ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

***Weronika Wojturska***
*Faulty of Law and Administration, University of Warsaw*
*wwojturska@op.pl*

# e-PRIVACY IN EU LEGISLATION

## Introduction

In the light of the advanced technological solutions of our civilization privacy is becoming a commonly desired good; the necessity to protect it has a legal dimension which is reflected in regulations both on national and global levels. The regulations should effectively guarantee every individual the right to control the sphere that does not concern the others and where the freedom from curiosity from outside is a *conditio sine qua non* for a free development of individuals[1]. Having in mind the challenges that result from the extended IT infrastructure and the developing market of new technologies, the author makes an attempt to assess the legal rights to privacy in electronic communication with regard to the existing EU regulations and the judgements of the European Tribunal of Justice. Thus, the article will include the analysis of the functioning of the right to be forgotten as well as the selected issues regarding the implementation of the 2016/679 regulation[2]. Moreover, the results of the investigation on the potential threats that are caused by the increasing amount of data about Web users will make it possible to find the answer to the question to what extent the famous Orwell'e slogan *Big Brother is watching you*[3] is coming true.

## 1. Privacy of Web users in the aspect of the international guarantees of basic rights protection

Since the end of World War II the protection of fundamental human rights and liberties has been the key area of the dynamically developing international law[4]. Together with the increasing trend to value the sense of individuality, distinctiveness and uniqueness, the

[1] M. Safjana, *Prawo do ochrony życia prywatnego* [in:] *Podstawowe prawa jednostki i ich sądowa ochrona*, edited by L. Wiśniewski, Warszawa 1997, pp. 127-128.
[2] 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) – later referred to as GDPR
[3] G. Orwell: *Rok 1984*, Warszawa 2003, pp. 7-8.
[4] M. Wujczyk, *Prawo pracownika do ochrony prywatności*, Warszawa 2012, p. 36.

necessity was recognized to ensure the right to privacy as an element of civil rights. The right to privacy was given the same status as other fundamental rights such as the right to dignity, freedom of conscience, religion and speech. The right to privacy is protected both by global and regional regulations[5]. For the purposes of the article, the author will take into consideration the element of privacy that is referred to as information autonomy, i.e. the freedom of individuals to dispose of and decide about the disclosure range of the data about them.

As regards the issues of human right protection in the Internet, one should particularly take into consideration the institutionalized operations of the United Nations Organization. The turning point was the foundation of a new supporting body of the UN General Assembly– the Human Rights Council – on the basis of resolution 60/251 of 15 March 2006[6]. The Resolution of 5 July 2012 on the Promotion, Protection and Enjoyment of Human Rights on the Internet was the first reformative act that emphasized the significance and the relationship between human rights protection and a free flow of information in the Internet[7]. Its main message was that the rights and freedoms that are protected in the real world should be adequately secured in the Internet. A particular attention was paid to the protection and respect of the freedom of speech regardless of the administrative frontiers and mass media used, with the compliance to Art. 19 of the Universal Declaration of Human Rights[8] and the regulations of Art. 19 of the International Covenant on Civil and Political Rights[9]. Despite the fact that the act was not legally binding, it encouraged in a precursory way the 47 member-states of the Human Rights Council (Poland including) to promote and facilitate the access to the Internet and to cooperate internationally as regards information flow that applies modern communication technology[10].

[5] M. Wujczyk, *op cit.*, p. 36.
[6] UN General Assembly Resolution A/RES/60/251 of 15 March 2006 . The UN Human Rights Council started work on 19 June 2006.
[7] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 29.06.2012, A/HRC/20/L.30.
[8] Universal Declaration of Human Rights of 10 December 1948, Art. 19 – " Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers", http://ms.gov.pl/prawa_czl_onz/prawa_czlow_12.doc, ( accessed: 20.03.2018)
[9] International Covenant on Civil and Political Rights of 19 December 1966 (Journal of Laws 1977, No.38 item 167), Art. 19 item 1: Everyone shall have the right to hold opinions without interference, item 2: Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
[10] The UN Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 29.06.2012, A/HRC/20/L.30.

The issue was considered more extensively in the subsequent resolutions of 2014[11] and 2016[12]. The first resolution emphasized the necessity to build trust in the Internet so that its potential is effectively used to create conditions for development and innovations, particularly as a tool that promotes the right to education[13]. The states were encouraged to deal with digital illiteracy and to solve the security problems concerning the freedoms of speech and association and privacy protection. The resolution stipulated for the development and acceptance of adequate national policies in a transparent way and with the cooperation of stakeholders with the aim to give effect to human rights in cyberspace and popularize the global and commonly accessible character of the Internet resources[14]. The other resolution made significant steps against the actions of countries that support discrimination, violence and digital exclusion as regards the Internet and the access to it[15]. It called for the necessity to design, distribute and develop ICT systems with the cooperation of persons with disabilities and to bridge several forms of digital divide with respect to gender [16].

EU recognized the need for the legal protection of the right to privacy in the environment of highly developed IT infrastructure and it deals with this issue – especially in the context of personal data protection[17] - both in its numerous legal regulations and through the judgements of the Tribunal of Justice. When looking at the EU primary legislation, the basis of such approach can be found in Art.16 item 1 of the Treaty on the Functioning of the European Union according to which "Everyone has the right to the protection of personal data concerning them". Another guarantee is given by Art.5 item 1 of the Treaty on European Union which declares the recognition by EU of the rights, freedoms and principles as defined in the Charter of Fundamental Rights of the European Union of 7 December 2007 and also confirms the accession of EU to the European Convention of Human Rights and Fundamental Freedoms.

[11] The UN Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 20.06.2014, A/HRC/26/L.24.
[12] The UN Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 27.06.2016, A/HRC/32/L.20.
[13] The UN Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 20.06.2014, A/HRC/26/L.24.
[14] Ibidem
[15] The UN Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 27.06.2016, A/HRC/32/L.20.
[16] Ibidem.
[17] H. Szewczyk, *Ochrona dóbr osobistych w zatrudnieniu*, Kraków 2007, pp. 53–113; J. Braciak, *Prawo do prywatności*, Warszawa 2004, pp. 61–111.

The issues of the protection of information privacy that are covered by the Chart and are legally binding in all EU member states under the Treaty of Lisbon of 13 December 2007[18] should be considered as crucial due to the fact that the act includes all rights of humans and citizens that are fundamental for contemporary Europe[19]. One should particularly mention here Article 8 of the Charter - *Everyone has the right to the protection of personal data concerning him or her* , (item 2*) such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified and* (item 3) *Compliance with these rules shall be subject to control by an independent authority*. This regulation, being a specific kind of primary law, should be considered a desirable one with the increasing volume of data that is stored by particular institutions. When looking at secondary legislation, the first fundamental *acquis communautaire* that was delegated from Article 16 item 2 of the Treaty of the Functioning of EU was the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data[20]. This was implemented to Polish legislation through the Act on Personal Data Protection[21]. One should agree with M.Wulczyk, who states that a certain dichotomy of objectives occurs as – in line with Article 1 of the Directive – all EU member states are obliged on the one hand to protect the rights of their citizens, including the right to privacy, and on the other they are committed not to restrict the free flow of personal data. First of all, it is important to point at the protection range that results from the Directive by defining personal data as all the information relating to a natural person that can or is going to be identified. Personal data processing is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (Directive 95/46/EU Art. 2 b) [22]. It is important that the Directive emphasizes the data subject's consent as one of the requirements for the legality of

[18] EU Official Journal C 303 of 14.12.2007, p. 1 with the corrigendum.
[19] J. Sieńczyło-Chlabicz, *Ochrona prywatności osób powszechnie znanych w świetle Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności i Karty Praw Podstawowych* (in:) A. Wróbel (ed.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009, pp. 231–251.
[20] EU Official Journal L 281 zof23.11.1995, p. 31 as amended.
[21] Act of 29 August 1997 on the protection of personal data (Journal of Laws 2016.0.922, consolidated text)
[22] M. Wujczyk, *op cit.*, p. 60.

data processing (Directive 95/46/EU Art.7). Finally the Directive guarantees every data subject the right of access to his/her data that is subject to processing Directive 95/46/EU Art. 12). In the light of the above regulations, the Directive should be considered to be the first basis for the contemporary protection of privacy as regards information autonomy in EU member states[23]. Due to the specific features and the threat to privacy resulting from an unauthorized access to data in the Internet, the Directive is supplemented by the Directive on Electronic Commerce[24], the setting up of the European Data Protection Supervisor and the **Directive on Privacy and Electronic Communications**[25]. One should not fail to mention GDPR on data protection of individuals as regards personal data processing and free movement which repeals Directive 95/46/EU. This regulation is will take effect in all EU member states on 25 May 2018 after a two-year transition period. Its basic objective is to reach a complete harmonization of material law within EU, which will be discussed below.

## 2. Interpretation of the right to be forgotten upon EU legislation

In the course of reforming the data protection system with regard to the dynamic development of information society, one of the fundamental postulates of the European Commission was to strengthen the so called right to be forgotten, i.e. *the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes*[26]. The issue of the control over personal data by individuals was introduced by Directive 95/46/UE whose provisions were reflected by the implementation of Art. 32, item 1 (6) Act on Personal Data Protection (UODO) in line with which every individual has the right to control the processing of data that concern him or her and are stored in data sets, especially the right to demand the data to be supplemented, updated and rectified, to stop its processing temporarily or permanently or to erase it if it is incomplete, outdated, not true or was collected in breach of the regulation or is no longer indispensable to achieve the purpose for which it was

[23] A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy o dyrektywie Unii Europejskiej*, PiP 1997, vol. 6, p. 29 and the following.
**[24]** Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000 P. 0001 - 0016.
[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (Official Journal *201, 31/07/2002 P. 0037 as amended)*
**[26]** Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union* COM(2010) 609, Brussels 2010

collected. One should consider progressive the introduction of the opportunity (item 7) to require the discontinuation of personal data processing in justified cases or to (item 8) object to data processing in the cases when the data controller intends to use the data for marketing purposes or when the data is transferred to another data controller.

A.Mednis is right to say that the analysis of the UODO regulations indicates that the control of individuals over their data, especially when it aims at the deletion of the data, is rather limited. This is due to the fact that the data controller is obliged to erase the data if it is collected with the violation of regulations and consequently this is impossible during the implementation of an agreement or in the cases of data that was collected in line with the agreement. One should also point at one of the rights of the data controller that involves a disturbing imprecision as regards the interpretation of the right according to which a written demand justified by *a special situation* of the data subject should be presented (Art. 32, item 1 (7) Act on Personal Data Protection ) (UODO) that the data processing should be ceased when based on some indefinite reasons, i.e. to accomplish tasks for the sake of the society and legally justified objectives[27].

In March 2010, one party to the proceedings, Mario Consteja Gonzalez – following an unsuccessful intervention at the publisher of the La Vanguardia – contacted Google and demanded that search engines in Google should not show the links to the outdated information concerning the bidding of a property[28] caused by his payment default. He complained to the Spanish Data Protection Agency which partially upheld the complaint and demanded the Google's search engine operator, as a body held responsible for data processing, to remove the data[29]. In the case of Google Spain and Google Inc., the Tribunal applied a previous definition that was worked out in the Lindqvist case where it was ruled that *processing of personal data wholly or partly by automatic means* [30] within the meaning of Art. 3 item 1 Directive 95/46 covers *any operation or set of operations which is performed upon personal data, whether or not by automatic means*[31]. The judgement was based on the interpretation of the right to remove data as specified in Art.12 (b) of Directive 95/46/EU and the right to object in Art. 14 (a). The

[27] A.Mednis, op.cit. p.29 and the following pages
[28] I.C. Kamiński, Z. Warso, *Czy można zniknąć z Google'a? Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González (C-131/12)*, in: D. Bychawska-Siniarska, D. Głowacka, "Wirtualne media – realne problemy", Warszawa 2014, pp. 51-52.
[29] I.C. Kamiński, Z. Warso, *op. cit.*, p. 52.
[30] Judgement of the EU Tribunal of Justice of 6 November 2003 in the Linquist case, C101/01, item 25, http://curia.europa.eu/juris/document/document. jsf? text=&docid=48382&page Index=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid= 1361686. (Accessed: 24 March 2018)
[31] Ibidem.

judgement pointed out that the processing of the individual's first and second name may affect significantly the right to privacy and personal data protection since the processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual[32]. Moreover, the data subject has the right to address himself to search engines in order to prevent indexing of the information relating to him personally and published on third parties' web pages[33]. The judgement emphasizes the role of search engines as data disseminating instruments that may lead to the violation of the right to privacy, which undoubtedly had its impact on the provision of the new regulation on personal data protection in EU.

## 3. Analysis of selected issues at the threshold of the EU reform of personal data protection

The long anticipated result of the EU debate on the reform of personal data protection – GDPR – will take effect on 25th May 2018. After 22 years, it will replace the directive on e-privacy in an attempt to meet the challenges of the temporary information society. According to *E. Bielak-Jomaa* and *D. Lubasz*, the date is a milestone in the development of the legal protection of personal data; this does not only concern the regulatory issues but also the choice of the legislative means to enforce the objectives of the regulation because– as a European act - it will operate directly in all member-states, which will limit significantly the negative effect of the minimum harmonization resulting from Directive 95/46 /EC [34]. The scale of the changes to be introduced is so wide that the Author of the article analyzed the issues that are significant to Web users.

The new regulations will concern a much wider group of entities, including companies that offer their services in EU but are based beyond EU borders. First of all, the regulation enforces that all companies wishing to offer their services in EU – regardless of the fact whether they are based in a member-state or not – should apply the European data protection law; thus level playing field is enforced[35]. Another crucial change is the requirement for business to conduct assessments of the impact of processing on personal data protection and - in specified

[32] M. Czerniawski, *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych*, "Europejski Przegląd Sądowy" 05/2015, pp. 4-5.
[33] Ibidem.
[34] E. Bielak-Jomaa (ed.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, LEX/el. 2018.
[35] K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?*, Warszawa 2017, pp. 20-22.

cases - to consult GIODO (Inspector General for the Protection of Personal Data) even before the processing is started. In line with the new regulation, the processing should meet the criteria of transparency, responsibility and accountability as regards entities that deal with big data commercialization. The clarification of protection standards in this area should encourage business actors to introduce innovative technological and organizational solutions that will protect personal data in an effective and efficient way against the violation of data confidentiality.

With regard to the concern about data security one should appreciate the fact that GDPR advocates for the removal of any data that enables user's identification (unless they are indispensable), the substitution of individualizing data with artificially generated identifiers and data encryption so that only authorized persons can read them[36]. When considering profiling, which currently tends to have increasingly invasive forms, it is of crucial significance that the regulation defines it *as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements*; (GDPR, Art. 4 item 4). The authorized person will have the capacity to collect data for purposes that are strictly defined in advance and after they are collected they cannot be processed for other purposes without an additional consent of the data subject, which practically means that the data controller cannot store more data then needed[37]. Considering the main objective of GDPR, i.e. the protection of information autonomy, data controllers will be forced to inform data subjects in a clear and comprehensible way about the time and method of the processing. It is crucial for the provision of real control that data controllers will be obliged to ensure the authorized persons the right to access the data, to rectify it, to restrict the processing and to remove the data (the right to be forgotten). According to Article 4, item 32 *Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.* One cannot disagree with K.Szymielewicz who says that that the standards concerning the consent

[36] Ibidem, p.22.
[37] K. Szymielewicz, W. Adamska, *op. cit.,* p. 20-22.

are not as strict as the current ones in Poland since GDPR does not require the consent to be expressed in a literal way[38].

In conclusion, a real achievement of the goal to harmonize the level of personal data protection does not only depend on the application of the new law by data controllers, supervising bodies and courts but also on the activity range of national legislators[39]. Due to the range of the changes that are being introduced, both the national legislator and data controllers should analyze as quickly as possible the new mechanisms of data protection and take steps to ensure the compliance of regulations with the EU regulation[40].

## Conclusions

The development of the market of new technologies which mostly involves collecting and processing data that are mainly commercial in character may pose a significant threat to the right to privacy of web users. The EU regulator is aware of the ubiquity of the storage of the data on the Internet users and the resulting threat to their right of privacy. The previous regulations regarding privacy protection, despite being fundamental, were created in a completely different technological situation and consequently there is now a demand for an update that will regain their effectiveness and match contemporary standards of information society. GDPR is an attempt to react to the challenge in a sustainable way and with respect to various business models by creating equal conditions for all entrepreneurs so that in the long run the gap is bridged between the real and the desired protection level of personal data. In the response to the remark made in the introduction about the Orwell ‘s vision that suggests the acceptance of the end of privacy in cyber space, the author wishes to make it clear that the protection of privacy is purposeful as long it is the condition for freedom.

## Bibliography

[1] Bielak-Jomaa E. (ed.), Lubasz D.(ed.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, LEX/el. 2018. (Commentary on GDPR)

[38] Ibidem
[39] Ibidem
[40] E. Bielak-Jomaa (ed.), D. Lubasz (ed.), *op. cit.*, LEX/el.

[2] Czerniawski M., *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych,* "Europejski Przegląd Sądowy" 05/2015.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *(Official Journal L 281 , 23/11/1995 p. 0031 – 0050 as amended*
[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000 P. 0001 - 0016.
[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (Official Journal *201 , 31/07/2002 P. 0037 as amended)*
[6] Kamiński I. C., Warso Z., *Czy można zniknąć z Google'a? Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González (C-131/12),* w: D. Bychawska-Siniarska, D. Głowacka, "Wirtualne media – realne problemy", Warszawa 2014.
[7] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union* KOM(2010) 609, Brussels 2010
[8] Mednis A., *Ochrona danych osobowych w konwencji Rady Europy o dyrektywie Unii Europejskiej*, PiP 1997, vol. 6.
[9] International Covenant on Civil and Political Rights of 19 December 1966 (Journal of Laws 1977, No.38 item 167)
[10] Orwell G. *1984*, Warszawa 2003.
[11] Universal Declaration of Human Rights of 10 December 1948; http://ms.gov.pl/prawa_czl_onz/prawa_czlow_12.doc.
[12] UN General Assembly Resolution A/RES/60/251 of 15 March 2006
[13] **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) (Official Journal EU** L 119/1 4.05.2016)
[14] Safjana M., *Prawo do ochrony życia prywatnego* [in:] *Podstawowe prawa jednostki i ich sądowa ochrona*, (ed. L. Wiśniewski), Warszawa 1997.
[15] Sieńczyło-Chlabicz J., *Ochrona prywatności osób powszechnie znanych w świetle Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności i Karty Praw Podstawowych* (in:) A. Wróbel (ed.), *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, Warszawa 2009.
[16] Szewczyk H., *Ochrona dóbr osobistych w zatrudnieniu*, Kraków 2007, pp. 53–113; J. Braciak, *Prawo do prywatności*, Warszawa 2004.
[17] Szymielewicz K., Adamska W., *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?,* Warszawa 2017.
[18] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 29.06.2012, A/HRC/20/L.30.

[19] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 20.06.2014, A/HRC/26/L.24.
[20] The UN Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, 27.06.2016, A/HRC/32/L.20.
[21] Traktat Lizboński z Lizbonie z 13 grudnia 2007 r. (Dz. Urz. UE C 303 z 14.12.2007, s. 1 ze sprost.). Treaty of Lisbon of 13 December 2007 (Official Journal EU C 303, 14.12.2007 p.1)
[22] Act of 29 August 1997 on the protection of personal data (Journal of Laws 2016.0.922, consolidated text)
[23] Wujczyk M., *Prawo pracownika do ochrony prywatności*, Warszawa 2012.
[24] CJUE Judgement of 13 May 2014, C131/12, in the case of Google Spain SL and Google Inc. versus Agencia Español-la de Protección de Datos (AEPD) and Mario Costeja González
[25] CJUE Judgement of 6 November 2003, C101/01, item 25, in the Lindqvist case

***Abstract***

The development of the market of new technologies which mostly involves collecting and processing data that are mainly commercial in character may pose a significant threat to the right to privacy of web users. Considering the challenge that results from a developed IT infrastructure, the author aims at the legal assessment of the right to privacy in e-communication in the light of the present EU regulations and the judgements of the UE Tribunal of Justice. The article presents the analysis of legislation regarding the right to be forgotten and the selected implementation issues of Regulation 2016/679 (GDPR)