RULES FOR THE PROTECTION OF PERSONAL DATA IN THE U.S. LEGAL SYSTEM

Araz Poladov
(*apoladov@llm20.law.harvard.edu*)
Harvard Law School, MA, US

Abstract

21st century can be surely called an era of digital and technological innovations. Information technologies have deeply penetrated almost every sphere of our lives. Nowadays, information is one of the most valuable assets the state, organizations or individuals can possess. Because of the importance of data in the hands of businesses, organizations and states, collection, processing, use and retaining of personal data poses certain significant risks. To cope with unauthorized collection of data and to provide a legal framework within which operations on data may be carried out, many jurisdictions enacted comprehensive and detailed data protection acts. Unlike those jurisdictions, the U.S. has no single data protection legislation, and a mix of laws enacted on both federal and state levels serve to protect the personal data of U.S. citizens and other subjects. Also, guarantees offered by these statutes differ from one state to another, while the acts in themselves are sector-specific. Another chunk of data protection norms is based on precedents and case law. This article seeks to track the development of notion of privacy in the U.S., explore the interplay between state and federal statutes, evaluate the scope of protection and offer analysis of case law and its importance in shaping the doctrine of personal privacy.

Keywords: *data protection, personal data, personal information, reasonable expectation of privacy, right to privacy, privacy, information privacy, human rights, international law, GDPR, 14th Amendment, Safe Harbor,*

1. Introduction

The right to privacy strengthened its position in the United States at the end of the 19th century. Although the right to privacy in the United States was initially a British political legacy, court decisions in England were more conservative and cautious than those of American judges.

One of the important features of this right in the Anglo-Saxon legal system is that it was previously established by judicial precedents and legal doctrine. It should be noted that the right to privacy was not among the subjective rights provided for in the American Bill of Rights.

The doctrinal approach, in particular, the famous article "The Right to Privacy" by Samuel D. Warren and Louis D. Brandeis in the issue of Harvard Law Review dated December 15, 1890 played a crucial role in the formation and development of the right to privacy in the United States in the modern sense, and correctly identified the direction of development of the legislation of the United States in terms of privacy. Moreover, it was a major step forward in the further development of this right in both the Anglo-Saxon legal system and the continental legal system. Although the article points out that this right already exists in France and should be recognized in the United States, it draws attention to differences in methodological approaches to this right in countries with continental and common law systems.

There is no specific article in the US Constitution on the inviolability of private life. However, the activity of the courts in this country has revealed the constitutional basis for the protection of private rights in the broadest sense from the interference in certain confidential areas of private life. It is based on the protection of individual liberties from state interference and is enshrined in the Fourth, Fifteenth and Fourteenth Amendments to the US Constitution.

2. Protection of Privacy at a Federal level

In general, there is a sectoral approach to data confidentiality in the United States. There is no specific federal law that guarantees the confidentiality and protection of personal information. Instead, legislation at the federal level primarily protects data in certain sectors. Unlike the General Regulations of the European Union, the United States is based on the existence of federal and state laws, administrative regulations and sectoral rules for self-regulation. Security measures to protect privacy depend on the specific area, and there are a number of legislative acts and court precedents in this regard. These acts apply only to specific areas such as "health, education, communications, protection of children's rights and financial services or data collection on the Internet"[1] . Although at first glance, comparative lawyers have a negative attitude towards the US system on the protection of privacy, the US system of personal data protection is more reliable and sophisticated than the European system.

There is no single comprehensive data protection act in the United States. In the United States, data protection laws are inconsistent. They usually apply to government agencies, not private ones. There are some laws that regulate individual institutions, but they are very specific, that is, they apply only to a certain area or area of application. In addition to the laws, there are some precedents that comment on constitutional protection, which are also close to defining the right to protection of personal data.[2]

At the federal level, the most important laws are the Privacy Act of 1974 and the Freedom of Information Act 2000. However, they only apply to federal agencies.

The Privacy Act of 1974 defines the procedure for the processing of personal data - the procedures for the collection, storage, use and dissemination of personal data stored in the databases of federal authorities. At the same time, citizens are given the opportunity to obtain information about themselves stored in the databases of these agencies, and it is prohibited to correct, add or disclose this information without the written consent of the person.

The Freedom of Information Act sets standards for government electronic resources for the circulation of personal data. The Act allows anyone to gain access to records kept by federal agencies, with a few exceptions. Two of the exceptions provide some degree of data protection. First, access to personnel and medical records and open documents and similar documents that may openly and unjustifiably infringe on personal information, and second, access to records or information compiled for law enforcement purposes is not permitted.

Similar provisions are enshrined in the Privacy Act of 1974, although most of the data protection principles set out in the OECD Guidelines and EU directives are met, and this Act only applies to records kept by federal agencies. The Privacy Act (a) restricts the disclosure of records without the consent of one person; (b) requires that most records be kept; (c) provide the right of access and the right to make notes, and (d) allow agencies to (1) maintain records, "only collect such information about the person concerned and necessary to achieve the purpose of the agency" (2) "collect information from the entity as directly as possible"; (3) the person requesting the information, (i) the authority to inform, encourage, (ii) the purpose and (iii) the usual methods of using the information, and (4) the accuracy, relevance, and timeliness of the "name of the official and official address" (5) "to the extent necessary to ensure fairness to a person" and (6) to establish appropriate technical and administrative procedures to ensure the security and confidentiality of records and to protect against threats to security or integrity;[3] .

The protection of personal data has always been the focus of the commercial and financial sectors. Legislation in this area is constantly improving. The first and most important of these laws is the Fair Credit Reporting Act of 1970. This Act extensively regulates the collection and disclosure of information protected by credit institutions. Under the Act, credit institutions must apply "reasonable procedures to ensure the highest possible accuracy" of the information held in them, as well as provide a wide disclosure procedure for those who wish to challenge the

completeness or accuracy of any information. Disclosure of any credit report to other individuals or legal entities is prohibited.

In general, the Federal Trade Commission, an independent law enforcement agency in the United States that has become a privacy agency, plays an important role in protecting personal information. In addition, the main legal functions of the Federal Trade Commission derive from Section 5 of the Federal Trade Commission Act (1914). The jurisdiction of the Federal Trade Commission consists of identifying and prosecuting breaches of confidentiality by organizations whose information practices are considered "fraudulent" or "unfair"[4] . In this sense, the Federal Trade Commission is a broad consumer protection system used to prohibit dishonest or misleading actions related to disclosure and protection procedures for the protection of personal data.

In addition to its authority to crack down on fraudulent or unfair trade practices, Congress authorizes the Federal Trade Commission to enforce a number of sectoral laws, including the Children's Online Privacy Protection Act (1998), the Equal Credit Opportunity Act (1974), and the Fair Credit Reporting Act (1970), Fair Debt Collection Practices Act (1977) and Telemarketing and Consumer Fraud and Abuse Prevention Act (1994) should be mentioned. Several other Acts give the Federal Trade Commission, a centralized grievance and consumer protection institution, broad powers.

In addition to the legislation under the jurisdiction of the Federal Trade Commission, there are a number of other important laws in the field of sectoral legislation at the federal level, including the following in terms of protection of personal data:

• Financial Services Modernization Act (Gramm–Leach–Bliley Act (GLBA) (15 USC §§6801-6827));

• Health Insurance Portability and Accountability Act (HIPAA) (42 US, § 1301 et seq.);

• Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act);

• Electronic Communications Privacy Act (US 18 § 2510);

• Computer Fraud and Abuse Act (18 US. §1030).

Now let's interpret these laws through the prism of personal data protection. First of all, let's start with Financial Services Modernization Act (Gramm–Leach–Bliley Act (GLBA).

This Act protects the "non-public" personal data of consumers when used by financial institutions. According to the Act, "Personal data" or "Non-public personal data" means personal financial information provided by a consumer to a financial institution; information obtained as a result of a transaction with a consumer or service provided to a consumer or information obtained by another financial institution. In any case, sensitive personal information is protected. Personal information open to the public is not protected.

According to the Act, during the processing of personal data, financial institutions may, if necessary, transfer information to individual companies for the provision of financial services. Necessary personal information may be provided to credit reporting authorities or financial regulators on a legal basis.

According to the Act, a commercial organization does not have the right to transfer the buyer's personal information to third parties if the transaction is carried out legally. Compulsory measures related to the transfer of personal data are possible in case of violation of the Act. The Federal Trade Commission is responsible for enforcing consumer protection legislation, but its activities have been widely criticized.

Proponents of the Act argue that the policy of regulating personal data should include a description of the terms of use of the service in a language that is clear and understandable to the user, specify that user data is stored accurately, who stored it and for what purpose. Critics argue that the effectiveness of personal data protection depends on the ability to evade the requirements of the Act, and to increase it, it is necessary to develop methods to inform the user

about the legal consequences, as well as a comprehensive understanding of how the data will be used.[5]

The Health Insurance Portability and Accountability Act of 1996 defines personal data as follows: "protected health information" means health information that can be identified individually, except as provided in paragraph 2 of this definition, i.e.: (i) electronic media transmitted by; (ii) information stored in electronic media or (iii) transmitted or stored in any other form or medium.

Regarding the processing of personal data, the Act states that the Safety Rules set minimum requirements for all health facilities and contractors that require administrative, physical and technical security measures to protect the confidentiality, integrity and availability of data from all information processors, as well as information on safety incidents. also requires.[6]

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, initiated by Senators Conrad Burns and Ron Wyden, regulates the collection and use of email addresses. The Act covers all e-mail communications, the main purpose of which is to advertise or promote a commercial product or service, including all commercial communications defined as e-mail promoting content on commercial sites.

The Act applies to any legal or natural person who sends and sends commercial messages by e-mail. Critically, this Act gives commercial email recipients the right to require marketers not to continue to send them emails.[7] The main purpose of the Act is to cover all commercial communications designated as any e-mail message intended to trade or promote a commercial product or service. This includes all emails that promote the product on commercial sites.

The Act does not exclude e-mails between businesses, as messages sent to former customers announcing new products must also comply with the Act. It is important to note that the CAN-SPAM Act does not create the right of individual action for consumers, on the contrary, the main responsibility for the implementation of the Act lies with the Federal Trade Commission. Many federal and state agencies, along with Internet service providers, have the opportunity to apply the provisions of this Act.[8]

The Electronic Communications Privacy Act of 1986 prohibits the eavesdropping of the personal data of other persons without the prior consent of one of the parties and without the permission of the court. Prohibits the use or disclosure of any information obtained as a result of illegal eavesdropping or electronic surveillance

The Computer Fraud and Abuse Act aims to prevent and punish hacking activities, which it defines as "unauthorized access" to secure computers. In addition, the Act prohibits individuals or legal entities from leaving the "permitted" area.

The Fair and Accurate Credit Transactions Act was adopted in 2003 as a key piece of legislation designed to protect personal information related to remote services. This Act is specifically designed to protect consumers from theft and to ensure that consumer credit information is accurate. The Act requires three major credit reporting agencies in the United States to provide free credit reports to consumers once a year. To increase the security of information related to plastic cards, the Act requires retailers that print payment card receipts to use PAN truncation (personal account number truncation) so that transaction receipts do not include the full consumer account number.[9] The Act also provides for a provision that allows consumers to place fraud warnings on credit documents so that they can track certain types of purchases to protect them from fraud.

We noted earlier that the protection of children's rights in the United States is a matter of special concern and always relevant. The main normative legal act in this area is the 1998 Act on the protection of children's privacy on the Internet.

This Act regulates the collection and use of information obtained from children under 13 years of age through Internet sites and mobile applications. Congress designated the Federal

Trade Commission as the primary body responsible for enforcing the Act and authorized it to interpret and enforce the Act.

In 2000, the Federal Trade Commission announced for the first time the rules for the protection of children's online privacy in order to implement the Act. These Rules detail the rules governing the collection and use of personal information about children and about them on the Internet. This Federal Trade Commission Regulation restricts the collection and processing of personal information about children by website operators or online services when using child-centered web services. However, violations of children's rights are common on the Internet due to the development of new technologies and advertising activities.

In particular, in 2013, the Federal Trade Commission amended the Act to expand the definition of "personal information" and include permanent identifiers that identify users over time and in various online services. All behavioral ads on Internet child center services now require parental notice and consent. The Act requires websites that publish information and advertisements about children to publish a privacy policy that specifies "what information the operator will collect from children, how the operator uses such information, and how the operator discloses this information."[10]

This applies to operators of websites or services intended for children, including manufacturers of mobile applications and "any operator that knows that it collects personal information from a child." The Act also requires website operators to obtain a more secure consent method if they attempt to disclose a child's personal information to third parties or make it public.

One of the specific acts in the field of personal data protection is the Video Privacy Protection Act of 1988. The Act was passed "to prevent the illegal sale of rental recordings or video-cassettes, video games. Congress passed the Act after the publication of the story of Robert Bork's rental video during his candidacy for the Supreme Court. This creates a liability for any "video cassette service provider" that is liable for loss of rental information of up to $ 2,500 outside of normal business practices.

This Act, also known as the Bork Act, defines "personal information" as "information that identifies a person in order to request or receive a particular video material or service." The Act allows the disclosure of such information to any person with the written consent of the consumer. At the same time, the Act allows a consumer to disclose his name and address if he has "the ability to make such a statement openly and clearly."

3. The role of judicial precedents in shaping the right to privacy

Finally, judicial practice and court decisions made at different times play an important role in regulating legal relations in the field of personal data protection in the United States.

It should be noted that until the 1970s, the decisions of US courts did not provide the necessary protection of privacy. In Whalen v. Roe (1977), the Supreme Court unanimously ruled that the registration of a specific centralized database in New York State containing the names and addresses of persons prescribing certain drugs does not violate the right to privacy. The Supreme Court ruled that various types of protected privacy interests include "preventing the disclosure of personal documents." The Supreme Court also noted that in various situations, the interests of the state take precedence over the interests of the individual.[11]

Until the end of the twentieth century, information about the inviolability of privacy was not provided with the necessary legal protection in US courts. Thus, in its ruling of Whalen v. Roe, the Supreme Court acknowledged that New York State law, which requires doctors and pharmacists to report all prescriptions for certain medications to the state and keep them in comprehensive databases, does not violate privacy rights, despite protests from some patients and doctors.

Some experts have even described the US Supreme Court's decision as an invasion of privacy. However, there were many supporters of this decision. The point is that the Supreme

Court has put the interests of the state above the interests of the private life of the people in monitoring the information on drug control. At the time, there was an opinion in US society that, although some courts recognized the inviolability of personal information, courts should balance their decisions and, in any case, make their decisions independently, taking into account the public interest.[12]

In its judgment of 18 June 1981 in the case of the United States v. Westinghouse, the US Ninth Circuit Court prepared a "balance test" to be used in deciding between competing interests. When looking for such information, it is necessary to refer to some factors that need to be taken into account. At the same time, the harm that can be done to a person with subsequent statements; measures to protect information from any disclosure and issues of public interest in disclosure were also clarified in the Decision.[13]

In Katz vs. US (1967), Supreme Court ruled that the Fourth Amendment to the U.S. Constitution prohibits wiretapping without a formal warrant, although the Supreme Court ruled that "confidentiality" reasonable expectation "criterion was applied.[14] The decision in Katz v. United States demonstrated significant changes in U.S. law, as the Supreme Court reconsidered its position in its 1928 decision, Olmstead v. United States. However, the decision stated that the 4th and 5th amendments to the US Constitution were not related to wiretapping. It should be noted that the "reasonable expectation of confidentiality" test is still used to determine the limits of state control. For example, in January 2012, the Supreme Court overturned a conviction based on data from a GPS tracking device installed in a drug dealer's vehicle.[15]

In Stanley v. Georgia (1969), the Supreme Court interpreted some specific provisions of Amendments 1 and 14 to the country's Constitution as protection of privacy, especially privacy, at home (mainly in this precedent, some confidential, secret, intimate items and information should be kept at home). In Roe v. Wade (1973), the Supreme Court recognized that the 14th Amendment allowed abortion. In Eisenstadt v. Baird case (1972), the right of single couples to contraception was recognized based on the Griswold v. Connecticut precedent and the principle of equality.

In Planned Parenthood of Southeastern Pennsylvania v. Casey (1992), the U.S. Supreme Court, based on Roe v. Wade the precedent, acknowledged that several provisions of Pennsylvania's Abortion Control Act were unconstitutional, as well as the doctor's duty to inform the woman about the negative consequences of abortion, the woman's obligation to inform her husband or parents before the abortion, and the obligation to postpone abortion for 24 hours.[16]

In its ruling, Doi v. Chao (2004), the Supreme Court interpreted the provisions of the Privacy Act of 1974 in connection with the minimum amount of compensation for violations of the right to privacy. The Supreme Court ruled that the provisions of this Act require a refund of $ 1,000 without the obligation of the plaintiff to prove the amount of damages and non-pecuniary damage, and if the plaintiff demands a large amount of compensation, the amount must be proved.[17]

These judgments have a limited scope and do not have a significant impact on the private sector, where there are many questions about privacy and confidentiality.

4. Conclusion

Under modern US law, the right to privacy is defined as the "right to be let alone." This concept encompasses a number of different rights that protect against personal interference in state relations or activities, the right of everyone to make independent decisions about their life choices. This right is not absolute. The right to privacy does not protect against certain socially dangerous behaviors, such as illicit drug use.

Thus, the development of the right to privacy in the United States has evolved from the recognition of doctrinal and judicial precedents to the formation and improvement of a system of specific legal acts that comprehensively regulate the right to privacy in various fields of human

activity. In the early stages of the formation of the doctrine of the right to privacy, the decisions of the British courts, which American authors often saw more than the British, had a serious impact on this process.

Continental law (primarily French law) also plays an important role in the formation of the right to privacy in the United States. The doctrinal impact of American law on EU legal concepts must also be assessed, as the United States already had a well-established judicial practice on the subject when the European Convention for the Protection of Human Rights and Fundamental Freedoms and the initial documents on the protection of personal data emerged.

But so far we can talk about serious differences in the concepts of the right to privacy in US and EU law. Modern EU standards place higher demands on the protection of personal data than American standards[18] .

References:

1. Terry, N. Existential Challenges for Health Care Data Protection in the United States // Third Ethics, Medicine, And Public Health, - 2017. N 19-27, - p. 21

2. Blanke, MJ "Safe Harbor" and The European Union's Direct on Data Protection // SAFE HARBOR ALBANY La w Journal, - 2016. Volume 11, N 4:43 , - p. 110. pp. 101-134.

3. https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

4. Sotto, L. United States / L. J.Sotto , APSimpson // Data Protection & Privacy in 26 Jurisdictions Worldwide: 2014, - 2014, p. 191. - 204 p.

5. Hodges, S. Examining the Gramm-Leach-Bliley Act's opt-out method for protecting consumer data privacy rights on the Internet // Information and communications technology law. - Oxford, 2013. - Vol. 22, N 1. - p. 85. P. 60–85.

6. Margaret, PE Managing your Data Processors: Legal Requirements and practical Solutions // BNAI's World Data Protection Report, - 27 August 2007, - p. 2.

7. https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

8. Brennan, MW Complying with the CAN-SPAM Act // Lexis Practice Advisor Journal, - 2016. https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/posts/complying -with-the-can-spam-act

9. Braverman, B. Fear FACTA: Beware the Truncation Requirement of the Fair and Accurate Credit Transactions Act. 4 December 2013. https://www.dwt.com/insights/2013/12/fear-facta-beware-the-truncation-requirement-of-th

10. Title 16 Commercial Practices Parts 0 to 999 (Revised as of January 1, 2014): 16-CFR-Vol-1. - Office of The Federal Register, Enhanced by IntraWEB , LLC. IntraWEB , LLC and Claitor's Law Publishing, - 2014, P. 397-399. - 768 p.

11. https://caselaw.findlaw.com/us-supreme-court/429/589.html

12. Chlapowski , FS The Constitutional Protection of Information Privacy // Boston University Law Review, - 1991. N 71, - p. 147. pp.133-160

13. https://www.globalhealthrights.org/health-topics/occupational-health/united-states-v-westinghouse/

14. Carmen, R. Criminal Procedure: Law and Practice. - Belmont: Cengage Learning, - 2007, - P. 224-225. 640 p.

15. http://www.nytimes.com/2012/01/24/us/police-use-of-gps-is-ruled-unconstitutional.html

16. Pozgar , GD Legal Aspects of Health Care Administration. - Burlington: Jones & Bartlett Publishers, - 2016, - p. 387. 588 p.

17. https://en.wikipedia.org/wiki/Doe_v._Chao

18. Reyers , CL The US Discovery - EU Privacy Directive Conflict: Constructing a Three - Tiered Compliance Strategy // Duke Journal of Comparative & International Law, - 2009. Vol. 19. No. 2, - P. 357-387.

Date of receipt of the article in the Editorial Office
(19.12.2019)