was given by the Court of Justice of the EU in its judgment in the case Maximillian Schrems v Data Protection Commissioner in October 2015.[10]

The paralysis of transatlantic trade, scientific and cultural exchange, in the absence of systemic solutions legalizing the transfer of personal data from EU countries to the United States, is not the result of the application of special and exceptional *ad hoc* solutions allowing for data transfer to the United States in spite of the persistent lack of certainty as to their safety and future fate (although the said *ad hoc* accessory remedies result in some improvement of the level of data protection in a country such as the United States[11]).

However, while the Directive 95/46 dealt with the assessment of the level of adequacy of personal data protection in a third country (article 25 of the Directive) *en bloc*, the General data protection regulation differentiates in that regard, referring to, in addition to the concept of a third State, *inter alia*, "territories" and their regulations in force (article 45 of the General Regulation). This regulation, which will apply from 25 May 2018, further justifies studies on personal data protection regulations in individual US states. It cannot be ruled out that the state regulations not only provide an adequate level of personal data protection in the territory of a given state, but provide better data protection than the EU regulations. Such studies may be conducive to the pursuit of convergence, understood as a process of harmonization of views and, consequently, uniform regulation of identical or at least substantially similar areas.[12] One manifestation of the convergence can be the interoperability of legal systems understood as "building bridges between different data protection systems".[13]

2 Selected regulations on personal data and privacy of information protection in the light of selected US state legislation

A brief and necessarily selective presentation of the legal regulations in the field of information privacy in force in several US states is important in order to become aware of the full complexity of the regulatory environment in the United States, in the light of the traditional American federalism which is the basis for US statehood, with fifty state legislations that require the development of federal (inter-state) conflict-of-law rules.[14] It should be emphasized that, despite any doubts as to the adequacy of the level of protection of personal data in the US legal system at federal level, local regulations often significantly contribute to raising the level of personal data protection in individual US states. Moreover, federal regulations sometimes force individual states to adopt and implement advanced rules in this area – for example, in order to obtain federal funds (grants) for the development of education, a given state must provide legal mechanisms for the protection of personal data of children.[15]

In the following section the focus will be on Californian regulations since they are considered to be the most advanced and comprehensive.[16] Furthermore, in view of its large population and developed high-tech industry, California is justifiably considered the state whose legislation is the most advanced in this field among US states.[17]

Firstly, therefore, we should examine the Constitution of the State of California which guarantees privacy not only in vertical relations (with state authorities), but also in horizontal relations (between private sector entities), as referred to below. Pursuant to Article 1 ("Declaration of rights") section 1 of the Constitution of the State of California, all people are by nature free and independent and have inalienable rights, which, apart from the right of enjoying and defending life and liberty, acquiring, possessing, and protecting property, also includes the right of "pursuing and

7 Cf. I. Lipowicz: Poland's public administration in the light of European standards, [in:] Administrative law Z. Niewiadomski, ed., Warsaw 2011, p. 335. With regard to the results of removing trade barriers see Z. Lewicki: The history of US civilization. The era of contradictions 1787 – 1865, Warsaw 2010, pp. 111 and 112.

8 P.M. Regan: American Business and the European Data Protection Directive: Lobbying Strategies and Tactics, [in:] Visions of Privacy. Policy Choices for the Digital Age, C. J. Bennett, R. Grant, eds., Toronto, Buffalo, London, 1999, p. 211, and P.P. Swire, R.E. Litan: None of your business. World Data Flows, Electronic Commerce, and the European Privacy Directive, Washington D.C. 1998, p. 144-on. See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Digital agenda for Europe, Brussels, 26.8.2010, COM(2010) 245 final/2,.

9 See art. 25 and subsequent of the Data Privacy Directive 95/46/EC and art. 45 of the General Data Protection Regulation (EU) 2016/679, which will apply from 25 May 2018 (OJ EU L 2016 No 119, p. 1 on.

10 C-362/14.

11 M. Jagielski: Prawo do ochrony danych osobowych. Standardy europejskie [The right to the protection of personal data. European standards], Warsaw 2010, p. 197.

12 For more on this topic, including the disappearance of structural homogeneity in legal systems see R.D. Kelemen: Eurolegalism, Cambridge, Massachusetts, London, England, 2011, p. 5 ff., and M. Ancel: Znaczenie i metody prawa porównawczego [The importance and methods of comparative law], Warsaw, 1979, p. 12.

13 C. Kuner: Transborder Data Flows and Data Protection Privacy, Oxford 2013, p. 176. For an extensive study on the interoperability see B. Szafrański: Interoperacyjność rejestrów publicznych [The interoperability of public registers], [in:] Rejestry Publiczne. Jawność i interoperacyjność [Public registers. Openness and interoperability], A. Gryszczyńska, ed., Warsaw, 2016, p. 57 ff.

14 P.M. Schwartz, J.R. Reidenberg: Data Privacy Law, A Study of United States Data Protection, Charlottesville, Virginia 1996, pp. 8 and 9, and M. Ancel: Znaczenie i metody prawa porównawczego [The importance and methods of comparative law], Warsaw, 1979, p. 89.

15 42 U.S.C. § 5106a(b) – Grants to States. Available on the website: http://www.law.cornell.edu/uscode/text/42/5106a.

16 P.M. Schwartz, J.R. Reidenberg: Data Privacy Law, A Study of United States Data Protection, Charlottesville, Virginia 1996, p. 132.

17 P.P. Swire, K. Ahmad: Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws, and Practices, Portsmouth, NH 2012, p. 44.

obtaining safety, happiness, and privacy".[18] It is hardly doubtful that the regulation also applies to information privacy, similar to, if not identical with personal data protection. This regulation also applies to the horizontal relations (among private sector entities), as confirmed by the judgment in the case Hill v. National Collegiate Athletic Assn of 1994.[19] It should be noted that other state constitutions, if mentioning the right to privacy, usually refer to the protection of privacy in vertical relations, and therefore in terms of US constitutional law, which in the traditional manner, protects individuals against interference of the authorities. Such is the example of the Constitution of Florida, in which Article 1 ("Declaration of rights") section 23 "Right of privacy" stipulates protection of the individual against illegal (that is to say: not allowed by the provisions of the Constitution) interference on the part of the authorities ("free from governmental intrusion") in the sphere of private life of individuals[20] and allows a wide access to government documents (which is a significant modification of the federal Freedom of Information Act[21]).

Both of the above examples clearly demonstrate that the direct constitutional regulation of privacy, including informational privacy, is not, in principle, contrary to the American republican system. The significance of this conclusion is not reduced by the fact that state case law in balancing opposing interests and values does not automatically confer primacy to information privacy (personal data protection).[22]

California is usually in the vanguard of change. From this perspective, not only the said regulation by state constitution should be noted, but also its expansion in relation to the public sector by the California Information Practices Act of 1977, which, *inter alia*, stipulates a broad right of access of the data subject to the information gathered about it.[23]

Another interesting piece of legislation, with regard to the private sector, is the California Financial Information Privacy Act of 2004 (known as SB1)[24], whose aim is to enhance legal protection of individuals by expanding and supplementing the federal Gramm-Leach-Bliley Act (GLB Act).[25] In accordance with the SB1 regulation, financial institutions are required to obtain an "affirmative consent" (§ 4051 (b) (2) SB1) for the transfer of any "non-public personal information" (section 4052(a) of the Act) to any entity not related to that institution. These non-public data are defined as data that cannot be obtained from publicly available official records, media or information subject to making them public under regulations in force (section 4052 (a) (1)-(3) of the Act).

This regulation hence significantly expands the protection of individuals granted by the federal GLB Act mentioned above. The corresponding federal law grants the consumer only the right to oppose the transfer of personal data to an entity not related to the data administrator (simple opt-out).[26]

Another noteworthy regulation is the California Business and Professions Code (Cal. Bus. & Prof. Code), Sections 350-352, and in particular Article 7, entitled "Personal Information and Privacy Protection"[27], establishing the Office of Privacy Protection, acting within the California Department of Consumer Affairs.[28] This Office focuses mainly on interventions in connection with notifications relating mainly to "identification theft", invasive business practices in relation to personal data and consumer privacy and Internet personal data bases. In addition, the Office also engages in dissemination and educational activities.[29]

In accordance with the California Civil Code Section 1798.82 (a) (Cal. Civ. Code), the Office of Privacy Protection plays a major role in connection with the regulation requiring business entities operating in California to notify consumers/authorities in the event of a breach (or even suspected breach) of data security. Such notification should be addressed in the first place to data subjects,[30] but in the event of the so-called "substitute" notification (that is through the media) the business entity is obliged to inform the said Office. In addition, in the event of issuing notification to more than 500 recipients, the data security breach incident should also be notified to the California Attorney General.[31] It is worth mentioning that the "data security breach notification" is a good example of the so-called "California effect" -- currently, virtually all US states have their own regulations regarding the mandatory notification of personal data security breaches.[32]

California Civil Code Section 1708.8 also stipulates detailed regulations facilitating the assertion of rights in the event of physical invasion of privacy. Personal data protection breaches are included in this category. The statutory test used to examine privacy breaches refers to a reasonable expectation of privacy.

It is worth mentioning that the said Code was amended (effective 1 January 2015), further enhancing the protection of person-

18 The Constitution of the State of California of 1879, article 1, section 1, as amended as a result of a universal referendum in 1974. The text of the Act is available online: http://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml.

19 Hill v. National Collegiate Athletic Assn. 865 P.2d 633 (1994). The judgment is available online: http://law.justia.com/cases/california/cal4th/7/1.html.

20 The Constitution of the State of Florida of 1968, article 1, section 23 as amended in 1998. The text of the Act is available online: http://www.leg.state.fl.us/statutes/index.cfm?mode=constitution&submenu=3#A1S23.

21 The Freedom of Information Act (FOIA), 5 U.S.C. § 552, https://www.foia.gov/.

22 Cf. on this topic: F.H. Cate: The Changing Face of Privacy Protection in the European Union and the United States. Indiana Law Review, Vol. 33, 1999; Indiana Legal Studies Research Paper Series, p. 210. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=933090.

23 Available online: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/StateInformationPracticesAct.aspx.

24 Available online: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=04001-05000&file=4050-4060.

25 The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338).

26 I would like to point out that while the primacy of SB1 over GLB Act is indisputable, the relationship between the SB1 and the less pro-consumer federal FCRA regulation was the subject of legal disputes – cf. D.J. Solove, P.M. Schwartz: Privacy, Information and Technology, Austin, Boston, Chicago, New York, The Netherlands 2009, p. 388.

27 The text of the Act is available on the website: http://law.justia.com/codes/california/2005/bpc/350-352.html.

28 See http://www.privacy.ca.gov/.

29 See data provided by: D.J. Solove and P.M. Schwartz: Privacy, Information and Technology, Austin, Boston, Chicago, New York, The Netherlands 2009, p. 469.

30 The California regulation stipulates the obligation to notify about the breach in data security: "(...) notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cf. Section 1798.82(a) (Cal. Civ. Code). The text of the regulation is available on the website:
http://www.dmv.ca.gov/pubs/vctop/appndxa/civil/civ1798_82.htm.

31 For more information on the topic see the following web page of the California Office of Privacy Protection:
http://www.privacy.ca.gov/privacy_laws/breach_notices.shtml.

32 The EU legislative body also intends to introduce the obligation of notification of data breaches –see articles 31 and 32 of the draft general data protection regulation.

al information of California residents, for example, by prohibiting the sale of Social Security Numbers.

3 Conclusions

Presenting selected provisions of some state regulations may be important for bringing closer the positions and for determining which solutions are "inadmissible" in view of different traditions and legal cultures.

My brief analysis indicates that the state of California regulations provide in some areas a high standard of personal data protection, and that the protection, which should be emphasized, has its source in the state Constitution. It can be established that, in accordance with the California-effect, as described in the literature, strict rules will be applied to new areas, and the Californian solutions will be gradually adopted in other US states.[33] Among the most interesting solutions applied in California, one may in particular include the requirement of notifying data security breaches to the state data protection authority. Such an obligation will be widely applied in the European Union pursuant to articles 33 and 34 of the General data protection regulation, only starting in May 2018. Hence, in certain areas, US state regulations may establish a higher standard of data protection than EU practice, widely regarded as exemplary.

The author hopes that the conclusions formulated in this brief article can contribute to developing a European position in the debate about a transatlantic, systemic protection of personal data. The debate will to a large degree determine the future of the increasingly digital world, and take place in the face of Brexit, with President Donald Trump questioning the need and the ideas behind the Transatlantic Trade and Investment Partnership (TTIP), and a rise in isolationist policies and attitudes in the United States.

33 C.J. Bennett, C.D. Raab: The Governance of Privacy. Policy Instruments in Global Perspective, Cambridge, Massachusetts, London, England, 2006, pp. 114 and 269-276.