PAM Pokrajinski arhiv Maribor

Moderna arhivistika

Časopis arhivske teorije in prakse
Journal of Archival Theory and Practice

Letnik 2 (2019), št. 1 / Year 2 (2019), No. 1

Maribor, 2019

Moderna arhivistika

Časopis arhivske teorije in prakse

Journal of Archival Theory and Practice

Letnik 2 (2019), št. 1 / Year 2 (2019), No. 1

ISSN 2591-0884 (online)
ISSN 2591-0876 (CD_ROM)

Izdaja / Published by:
Pokrajinski arhiv Maribor / Regional Archives Maribor

Glavni in odgovorni urednik / Chief and Responsible editor:
Ivan Fras, prof., Pokrajinski arhiv Maribor, Glavni trg 7, SI-2000 Maribor,
telefon/ Phone: +386 2228 5017; e-pošta/e-mail: ivan.fras@pokarh-mb.si

Glavna urednica / Editor in chief:
mag. Nina Gostenčnik

Recenziranje / Peer review process:
Prispevki so recenzirani. Za objavo je potrebna pozitivna recenzija. Proces recenziranja je anonimen. / All articles for publication in the conference proceedings are peer-reviewed. A positive review is needed for publication. The review process is anonymous.

Lektoriranje / Proof-reading:
mag. Boštjan Zajšek, mag. Nina Gostenčnik

Prevajanje:
mag. Boštjan Zajšek (slovenščina), mag. Nina Gostenčnik (slovenščina, angleščina), Lučka Mlinarič (bosanščina, hrvaščina, srbščina)

Oblikovanje in prelom / Design and typesetting:
mag. Nina Gostenčnik

http://www.pokarh-mb.si/si/p/3/49/moderna-arhivistika.html

Prejeto / Received: 4. 1. 2019

1.04 Professional article *1.04 Strokovni članek*

PROTECTION OF PERSONAL DATA IN DOCUMENTS - APPLICATION OF THE LAW ON PERSONAL DATA PROTECTION IN SERBIA AND ABROAD

Mirjana BOGOSAVLJEVIĆ, M. Sc.
Archives of Serbia, Belgrade, Serbia
bogosavljevicmirjana@yahoo.com

Abstract:

The rapid and continuous development of information technologies that encompasses almost all spheres of social life, imposes the key issue of protecting the privacy personal data, the issue of their availability, the way of their storage, processing, transmission and use.

The contemporary concept of privacy puts emphasis on information control, security and data protection in computer information systems. Protection of privacy primarily concerns the issue of protection against abuse, fraud, embezzlement and deliberate or accidental damage.

This paper covers several key issues: what are the mechanisms for protecting personal data in documents; is it feasible to achieve higher security of computer systems in terms of data protection; is it possible to limit the distribution of certain types of data (medical reports, financial institutions, schools); what is done regarding data protection in terms of establishing laws, regulations and standards.

From the point of view of archivists and archival staff in the era of digitalization of archival material when it becomes accessible and available for use, the protection of personal data in documents is certainly an issue that deserves special attention and consideration.

The paper shall provide an overview on the up to date achievements in this field within the archival services in our country and abroad.

Key words:

protection of personal data in documents, data, law, regulations, digitization

Izvleček:

Varstvo osebnih podatkov v dokumentih – implementacija Zakona o varstvu osebnih podatkov v Srbiji in svetu

Hiter razvoj informacijskih tehnologij, ki zajema skoraj vse vidike družbenega življenja, postavlja vprašanje varstva osebnih podatkov v dokumentih, dostopa do teh podatkov, njihovo hrambo, obdelavo, prenos in uporabo.

Sodobni koncept zasebnosti poudarja nadzor nad informacijami ter njihovo varnost in zaščito v računalniških informacijskih sistemih. Varstvo podatkov v dokumentih zajema zaščito pred zlorabo, prevaro, poneverbo ter namerno ali nenamerno povzročitvijo škode.

Prispevek obravnava nekaj ključnih vprašanj: kakšni so mehanizmi za zaščito podatkov v dokumentih, možnost doseganja višje stopnje varnosti računalniških sistemov v smislu varstva podatkov, možnost omejitve distribucije določenih tipov podatkov (zdravniška poročila, finance,

šolski podatki) ter kaj je bilo narejeno na področju varstva podatkov v smislu sprejemanja zakonov, podzakonskih aktov in standardov.

Z vidika arhivistov je v dobi digitalizacije, ko je arhivsko gradivo širše dostopno za uporabo, vprašanje varstva podatkov posebej pomembno in vredno diskusije.

Prispevek bo podal pregled sprejetih ukrepov znotraj arhivske službe v Srbiji in širše.

Ključne besede:

zaščita osebnih podatkov, zakonodaja, digitalizacija

1. INTRODUCTION

Everyday use of personal data has gone so far that it already surpasses even the default meaning of the term of protection of private personal data. Laws, international conventions and various types of contracts fail to protect not only the political and security interests of the country. Citizens themselves with their open exchange of private information are at risk and completely unprotected.

Similarly, it is difficult to establish a framework of rights and obligations that are protecting personal data of each individual. Experts around the world are working to establish legal frameworks, regulations, laws, principles of protecting the interests of individuals against the improper and often malicious usage of personal data, whether by institutions, private companies or even individuals.

This paper deals with the issue of the legal framework for the protection of personal data in EU and in Serbia and with particular aspects of provisions of EU regulation aims for the implementation within archives and related activities as general.

2. WHAT IS PRIVACY?

The right to privacy, even though it is protected by a number of international conventions as a basic inalienable human right, is a dynamic process in any legislature in the world and is not fully defined. An individual has a right to independently decide on what and to whom will communicate his/her personal details, life etc. The problem is that the privacy issue can be observed in different ways and is conditional on the status of an individual in society and social relations in which he/she participates.

The meaning of the word privacy has historically been interpreted in different ways. In 1890, American lawyers Samuel D. Warren and Louis Brandeis wrote an article in which they defined the privacy as "the right to be left alone", which included the protection of personal autonomy, moral and physical integrity, the right to a lifestyle choice, interaction with other people and so on. This broad definition of privacy is certainly vague in terms of legal provisions, but the very notion of an "individual right" has become very important for the common man and therefore discussions on the protection of personal data are still strong. Certainly the right to privacy is not just a "right to be left alone," it includes the control over how much and what information about themselves and others are given to the public. Data security in the sense of the "right to be left alone" is actually replaced by the belief that the individual "has nothing more to hide" a growing number of security measures actually have become a major threat to the protection of personal data.

Privacy and private life can be defined in different ways in which these two concepts in European literature generally are treated as identical, although legal privacy has a broader basis. The right to privacy is simply defined as a primordial human right to be left alone and the legal point of view can be seen from several aspects: as a human right in international legal nature, as a fundamental constitutional right and as a personal right protected by the provisions of the civil law.

How and to what extent can one encroach on the privacy of another person? There is only one answer to that question. Except in the cases defined by the law, it is unlawful to process, publish or otherwise use personal data without the written consent of that person. Protecting data against unauthorised use is at the same time the protection of the person to whom the data belong to.

Today people have less and less means to preserve their interests, rights, freedoms and especially the most intimate life. One of the prerequisites for the development of modern democratic society was exactly the creation of conditions for self-determination of citizens who are familiar with the laws in the direction of realizing the right to privacy.

On the other side, the state that should ensure the protection of citizens' personal data and thus prevent their misuse.

Before we go into the analysis of legally defined rights to privacy and data protection, it is important to point out another important fact and that is the need to distinguish between the concept of information and data. In everyday language, we often hear how someone only provides information about a person but does not ask what it actually means. The difference between data and information is important because these terms are often identified. Data is basically a message that may or may not be used. If the data may be unambiguously and accurately used to represent an undeniable fact than it represents the information.

We have to distinguish between these two terms because often some data about a person need not have a special meaning until they form information - that is they get a certain meaning. The more specific information, the worthier it gets. Collection of data, such as for instance information on a person: name, address, etc. becomes information and data on marital status or health condition of that person double the importance of the data, which still keeps growing correlated with different information for example, income, habits and so on. That threatens the privacy of a person even without having her/him to know anything about it. In this regard, the concept of privacy of information often is identified with the concept of confidentiality. However, unlike the notion of privacy of information that includes the individual's right to certain information not inform the third parties, the concept of confidentiality of information includes the right of individuals to prevent further disclosure of certain sensitive information that was originally communicated in a confidential relationship, for example doctor-patient (Rothstein, M. A., 1998, p.198).

3. LEGALLY DEFINED RIGHTS TO PRIVACY AND DATA PROTECTION IN THE WORLD

The right to the protection of personal data forms a part of the right to privacy. Already in the seventies some countries in Europe enacted data protection laws. The first data protection law in Europe had been passed in Sweden in 1971; followed by Germany (1977), France (1978), Austria, Denmark, Norway, Finland, Luxemburg, etc. Alan F. Westin (1968) defines privacy as the right of an individual to determine what information about themselves he/she wants to reveal to others. Comprehensive and

detailed insight into the theory of privacy, different definitions of policy from the perspective of lawyers, philosophers and sociologists are given in the Daniel J. Solove's paper (2007) *I've Got Nothing to Hide and Other Misunderstandings of Privacy.*

The basic framework for the protection of privacy and personal data in the European Union was adopted in 1995 in Strasbourg *(The 1995 Data Protection Directive of the European Union - Directive 95/46 / EC) - The Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (ratified in 2005).* Member States of the Council of Europe, signatory to this Convention, respect for the rule of law, and human rights and fundamental freedoms, considered it desirable to extend the protection of fundamental rights and freedoms of individuals in the direction of respect for privacy with regard to the increasing use of personal data which are subject to automatic processing in order to reconcile the fundamental values of respect for privacy and the free exchange of information among nations.

Article 2 of the Convention relating to the definition of personal data says that personal data is any information relating to an identified natural person or a person who can be identified ("interested person").

In Chapter II of *The Basic Principles for Data Protection,* it is stated that each State which is signatory of the Convention is obliged to take the necessary measures within their own legislation in order to assure real implementation of the basic principles relating to data protection. Further on the Convention establishes the rules that personal data must be legally obtained and processed to be used in well-established legitimate purpose and that every person should be informed of the existence of an automated database, with personal data, its purpose, and that person may file a complaint in case of any misuse.

Article 10 Sanctions remedies reads: *"Each Party undertakes to establish appropriate sanctions and remedies against violations of the provisions of internal law which apply the basic principles of data protection indicated in this section."*

This is where the problem arises. Many countries have not actually defined neither sanctions nor mechanisms for checking the abuses and the possibility of punishing them. This is why many countries have subsequently ratified the two general rules:

- *The Additional Protocol to the Convention regarding supervisory authorities and transborder data flows, 2001 (Serbia ratified in 2008)*
- *Directive 95 / 46 EP and Council of EU minimum standards for the protection of rights and freedoms with regard to the processing of personal data. In the application only in EU member states. EK SE and preparing significant changes to the Convention 108 and Directive 95/46*

The Directive 95/46 EP over the time became totally inapplicable and obsolete. After the social conditions changed, the European Union launched the legislative procedure for the adoption of the new regulation in 2012.

In April 2016, the European Parliament and the EU Council passed the *General Data Protection Regulation - GDPR.*

This regulation applies to respect the rights and freedoms and in particular the protection of personal data. The importance of this regulation is reflected in the fact that it allows individuals to always find out what is the purpose of inquiring their personal data, and have their data erased from databases if they wish to do so. The owner of information has a right to evaluate how much harm would be done by the disclosure of information about his personality. In brief, this Regulation guarantees the control over personal data.

States, which are signatories to this Accord, are required to pass new data protection laws, which must be in line with the Regulation within a certain period of time. The aim of this regulation is to restore confidence of the public in institutions which collect and store data about them. At the same time, people shall be better informed on the meaning of the consent to the use of their personal data and the consequences of such decisions.

Article 12 of GDPR stipulates the lawful and fair processing of personal data, transparent in terms of how personal information is collected, used, disclosed to or otherwise processed, and the extent to which this personal data is processed or will be processed. The principle of transparency requires that all information and communication in relation to the processing of personal data is easily accessible and understandable, and uses clear and simple language.

Article 15 of GDPR defines the right of interviewee to have access to personal data collected at regular intervals to be able at any time to check if the data processing is done in compliance with the law. An individual to whom the information relates to has the right to seek and obtain confirmation from the data processor, whether his/her data are actually processed and if it is confirmed, has the right of access to such data.

The person to whom the data refer, is on the basis of the Article 16 and 17 of GDPR entitled to update their own personal data or to have them deleted (right to be forgotten), if the retention of such data violates the regulation or EU law or the law of the Member States applicable to data processing party.

The issues of data security regulation are given great importance. In Article 25, the data processor is required to apply certain technical and organizational measures for the effective implementation of the principles of data protection. Articles 32, 33 and 34 precisely define appropriate technical and organizational measures aimed at maximizing the security of personal data. The measures primarily relate to regular testing, evaluation and assessment of the effectiveness of technical and organizational measures to achieve the safe processing of personal data

A special group of articles from 51 to 59 define the status, authority, duties and powers of the independent supervisory authority, which is in each country responsible for the implementation thereof, in order to protect fundamental rights and freedoms of natural persons in relation to the processing of personal data.

Finally, it is important to emphasize that this Regulation applies to anyone who processes data relating to citizens of countries of the European Union regardless of whether data processing is performed in the EU and whether a data processor is based in a Member State of the EU. In order to implement the GDPR rules for data protection, the EU Commission is committed to develope mechanisms for international cooperation to ensure international mutual legal assistance, engage relevant stakeholders and promote the exchange and documentation of the law on protection of personal data between the EU countries and those which are not.

4. PROTECTION OF PRIVACY AND PERSONAL DATA IN SERBIA

The concept of privacy in our country was established in 2008 when the *Law on Protection of Personal Data (2008)* was passed*.* Following the introduction of this Law, the Commissioner for Information of Public Importance and Personal Data Protection was appointed, which marked the beginning of a better regulation of the protection of personal data and awareness of the *management of the data of each person.*

Article 1 of the 2008 Law states: *"Protecting personal data is provided for each natural person, regardless of nationality and place of residence, race, age, gender, language, religion, political or other belief, ethnicity, social origin and status, property, birth, education, social status or other personal characteristics.*

The tasks of protection of personal data are performed by the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter Commissioner), as an autonomous state body, independent in exercising its jurisdiction."

Article 5 defines the information that the law applies to:

1. *"data that are available to anyone and published in the media, and publications or available in archives, museums and other similar organizations;*
2. *data to be processed for family or other personal use and not available to third parties;*
3. *data on members of political parties, associations, trade unions and other organizations that are processed by these organizations, provided that the member gives a written declaration that certain provisions of this Act shall not apply to the processing of data about it for a certain time, but not longer than the duration of his/her membership;*
4. *information that a person, capable of taking care of his/her own interests, had released himself/herself."*

Due to the rapid development of information technology, there is a need to further protect the rights of citizens because of the frequent misuse of personal data, such as identification number, bank account number, biometric data, e-mail address and so on. Bearing in mind that the text of the applicable law has not been changed for nearly nine years of implementation and the fact that Serbia had an obligation to the process of joining the EU to submit a new bill that has been done to ensure compliance by *Regulation 2016/679 on the protection of individuals with regard to the processing personal data and the free movement of such data.*

The draft law introduces novelties especially in the area of personal data processing: it is possible to file an objection to the processing and use of personal data, then file a complaint to the Commissioner for Information of Public Importance and Personal Data Protection who can provide appropriate assistance. The bill also explicitly provides for the right to receive compensation from the person who is abusing personal data. This draft law is for the first time clearly stipulating the special provisions relating only to the competent authorities which ensure the legality of their actions.

The Ministry of Justice's explication of the Law proposal indicated that the new legislation significantly improves the protection of personal data. Provisions of that law are harmonized with the new EU regulations, so all the personal data of citizens of Serbia should be protected in the same way as of the citizens of the EU member states.

Given all of the above, the Regulation brings novelties in the field of the system for control and supervision of the processing of personal data, tightening penalties for both EU Member States and those that are not (or are indirectly involved in the system of sanctions), indicates the seriousness of the state administration to have the Regulation fully implemented all the way, primarily in the field of human rights violations as well as to privacy and respect for personal data. The GDPR also obliges the EU Commission as well as its member states and non-member states to develop mechanisms of

international cooperation, provide international mutual assistance, engage relevant stakeholders, and promote the exchange of documents and data protection laws.

5. ARCHIVES AND GDPR

The European Archives Group issued guidelines on the implementation of the Regulation on the protection of personal data (General Data Protection Regulation – GDPR) in the document "*Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector*", published as a draft at their web site in October 2018.

These guidelines provide only basic information and guidance to archivists regarding the practical application of the GDPR in the archival sector. They are applicable to both public and private establishments and institutions that hold records that have been selected for permanent preservation, including in the first place the national, state, regional and municipal archives but also museums, libraries, foundations and similar public and private entities that preserve archives. No room was left for any exceptions or changes for archival purposes in the public interest.

The fact that the GDPR protects only personal data of living persons has been addressed by the Guidelines with special care because it is common case in the archival practice that an archivist may not know if the subject is alive or deceased.

The Guidelines pay attention to the principle of "archiving purposes in the public interest". Since the GDPR allows for a number of exceptions in favour of "archiving purposes in the public interest" in the following way: "*Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest.*"

The EAG Guidelines explain that the archives have to follow their legally defined status. For example, the law might dictate that a specific agency or department has a mission of acquiring, preserving and making available to researchers the personal papers of writers, scientists or political activists that were victims of political repression.

Particular attention in the Guidelines is paid to the issue of the data subject's rights: granting individuals control over their personal data, provision of information in case personal data have not been obtained from the data subject, the right of access by the data subject, right to data erasure etc. Those matters are found to be extremely sensitive and hard to implement within the regular scope of work, especially at National and State archives due to the already established every day practice.

The EAG Guidelines also elaborate the issues of processing categories of personal data that require special safeguarding (criminal records), data security and measures for promoting transparency and compliance. All of which require a fairly complex approach in everyday practice and potential considerable technical and organizational changes as well.

In case of Serbia, protection of personal data within public archival and documentary material is not precisely defined. For example, Article 5 of the Law on Protection of Personal Data from 2008 stipulates that personal information also includes information that is "*available to anyone and published in public media and publications or accessible archives, museums and other similar organizations."*

In late November 2018, the Parliament of the Republic of Serbia passed a *Law on Personal Data Protection,* which aims to comply with GDPR (2016).

What was introduced by the new law on the protection of personal data, which would be important for the archives?

Firstly, Article 98 of the GDPR (2016) stipulates that keeping the Central Register of data collections shall be brought to an end, and that the central register, as well as the data contained in this register shall be treated in compliance with the regulations governing the handling of archive material.

It should be noted that although Central Register of data collections shall not be kept any longer, the provisions of the new law are not repealing the provisions of the old law concerning the obligations of data controllers regarding the establishment and registration of already established collections of personal information.

Equally arguable was the Article 40 of the Law from 2008 which stipulates that the rights of citizens related to access, delete, and modify data may be restricted by law only in order to protect national security, defence, and public security and so on. In the new law, this provision is removed. Article 40 from 2008 remained in but it is changed - it no longer holds a formulation which shows that citizens' rights (right to amendment, deletion or restriction of data processing) may be restricted by law, but only to be limited. Thus stipulated the article leaves room for state bodies and agencies to handle personal data of citizens without legal restrictions. For example, the Ministry of Interior and security services have a free hand to the free assessment of the decision not to respond to requests from citizens who want to know if they are tapped, what data about them is collected and for what purposes.

6. CONCLUSION

Generally, when it comes to the protection of personal data, Serbia is still at the very beginning of the introduction of European standards in the legal system and the everyday life. It is very important to move the process forward and accelerate.

The direct result of an inadequate and irresponsible attitude towards the state normative level of protection of personal data is the fact that no law yet regulates numerous very important areas for the protection of personal data, such as video surveillance and biometrics, which means that the citizens are exposed to numerous potential and real risks of violations of their rights.

A rising number of actual incidents and violations of the right to protection of personal data, imperatively demands that the relationship between the state and society as a whole towards the protection of personal data and privacy in general, changes completely, from the root. That is also a mandatory request of the integration processes of our country with the EU and, more importantly, the need to promote and protect human rights guaranteed by the Constitution of Serbia.

Very good sign is shown by the Serbian legislators by the recent introduction of the *Law on Personal Data Protection.* Now the archives and archivists in Serbia have a starting point for their journey into safe keeping of personal data that they had been entrusted with.

POVZETEK

VARSTVO OSEBNIH PODATKOV V DOKUMENTIH – IMPLEMENTACIJA ZAKONA O VARSTVU OSEBNIH PODATKOV V SRBIJI IN SVETU

Mag. Mirjana BOGOSAVLJEVIĆ
Arhiv Srbije, Beograd, Srbija
bogosavljevicmirjana@yahoo.com

Prispevek predstavlja pravni okvir, ki definira pravico do zasebnosti in hkrati opozarja na to, da je priprava preciznega in uporabnega pravnega okvira zelo težka.

Srbsko Ministrstvo za pravosodje je kot predlagatelj zakona o varovanju osebnih podatkov v svoji razlagi nakazalo, da sicer nova zakonodaja bistveno izboljšuje varovanje osebnih podatkov, vendar pa mnoge težave še niso razrešene. Potrebno je poudariti, da je nova zakonodaja v skladu z evropsko ureditvijo, tako da so osebni podatki državljanov Srbije zavarovani enako kot na evropski ravni. Varovanje osebnih podatkov v arhivskem in dokumentarnem gradivu v Srbiji pa še ni definirano.

Evropska arhivska skupina je podala smernice za implementacijo Splošne uredbe za varstvo podatkov GDPR. Te smernice podajajo le osnovne informacije v zvezi s praktično implementacijo GDPR na arhivskem področju. Uporabljajo se tako za javne kot zasebne ustanove ter ustanove, kjer je gradivo odbrano za trajno hrambo.

Čeprav pravico do zasebnosti ščitijo mnoge mednarodne konvencije kot eno izmed osnovnih neodtujljivih človekovih pravic, gre za dinamičen koncept, ki v nobeni državi še ni bil popolnoma definiran. Prav tako je odprto tudi vprašanje zaščite javnega arhivskega gradiva, ki zahteva resen pristop in vključevanje arhivskih strokovnjakov.

Sources and literature:

***Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector*. (2018).** European Archives Group. Retrieved 18. 12. 2018 from: https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf.

Law on Protection of Personal Data (2008). Official Gazette of RS, no. 97/08 from 27. 10. 2008, 104/09 – law 68/2012 - decision of CC and 107/2012.

Law on Ratification of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (1995). Official Gazette RS - International Treaties, no. 98/2008 and 12/2010.

Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016). Official Journal of the European Union. Retrieved 1. 11. 2018 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

Rizza, C. et al. (2011). Interrogating Privacy in the digital society: media narratives after 2 cases. *International Review of Information Ethics*, Vol. 16 (12/2011). Retrieved 11. 11. 2018 from: https://www.researchgate.net/publication/264310287_Interrogating_privacy_in_the_digital_society_media_narratives_after_2_cases.

Rothstein, M. A. (1998). Genetic privacy and confidentiality: why they are so hard to protect. *The Journal of Law, Medicine and Ethics*, 26 (3), 198-204. Retrieved 8. 11. 2018 from: https://aquila.usm.edu/cgi/viewcontent.cgi?article=1000& context=ojhe.

Solove, D. J. (2007). *I've Got Nothing to Hide and Other Misunderstandings of Privacy*. George Washington University, GW Law Faculty Publications & Other Works. Retrieved 22. 12. 2018. from: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications.

Warren, S. D., Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, vol. 4, no. 5, 193-220. Harvard Law Review Association. Retrieved 1. 11. 2018 from: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.