BÁNKI KÖZLEMÉNYEK
2. ÉVFOLYAM 1. SZÁM

A right to privacy as a fundamental human right in correlation with data protection

A magánélethez való jog mint alapvető emberi jog az adatvédelemhez való viszonyulás tekintetében

Ivona Ninkov
'Rights 4 All', Novi Sad, Serbia
ivonakakas@yahoo.com

***Abstract* — This paper presents a general overview of the rights to privacy as a fundamental human right in the correlation with data protection. The paper aims to illustrate how rights of privacy are developed after the Second World War and the data protection regulation after the case of Snowdan. It clarifies the difference between the right to privacy and data protection in the lights of the General Data Protection Regulation, which entered into force on May 25th, 2018. The paper outlines data protection terminology, people's rights and how these rights are enforced through international legal treaties. During the research the author used a comparative method to find the similarity and differencies between the privacy rights and personal data protection focusing on the rich jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). In the paper it is concluded that the right of privacy and the right of personal data protection are closely linked, but they should not be considered to be identical.**

***Keywords*:** right to privacy, human rights, data protection, security, legal treaties.

***Összefoglalás* — Ez a cikk általános képet nyújt a magánélethez füződő jogokról, mint alapvető emberi jogról, az adatvédelemmel összefüggésben. Tanulmány célja annak bemutatása hogy a második világháború után hogyan alakult ki a magánélethez való jog. Tisztáza a magánélet és az adatvédelmi közötti különbséget az Általános adatvédelmi szabályozás fényében amely 2o18. május 25-én lépett hatályba. A cikk felvázolja az adatvédelmi terminológiát, az ember jogait és ezek a jogok érvényesítése nemzetközi jogi egyezmények alapján. A szerző összehasonlító módszert alkalmazott a magánélethez füződő és a személyes adatok védelme jogokra különös hangsúlyt fektetve az Emberi Jogok Eurrópai Bíróságának és az Európai Unió Bíróságának gazdag ítélkezési gyakorlatára. A jogi kérdéseket vizsgáló kutatás során arra a következésre jutott, hogy a személyes adatok és ezek védelme szorosan összefüggnek az Emberi Jogok Európai Bírósága és az Európai Unió Bírósága tapasztalata szerint, de nem feltétlenül azonosnak kell leniük.**

***Kulcsszavak*:** a magánélethez való jog, emberi jogok, adat védelem, biztonszág, jogi szerződések.

1 INTRODUCTION

The rapid technological development of the society in the past decades has made a significant impact on our lives and created a requirement for new legal solutions. In recent years during the Third Industrial Revolutions new types of communication between individuals is developed. Let us mention the most often used ones:

- the Internet
- e-commerce,
- social networks, etc.

These technologies require and apply many personal data (name, surname, postal and e-mail address, photo, IP address, location data, date and place of birth and so on). The main question is, whether the basic human right for privacy is disturbed due to publishing of personal data? The problem is how safely to store these data and protect them of the abuse. In addition, it is the question how the public notation of the data affects the personal safety. For sure, the legal advice is necessary. Namely, development has given rise to a plethora of legal problems, particularly in data protection law [1].

In this paper the regulation of protection of personal data in correlation with the right of privacy is investigated. An overview on legal acts dealing with problem of personal data protection is given.The right of privacy and the right of personal data protection are compared. Similarity and differences between these legal acts is set up. Based on these conclusions, a suggestion for application of the personal data protection regulation is given.

The paper has five sections. In the Section 2 the history of personal data collection procedures and the introduction of the basics of human rights in legal practice is presented. Section 3 explains the legal aspects of the personal data protection and the General Data Protection Regulation (GDPR) proclaimed by the European Union in 2018. In Section 4, the right for protection of personal data in correlation bith basic human rights is discussed. The paper ends with conclusion.

2 HISTORIC OVERVIEW

During history, we are witnesses of the destructive power that information could have in the hands of the government. Unfortunately, information gathered for one purpose could be reused for a wide range of sinister purposes.

The great example for this is the method of collection the information about Jewish people during the Second World War. Have we ever asked ourselves how did Nazi authorities know exactly who was Jewish? How did they identify the most common Jewish residential areas?

After the Second World War this extreme example of abused identification made a ground for introducing of legal acts concerning one of the most important rights: the international human rights. As the special right is the right for privacy.

Nowadays, almost every country in the world recognizes the right to privacy in various international human rights legal instruments. It is enriched in the article 12 of the Universal Declaration of the Human Rights [2], article 8 of the European Convention on Human Rights [3] , article 7 of the European Charter of Fundamental Rights [4], article 17 of the International Covenant on Civil and Political Rights [5], in Article 10 of the African Charter on the Rights and Welfare of the Child [6], article 11 of the American Convention on Human Rights [7], articles 7 and 8 of the Charter of the Fundamental Rights of the European Union [8], and article 21 of the Arab Charter on Human Rights [9]. Not only that the right to privacy is one of the fundamental human rights it is also a tremendously important social value.

However, an event in 2013 shows the defect of the existing documents in human rights. In June 2013, a National Security Agency contractor, Edward Snowden leaked documents on America's global surveillance which showed that the National Security Agency had backdoor deals with Silicon Valley companies, allowing them to use consumer data as the basis of their counterintelligence operations. At that time the existing legal documents were not enoughly specified to protect the personal data. Already that year a negotiation on legal regulation of personal data protection began.

In 2016 the European Union (EU) adopted a new legal framework - the General Data Protection Regulation (GDPR). It entered into force on 25th May 2018 and superseded the EU's 1995 Data Protection Directive and all member state law based on it, including the UK's DPA 1998 (Data Protection Act 1998). GDPR is the most comprehensive piece of data protection legislation in the world.

3 Explanation of GDPR

GDPR is a regulation (not a directive), which is under the EU law, directly applicable and there is no need for national implementation. GRPR provides consistent data protection rules throughout EU. It is truly important because it establishes an environment of legal certainty.

The GDPR extends the data rights of individuals (data subjects), and places a range of new obligations on organizations that process EU residents' personal data. GDPR is given in 11 Chapters divided into Sections and 99 Articles:

Chapter 1 - General provisions contains 4 articles: Subject – matter and objectives, Material scope, Territorial scope and Definitions.

The Chapter 2 – Principles has 7 articles: Principles relating to processing of personal data, Lawfulness of processing, Conditions for consent, Conditions applicable to child's consent in relation to information society services, Processing of special categories of personal data, Procession of personal data relating to criminal convictions and offences and Processing which does not require identification.

Chapter 3 – Rights of the data subject is divided into 6 sections: Section 1 – Transparency and modalities with the article Transparent information, communication and modalities for the exercise of the rights of the data subject, Section 2 – Information and access to personal data with three articles (Information to be provided where personal data are collected from the data subject, Information to be provided where personal data have not been obtained from the data subject, Right of access by the data subject), Section 3 – Rectification and erasure with 5 articles (Right to rectification, Right to erasure ('right to be forgotten'), Right to restriction of processing, Notification obligation regarding rectification or erasure of personal data or restriction of processing, Right to data portability), Section 4 - Right to object and automated individual decision-making with two articles (Right to object, Automated individual decision making, including profiling) and Section 5 – Restrictions.

Chapter 4 – Controller and processor has 4 Sections: Section 1 - General obligations with 8 articles (Responsibility of the controller, Data protection by design and by default, Joint controllers, Representatives of controllers or processors not established in the Union, Processor, Processing under the authority of the controller or processor, Records of processing activities, Cooperation with the supervisory authority), Section 2 - Security of personal data with three articles (Security of processing, Notification of a personal data breach to the supervisory authority, Communication of a personal data breach to the data subject), Section 3 - Data protection impact assessment and prior consultation with two articles (Data protection impact assessment, Prior consultation), Section 4 - Data protection officer with three articles (Designation of the data protection officer, Position of the data protection officer, Tasks of the data protection officer), Section 5 - Codes of conduct and certification with four articles (Codes of conduct, Monitoring of approved codes of conduct, Certification, Certification bodies).

Chapter 5 - Transfers of personal data to third countries or international organizations has 7 Articles (General principle for transfers, Transfers on the basis of an adequacy decision, Transfers subject to appropriate safeguards, Binding corporate rules, Transfers or disclosures not authorized by Union law, Derogations for specific situation, International cooperation for the protection of personal data).

Chapter 6 - Independent supervisory authorities has two sections. Section 1 titled Independent status has two sections. The first tesion has four Articles (Supervisory authority, Independence, General conditions for the members of the supervisory authority, Rules on the establishment of the supervisory authority), while the Section 2 - Competence, tasks and powers has three Articles (Competence of the lead supervisory authority, Tasks, Power, Activity reports).

Chapter 7 - Cooperation and consistency includes 3 sections: Section 1 – Cooperation and 3 Articles (Cooperation between the lead supervisory authority and the other supervisory authorities concerned, Mutual assistance, Joint operations of supervisory authorities), Section 2 – Consistency with 5 Articles (Consistency

mechanism, Opinion of the Board, Dispute resolution by the Board, Urgency procedure, Exchange of information), Section 3 - European data protection board with 9 Articles (European Data Protection Board, Independence, Tasks of the Board, Reports, Procedure, Chair, Tasks of the Chair, Secretariat, Confidentiality),

Chapter 8 - Remedies, liability and penalties with 8 Articles (Right to lodge a complaint with a supervisory authority, Right to an effective judicial remedy against a supervisory authority, Right to an effective judicial remedy against a controller or processor, Representation of data subjects, Suspension of proceedings, Right to compensation and liability, General conditions for imposing administrative fines, Penalties).

Chapter 9 - Provisions relating to specific processing situations with 7 Articles (Processing and freedom of expression and information, Processing and public access to official documents, Processing of the national identification number, Processing in the context of employment, Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, Obligations of secrecy, Existing data protection rules of churches and religious associations).

Chapter 10 - Delegated acts and implementing acts with two Articles (Exercise of the delegation, Committee procedure) and Chapter 11 - Final provisions with 6 Articles (Repeal of Directive 95/46/EC, Relationship with Directive 2002/58/EC, Relationship with previously concluded Agreements, Commission reports, Review of other Union legal acts on data protection, Entry into force and application).

Some definitions and additional explanation to the Regulation is necessary.

3.1 Meaning of the Personal Data

First of all it is important to clarify the meaning of the term Personal Data - it means "any information relating to an identified or identifiable natural person ('data subject'). Namely, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as [10]:

- a name,
- an identification number,
- an online identifier or0
- personal data includes IP address, device ID and customer reference numbers
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. "

Personal data is any information relating to an identified or identifiable natural person ('data subject').

Let us mention some of these special categories of personal data are:

- Race
- Religion
- Political opinions
- Trade union membership
- Sexual orientation
- Health information
- Biometric data
- Genetic data

The last two data are recently introduced as specific for person identification.

3.2 Principles of data processing according to GDPR

Six general principles are prescribed for data processing in the GDPR:

- Processing has to be lawfully, fairly and transparently.
- Collection of personal data is allowed only for specific legitimate purposes.
- Apply adequately, relevantly and limited to what is necessary.
- Dates have to be kept up accurately to date, where necessary.
- Dates have to be stored only as long as is necessary.
- Appropriate security conditions have to be satisfied during the data processing.

These principles correspond to data protection ones.

3.3 Processing has to be legal

The processing with data has to be in accordance with the law. It is required:

- Subject to give his consent for data processing.
- Contractual obligations has to be met.
- Legal obligations have to be complied.
- Vital interests of the data subject's has to be protected.
- Data to be applied for tasks in the public interest.
- Data to be used only for the legitimate interests of the organization.

3.4 Complience with the GDPR

The governance according to GDPR can be proved by various statements. Let us mention some of them:

- Establishing a governance structure with roles and responsibilities.
- Keeping a detailed record of all data processing operations.
- Documenting data protection policies and procedures.
- Carrying out DPIAs (data protection impact assessments) for high-risk processing operations.
- Implementing appropriate measures to secure personal data.
- Conducting staff awareness training.

If it is necessary the protection officer has to be appointed.

3.5 Privacy rights of individuals

In GDPR privacy rights of individuals are defined in 8 itoms:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision-making and profiling.

3.6 Subject's valid consent

The GDPR introduces stricter rules for obtaining consent for data processing:

- Consent must be freely given, specific, informed and unambiguous.
- A request for consent must be intelligible and in clear, plain language.
- Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
- Consent can be withdrawn at any time.
- Consent for online services from a child under 13 is only valid with parental authorisation.
- Organizations must be able to evidence consent.

Thus, GDPR brings us several improvements concerning data protection. For example:

- Privacy policies have to be written in a clear, straightforward language instead of using complicated terms,
- The user needs to give an affirmative consent before his/her data can be used,
- It cannot be assumed that the user's silence means consent to data processing.

According to GDPR different forms of expression of an assent could be given. The statement can be a written or an oral one.

Also, now businesses can collect and process data only for a well-defined purpose and not for different purposes than for the reason initially announced without informing the user about it.

3.7 Notices of transparency and privacy

GDPR prescribes how personal data is going to be processed, by whom and why. Organizations must be clear and transparent about the following:

- When personal data is collected directly from data subjects, data controllers must provide a privacy notice at the time of collection.
- When personal data is not obtained direct from data subjects, data controllers must provide a privacy notice without undue delay, and within a month. This must be done the first time they communicate with the data subject.
- For all processing activities, data controllers must decide how the data subjects will be informed and design privacy notices accordingly. Notices can be issued in stages.
- Privacy notices must be provided to data subjects in a concise, transparent and easily accessible form, using clear and plain language.

3.8 Data protection realization procedure and prediction

Implementation of the data processing principles is effectiv with tendency of increase if suitable technical and organization measures are incorporated by data controllers and processors. Thus, it is required:

- Appropriate safeguards to be integrated into the processing.
- Data protection must be considered at the design stage of any new process, system or technology.

3.9 GDPR in Buisness

Application of GDPR in buisness is strictly defined.

- Businesses can collect and process data only for a well-defined purpose and not for different purposes.
- Reason for data collection has to be initially announced
- Data cannot be used without informing the user about it.

It gives much more restriction for data processing.

3.10 Where is the GDPR Applied?

GDPR is applied in all countries of EU. However, the data protections apply to all corporate entities that process the personal data of EU citizens, even if the processing of relevant data does not take place within the EU. Namely, the new regulation also contains restrictions on transferring personal data outside of the EU.

The new regulation also contains restrictions on transferring personal data outside of the EU. All the rights in the GDPR together are at the heart of the regulation's purpose—to give citizens back control over their personal data. Further more Under the GDPR, consent has to be unambiguous [11]. Thanks to GDPR, now more than 100 countries around the world have data protections law in place.

4 BENEFITS OF GDPR IN THE SENCE OF HUMAN RIGHTS

There is a greater need than ever before to strengthen the realization of the right to data protection as a fundamental human right owed to all individuals.

Analyzing the GDPR two question are generated: 1) What are the benefits of the regulation, and 2) How right of privacy acorrelate to the data protection declaration in the sense of the General Data Protection Regulation (GDPR).

It is obtained that the privacy is a value that the right to data protection seeks to protect.

There is a greater need than ever before to strengthen the realization of the right to data protection as a fundamental human right owed to all individuals. Examples of abused identification made a ground for adoption of international human rights treaties. Nowadays, the right to privacy is represented as fundamental human right, today.

Even though, GDPR is directly applicable, the Member States should update their existing national data protection laws. The DPA 2018 (Data Protection Act 2018) supplements the GDPR by filling in the sections of the Regulation that were left to individual member states to interpret and implement. These are:

- right to be forgotten- grants data subjects a possibility to have their personal data deleted if they don't want them processed anymore and when there is no legitimate reason for a data controller to keep it.
- easier access to your data
- the right to transfer of personal data from one service provider to another- The right to data portability can be exercised when the legal basis for lawful processing is either- consent, explicit consent or actual necessity
- clear and affirmative consent when it is required,
- information about data breach without delay – within 72 hours
- transparency about how your data is used with easy-to-understand information
- administrative and juridistical remedies in the case of violation
- Data protection originates from the right of privacy.
- Data protection and the right of privacy have the instrumental role in promoting fundamental values.

Even though the rights to privacy and data protection are commonly recognized all over the world, they represent two separate rights. They are both crucial components for a democratically oriented society. The data protection originates from the right to privacy and together they have the instrumental role in promoting fundamental values. It is very important to make it clear that the protection of personal data is of fundamental importance of the enjoyment of the right to privacy so, the right to respect for private life and the right to personal data protection, although closely related, are distinct rights. This distinction raises the question of the correlation and differences between these two rights.

Both of them protect the similar value – the dignity of human beings. Also, both of them represent the prerequisites for the exercise of other fundamental freedoms [12]. It is clear that privacy, itself a fundamental right, is a value that the right to data protection seeks to protect [13].

Data protection in the EU is much older and wider than the General Data Protection Regulation (GDPR) and it has already invited the highest Courts in Europe to weigh in on the protection of this right, so the term "any information" reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject" [14].

5. CONCLUSION

The folowing is concluded:

1.The GDPR is not a total win for privacy advocates as it still have many loopholes. But without the glaring spotlight of the Snowden revelations, it would be far weaker.

2. As the right to privacy represents the fundamental human right, the personal data protection is the part of the human right legality. Protection of personal data is of fundamental importance of the enjoyment of the right to privacy.

3. At the moment GDPR is the most comprehensive piece of data protection legislation in the world.

4. Data protection and the right of privacy protect the similar value – the dignity of human beings.

5.Data protection and the right of privacy represent the prerequisites for the exercise of other fundamental freedoms.

6.Privacy and Protection of personal data are closely linked in the jurisprudence of

- European Court of Human Rights and
- Court of Justice of the European Union,

but they should not be considered to be identical.

7.Even though, GDPR is directly applicable, the Member States should update their existing national data protection laws.

ACKNOLWLEDGESMENT

I have to thank to the members of the ngo 'Rights 4 All' for supporting me in this investigation.

REFERENCES

[1] Dasko, N. (2018). General Data Protection Regulation (GDPR) – Revolution Coming to European Data Protection Laws in 2018. What's New for Ordinary Citizens?

[2] UN General Assembly, (1948). *Universal Declaration of Human Rights*, 10 December 1948, 217 A, article 12.

[3] Council of Europe, (1950). *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, article 8.

[4] European Union, (2012). *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, article 7.

[5] UN General Assembly, (1966). *International Covenant on Civil and Political Rights*, 16 December 1966, article 17.

[6] Organization of African Unity (OAU), (1990). *African Charter on the Rights and Welfare of the Child*, 11 July 1990, CAB/LEG/24.9/49 (1990), article 10.

[7] Organization of American States (OAS), (1969). *American Convention on Human Rights, "Pact of San Jose", Costa Rica*, 22 November 1969, article 11.

[8] European Union, (2012). *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, article 7 and 8.

[9] League of Arab States, (1994). *Arab Charter on Human Rights*, 15 September 1994, article 21.

[10] – (2016). 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 the free movement of such data.

[11] – (2016). Repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, L119, 1-88, (4 May 2016), article 7.

[12] – (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

[13] McDermott, Y. (2017). *Conceptualizing the right to data protection in an era of Big Data*. Big Data & Society.

[14] – (2017). Protection of individuals with regard to the processing of personal data,Directive 95/46/EC,Article 2(a), Concept of 'personal data', Written answers submitted by a candidate in a professional examination — Examiner's comments with respect to those answers, Article 12(a) and (b), Extent of the data subject's rights to access and rectification, Case C-434/16, CJEU, Nowak.