ASEJ
Scientific Journal
Bielsko-Biala School of Finance and Law

Volume 25 | Number 4 | December 2021

ISSN2543-9103
eISSN2543-411X
www.asej.eu

Bielsko-Biała

Bielsko-Biala School of Finance and Law
Wyższa Szkoła Finansów i Prawa w Bielsku-Białej

Scientific Journal

Zeszyty Naukowe

Academic Quarterly Publication
Vol 25, No 4 (2021)

Bielsko-Biala 2021

DOI: 10.19192/wsfip.sj4.2021.4 ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

The right to privacy and personal data protection in the age of new technologies

Krystian Kucharczyk[1], Paweł Joachymczyk[2]

[1]Bielsko-Biala School of Finance and Law
Tańskiego 5 43-300 Bielsko-Biała - Poland

[2] University of Warsaw
Krakowskie Przedmieścia 26/28, Warszawa - Poland

***Abstract*— The issue of the existence of the right to privacy and the related right to protection of personal data is so wide in the modern world that it prompts an analysis of the regulation in this area. The last decades have brought a significant development of new technologies, having a huge impact on our lives. It is linked to two industrial revolutions: the third (scientific and technological) and the fourth (digital). The biggest change facing the individual is the process of digitisation of social life. The possibilities of new devices are constantly increasing in terms of reception, data processing and also automation. With this progress, a significant part of everyday duties has been transferred to the virtual sphere. Taking this into account, the topic of this work is limited to issues related to ICT technologies, which influence people directly and indirectly on a daily basis. This is mainly due to the fact that an individual constantly interacts with such technologies, for example in the form of mobile phones, computers or the Internet. This is shown by a report prepared by the National Debt Register, according to which, even before the pandemic, as many as 80% of Poles spent more than one hour a day in front of a screen, and one in four spent more than three hours. Furthermore, almost half of Poles use e-banking, and among the five activities they do most frequently using their phones, as many as three relate strictly to the Internet.**

Keywords—New technologies, personal data, Poland, UE law

I. INTRODUCTION

The issue of the existence of the right to privacy and the related right to protection of personal data is so wide in the modern world that it prompts an analysis of the regulation in this area. The last decades have brought a significant development of new technologies, having a huge impact on our lives. It is linked to two industrial revolutions: the third (scientific and technological) and the fourth (digital). The biggest change facing the individual is the process of digitisation of social life. The possibilities of new devices are constantly increasing in terms of reception, data processing and also automation. With this progress, a significant part of everyday duties has been transferred to the virtual sphere. Taking this into account, the topic of this work is limited to issues related to ICT technologies, which influence people directly and indirectly on a daily basis. This is mainly due to the fact that an individual constantly interacts with such technologies, for example in the form of mobile phones, computers or the Internet. This is shown by a report prepared by the National Debt Register, according to which, even before the pandemic, as many as 80% of Poles spent more than an hour a day in front of a screen, and one in four spent more than three hours. Furthermore, almost half of Poles use e-banking, and among the five activities they do most frequently using their phones, as many as three relate strictly to the Internet.

II. THE MAIN PART OF THE CONSIDERATION

Before the COVID-19 pandemic, 35% of our country's population spent 2-3 hours using the Internet for private purposes each day, while one in four exceeded the indicated time frame (kdr.pl). The use of Internet systems has increased, and so has the flow of our data. This forces us to think about privacy in the face of the increasing digitalisation of life. The processing, collection or retrieval of personal data has become an everyday reality. The protection of personal data will be a challenge for years to come, due to technological processes and the aforementioned progressive digitisation. We should agree with the words of A. Sakowicz: "The twentieth century was a breakthrough period in terms of giving meaning to the word "privacy", as a result of which at the beginning of the twenty-first century it is very well known through the mass media. The modern individual learns more and more often about violations of his/her personal rights, including privacy. The technical possibilities of modern civilisation mean that we often become

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 25, No 4 (2021), pages 6
DOI: 10.19192/wsfip.sj4.2021.4
Received: September 2021 Accepted: December 2021 Published: December 2021

unconscious victims, we only begin to feel the need for privacy, like air, when it is in short supply, and Orwell's fiction with the leading slogan 'Big Brother is watching' becomes reality."(Sakowicz, 2006 p. 16-29)

When operating in the digital space, we unknowingly provide a range of different information about ourselves. According to Article 4(1) of 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), hereafter referred to as GDPR, by personal data we mean "any information about an identified or identifiable natural person"((EU) 2016/679) According to D. Chromicka: "The personal data required for the registration of a new user by the above-mentioned service providers are name, surname, date of birth, e-mail address, but they can also be: town, province and chosen industry" (Misztal-Konecka, Tylec, 2012, p.56). The development of technology has meant that our movements, the people we talk to, our interests, the materials we look at and the time we spend on them, the sports we practice, and the ways we eat every day are all subject to tracking (Jaskiernia, Spryszak, 2016, p.202-203). Increasingly, these are data obtained from the information we search or details about our health. Currently, their scope is growing, causing difficulties in defining it concretely. When data are collected or processed, our privacy is violated. Again, one has to agree with A. Sakowicz: "It would be a mistake to put all the blame for the increasingly frequent invasion of privacy on the development of civilisation. After all, it is the individual who, to a significant extent, decides how the so-called technical novelties will be used and what will happen with the acquired information or data. It is an obvious fact that invasion of privacy can take place without any technical tools or with the help of legal norms."(Sakowicz, 2006, p. 16-29). Threats emerging with technical development become much more complicated. The processes that take place using personal data (aiming at profiling) are more autonomous, independent of human will. There is a growing need to pay special attention to the problem of data protection, both from the systemic point of view, implemented by the state and supra-state organizations, as well as by the users of new technologies, understood not only as consumers operating on the digital market, but also companies providing services to the entities in this space. Given the increased consumer awareness and systemic requirements, the demands for transparency of procedures, ethical principles and objectives of enterprises will gradually increase. Special attention should be paid to the fact that breaches of privacy are committed not only by enterprises, but also by other organisms, including countries, individuals or non-state actors, such as terrorist or criminal organisations. The problematic issue of the activities of states is directed towards immigrants and their own citizens, which is why emphasis is placed on regulation, control of the actions of the administration, and axiological motivation of the behaviour of states. Therefore, the words of M. Rojszczak are true: "Transferring successive spheres of human activity to cyberspace has caused it to become more and more often the subject of interest of public opinion and scientific circles. Due to the lack of reference to physical boundaries, cyberspace is both an opportunity and a threat for building a modern society based on information. An opportunity, because mankind has never before had a tool allowing for a universal exchange of views, unlimited by the available media, and development of new forms of building social relations (e.g. dynamic development of social networks). A threat, because the same technologies that facilitate communication between groups of people can also be used for detailed monitoring of their activity. Electronic surveillance also existed in the times before the emergence of the Internet, but the technical possibilities associated with its conduct were nothing like the solutions available today."(Rojszczak, 2018, p. 32-49) The obligation to take appropriate legislative action to standardise and regulate the digital market rests with the state (Domagała, 2010, p. 75-86). In most cases, appropriate regulations have already been adopted or steps have been taken towards this. However, the constant progress of technology forces constant analysis of the market and the obligation of the legislator to adapt to new technologies. The issues of artificial intelligence, user profiling, new financial technologies or advanced spyware cannot be ignored. Regulations should keep pace with a digitalised market that has no borders in the classic sense. The technological and legislative challenge facing public bodies will not go away in the coming years, and constant reflection and market observation is required.

So far, no comprehensive definition of privacy has been found in the doctrinal and normative spheres (Machowicz, 2009, p. 81). A. Sakowicz defines the problem of interpretation of the right to privacy as follows: "It should be further stated that privacy is not a unidimensional concept in terms of terminology or content. This causes privacy to be called "a general label, stuck to the baggage of values and rights", and arriving at its definition is no easier than finding a consensus in relation to the definition of freedom. It also causes that definitions of privacy are vague, they do not enumerate its components - they indicate them in a non-specific way, therefore they are of a general nature." (Sakowicz, 2006, p. 16-29) Transmission of data to virtual reality causes the possibility of loss of privacy, contained in the data. Article 17(1) of the International Covenant on Civil and Political Rights states that: "No one shall be subjected to arbitrary or unlawful interference with his private life, family, home or correspondence nor to unlawful attacks on his honour and reputation" (ibr.sejm.gov.pl). Article 12 of the Universal Declaration of Human Rights formulates the matter similarly: "No one shall be subjected to arbitrary interference with his private life, family, home or correspondence, or to attacks on his honour and good name. Everyone has the right to legal protection against such interference and attacks"(libr.sejm.gov.pl) The Polish legal system, facing the challenge of protecting the rights of individuals, has also introduced the right to privacy as one of the guaranteed rights in the Constitution, in the form of Article 47 of the Polish Constitution: "Everyone has the right to legal protection of his private life, family life, honour and good name and to decide on his personal life"(Journal of Laws 1997 No.

78 item 483) Based on this, we can assume that by privacy is understood the good being peace in personal life, family life or as the secrecy of correspondence and good name and dignity of the individual. In turn, the Constitutional Court, in the justification of the judgment of 24 June 1997 on banking and brokerage secrecy and the secrecy of investment instructions, notes that the right to privacy constitutes: "principles and rules relating to various spheres of an individual's life, and their common denominator is the grant to the individual of the right to live his or her own life arranged according to his or her own will with the limitation to the necessary minimum of any external interference"(Judgment ref. K21/96) A similar view, according to K. Machowicz, follows from the line of jurisprudence of the European Court of Human Rights(Machowicz, 2009) The Supreme Court cites the decision of 18 August 1999 in which the ECHR indicates in its judgments: "[...] by privacy is to be understood as a state of affairs in which the individual would be left alone in all essential spheres of physical and spiritual life (not connected with the conduct of public activities) when he or she so wishes and when this does not conflict with important general interests and the freedoms of other persons"(Syng. Judgment II CKN 321/99) The opinion of the Supreme Court should also be noted, presented in the judgment of 29 March 2017, where it is presented that the right to privacy is expressed primarily in the right to lead one's own life with a minimum of interference from other persons, by the concept of privacy many goods are understood (Judgment Syng. IV KK 413/16).

Kosonoga referred to the judgment, stating: "In Article 190a § 1 of the Criminal Code, the legislator did not narrow this concept to specific values. Such a redaction of the provision leads to the conclusion that the legislator's intention was to provide broad criminal law protection. Privacy as defined in article 190a § 1 of the Penal Code can therefore be perceived in the aspect of private life, family life, inviolability of dwelling, secrecy of correspondence or protection of information concerning a given person. In the legislative recitals it was reasonably emphasised that the notion of privacy cannot and should not be identified exclusively with a person's life centre, such as a property, a flat or a house, for privacy is not only a place in the world, but first and foremost the sphere of freedom to decide about everything that is important from the point of view of personal life and the lack of obligation to endure conditions that significantly violate a person's personal goods, in particular such as: health, freedom, honour, surname, image or the secrecy of correspondence. " (Kosonoga, 2017) It is also worth looking at the explanation of the need for the provision, i.e. the justification of Article 190a of the Criminal Code, in which attention was drawn to the use of electronic means in prohibited activities(senat.pl). The amendments to the Penal Code emphasise the increasing frequency of this type of behaviour and the function of privacy protection provided by the provision (senat.pl). Confidentiality is a broader issue than personal data, however it is based on them.

Going beyond the classical conceptual framework for the purposes of this work, we may consider that the right to privacy consists of the broadly understood right to the protection of personal data, representing the translation of our lives from the real to the virtual sphere, as well as the totality of our actions taken on the Internet. Due to the nature of this paper, selected legal aspects of the protection of rights will be discussed rather than reference to the practice of their use. The challenge facing the justice system is very well illustrated by the words of Mark Zuckerberg, the main creator and CEO of the social networking site Facebook: "Privacy is no longer a social norm"(theguardian.com) However, in contrast to Mark Zuckerberg's words, the right to privacy is a constituent element of many different legal systems and is a universally recognised human right (Rojszczak, 2019).

The right to protection of private life does not apply only to the actions of the state, but also to other institutions or persons - both private and public. According to Machowicz: 'the right to private life implies the obligation of the state to ensure the physical and psychological integrity of the person' (Machowicz, 2009, p. 81) In Poland it has no long-term historical basis (Chmaj, 2016, p. 120). The Constitutional Court pointed out the close relationship between the right to privacy (Article 47 of the Polish Constitution) and the right to personal data protection (Oniszczuk, 2004). This affects this part of the work, focusing on the legal aspect of privacy protection with regard to the right to personal data protection. In the context of the development of new technologies in the creation of a digital society, two problems stand out the most. The judicial system is confronted with the concept of the 'right to be forgotten' and the issue of regulating the processing and sharing of user information. When we decide to transfer our data, we enter into an electronic contract for the provision of services (Misztal-Konecka, Tylec, 2012). Pursuant to Article 8.1.1 of the Act of 18 July 2020 on the provision of services by electronic means (Journal of Laws of 2002, No. 144, item 1204), the service provider is obliged to determine its regulations, including the conduct of activities in social media. The same normative act contains an indication in paragraph 3, point 3, Article 8, concerning components of the regulations, namely: "conditions for conclusion and termination of contracts for the provision of services by electronic means", thus the issue of abandonment of the presence in the sphere of digital service. This issue is also addressed in Article 17 of the GDPR. The regulation gives the right to demand from the controller the "immediate erasure of personal data" and orders to execute it without undue delay, provided that one of the prerequisites is met. The European Parliament has distinguished that such an action may take place in the event: the achievement of the purposes and the loss of the necessity of the data possession by the controller, the withdrawal of the consent to the data processing required by Article 6(1)(a), the exercise of the right to object contained in Article 21(1), giving the possibility to bring it against the processing of the information, related to his/her particular situation, and the illegality of the data processing. Furthermore, the deletion of data is due to a legal obligation or following the consent of a child over 16 years of age or younger with parental consent, in the case of the provision of information society services.(OJ L 119, 4.5.2016). At the same time, this nullifies the possibility of their processing by the controller

The EU law also imposes on the controller the obligation to restrict the processing of personal data in cases described in Article 18 of the aforementioned Regulation or, pursuant to Article 16, to rectify the data immediately. In case of these three situations, which have their source in Article 16, 17 and 18, there is also an obligation (if possible and not requiring disproportionate measures) to inform about the change of the status of personal data and to release the data about their recipients. The basis for this is Article 19 of the GDPR. P. Fajgielski in his commentary to the Regulation points out to the debatability of the obligation to inform, where "it also refers to situations where the controller completed the processed data at the request of the data subject, in case they were incomplete (pursuant to Article 16, sentence 2). The literal interpretation leads to the conclusion that the obligation to notify does not cover this kind of cases, as they are not explicitly indicated in the commented provision, whereas the functional interpretation leads to the opposite conclusion. It seems that, in practice, the controller should assess whether the data supplementation entails the necessity to notify the recipients (due to the need to protect the data subject's rights) and, if such necessity is found, should notify the recipients of the data supplementation."(Fajgielski, 2018). Section 4 of the GDPR addresses the issue of the right to object and automated decision-making in individual cases. In Article 21 there is the right to object, i.e. to stop the processing of data. It is of a specific nature and is used only in the cases listed in the Regulation, for which the legislator has reserved this model of procedure. The specificity of the provision stems from "the balance between the rights of the data subject and the rights of the controller processing the data." (Fajgielski, 2018) The legislator reserves situations in which this is not available. P. Fajgielski explains that: "the right to object does not apply in cases where the controller has obtained the consent of the data subject; performs a contract; there is a legal obligation for the performance of which the processing is necessary, and where the processing is necessary to protect the vital interests of the person" (Fajgielski, 2018). The issue of profiling, or according to Article 4 of the Regulation: "any form of automated processing of personal data which consists in using personal data to evaluate certain personal factors relating to an individual, in particular to analyse or predict aspects relating to that individual's performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement" (OJ L 119, 4.5.2016), is addressed by Article 22 of the Regulation. This provision deals with the method of decision-making by automated means in relation to the data subject. It is worth noting that the legislator emphasizes the application of the provision only if the decision produces legal effects in relation to the person, or affects him in a similar way. The legislator pays particular attention to the mechanisation of the decision-making process, because in the case of a full, autonomous, human-independent process of modernisation of data processing, persons do not have the possibility to correct or interfere with this process (Fajgielski, 2018) The GDPR regulations also include the obligation to compel the controller to perform an impact assessment of the planned data processing. The legislator emphasises that this measure should be applied in particular to new technologies (OJ L 119, 4.5.2016.) The application of personal data protection regulations (not only concerning GDPR) is an increasingly frequent phenomenon. An example is the case of Lynette Copland v UK before the ECHR (judgment 62617/00). It concerned the control of emails by an employer, as well as web browsing and telephone calls (judgment 62617/00)

The GDPR regulations are not the only provisions applicable in Poland, as in addition to them there are also specific provisions in other laws. Further work is currently underway to improve the standards for the protection of the right to privacy and the right to personal data protection. Particular mention should be made here of the "E-Privacy Regulation." (ur-lex.europa.eu) that is planned for introduction. An important normative act to mention here is also Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, laying down measures on access to the open internet and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks or services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. It restricts the use of our personal data to "serve" profiled, often third-party dependent, information on the internet. The regulation implements the right of internet neutrality (OJ L 310, 26.11.2015). As justification for its introduction, the desire to limit the arbitrary decision of the operator, usually motivated by commercial considerations, was indicated. Information about concrete commercial offers is mainly created based on "click-through" data, web content viewed or material made publicly available

The right to privacy can also be violated by breaking criminal law. Article 190a §1 and §2 of the Criminal Code addresses the phenomenon of stalking. The Court of Appeal in Wrocław presented a view according to which: "The persistent behaviour of the perpetrator will be evidenced, on the one hand, by his/her particular mental attitude, expressed in the persistence of harassment, i.e. persisting in a kind of stubbornness, despite requests and admonitions from the victim or other persons to cease the behaviour in question, and on the other hand, by the prolonged lapse of time over which the perpetrator engages in it. The effect of the perpetrator's behaviour must be to create in the victim a justified sense of threat or a sense of a significant breach of their privacy."(ruling II AKa 18/14). The legislator in Art. 190a of the Penal Code does not specify the manner of carrying out stalking or impersonating another person. Therefore, we may assume that an activity carried out with the use of new technologies is also subject to criminal liability from 6 months to 8 years imprisonment. The Parliament pays great attention to this type of crime, as illustrated by the amendment to the Penal Code, during which the possible penalty for this type of act was increased by 5 years. Looking at their frequency, in 2015 as many as 6697 proceedings were initiated under Article 190a of the Penal Code, of which crimes under §1 constituted the dominant majority - 5436 proceedings were recorded (stalking.com.pl). It is worth noting that in Poland there is also a practical use of §2 of Article 190a. An example

of this is the judgment of the District Court in Olsztyn of 29 September 2014(judgment VII K 700/14).

III. cONCLUSION

To recapitulate, the legislator has prepared a number of different legal norms, derived from both EU and national law. They provide a wide range of possible actions for users of the law and individuals to protect themselves in the digital revolution era. It should not be forgotten, however, that technological progress will force the increasing use of new regulations and their constant modification, which legislators - EU and national - must bear in mind. This results in constant monitoring of the phenomena by the UODO, and consequently in the transfer of even broader competences to it than currently envisaged (Journal of Laws 2018, item 1000). Procedures and rules for data processing should be developed. At the same time, the legislator must note that the progress in this field is enormous and the rules in the traditional legislative way may not keep up with it. As a consequence, the best proposal may be to transfer the regulatory competences (in this respect) to the PDO or, in the case of the digital sphere, to the Ministry responsible for digitalisation. It should also be mentioned that due to the Digital Single Market policy of the European Union, it is necessary to coordinate all activities related to European institutions. Every year we produce as much as 1.2 zettabytes of data, so they must be used with respect for the right to privacy and protection of personal data (Jaskiernia, Spryszak, 2016) Currently, this is quite a challenge, but still, thanks to legislative efforts, feasible. Again, the answer to the title question is difficult. The existence of the right to privacy and personal data protection, provided by the judiciary and an extensive system of legal norms, seems to be the most correct. Particularly important was the introduction of EU regulations in this aspect in 2016 along with the possibility of financial penalties, which increased the responsibility of companies. The EU regulation is assessed as one of the most comprehensive solutions of its kind.(Rojszczak, 2019) Similarly, the changes that are being introduced into the Polish system are adequate. Nevertheless, it should be noted that even the best law does not work without people, hence education in this area is important, as well as ensuring adequate pressure, in the form of possible sanctions in the future, for individuals who break legal norms. It is necessary for the law to undergo constant reflection and evolution in order to keep up with the changing world. New regulations must be constantly introduced so that the law does not become outdated. It should be mentioned that this mainly concerns executive acts, laws and EU regulations. It is also important to make broader efforts to coordinate legislative activities at international and EU level. In modern times, despite the challenges, the right to privacy and protection of personal data has not lost its sense of existence.

IV. REFERENCES

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 nr 78 poz. 483).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych (Dz.U. 1977 nr 38 poz. 167).

Powszechna Deklaracja Praw Człowieka, źródło: http://libr.sejm.gov.pl/tek01/txt/onz/1948.html [dostęp na 14.11.2019 r.].

Ustawa z dnia 18 lipca 2020 o świadczeniu usług drogą elektroniczną (Dz. U. 2002 Nr 144 poz. 1204).

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz.U. L 119 z 4.5.2016.

Ustawa z dnia 10 maja 2018 r. o Ochronie Danych Osobowych [Dz.U. 2018 poz. 1000].

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny [Dz.U. 1997 Nr 88 poz. 553].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii [Dz.U. L 310 z 26.11.2015].

Wyrok Trybunału Konstytucyjnego w sprawie tajemnicy bankowej i maklerskiej oraz tajemnicy dyspozycji inwestycyjnych; art. 1 ustawy z dnia 31 maja 1996 roku o zmianie ustawy o zobowiązaniach podatkowych oraz o zmianie niektórych ustaw [sygn. K21/96].

Wyrok Europejskiego Trybunału Praw Człowieka z 3 kwietnia 2007 [sygn. 62617/00].

Wyrok Sądu Najwyższego z dnia 18 sierpnia 1999 r. [sygn. II CKN 321/99].

Wyrok Sądu Najwyższego z dnia 29 marca 2017 r. [sygn. IV KK 413/16].

Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 19 lutego 2014 r. [sygn. II AKa 18/14].

Wyrok Sądu Rejonowego w Olsztynie z dnia 29 września 2014 r. [sygn. VII K 700/14].

Chamaj M(2016) Wolności i Prawa Człowieka w Konstytucji Rzeczypospolitej Polskiej(ed.), 3 wydanie, Warszawa

Domagała M.(2010), Prawnokarna ochrona prywatności użytkowników Internetu, PiP, nr 3

Fajgielski P.(2018), Ogólne Rozporządzenie o Ochronie Danych Ustawa o Ochronie Danych Osobowych Komentarz, 1 wyd, Warszawa,

Jaskiernia J, Spryszak K. (red.), Międzynarodowe standardy ochrony praw człowieka a doświadczenia Polski, Toruń 2016,

Kosonoga J.(2017), Głosa do wyroku SN z dnia 29 marca 2017 r., IV KK 413/16.

Machowicz K.(2009), Ochrona praw człowieka w Rzeczypospolitej Polskiej na tle standardów europejskich, 2 wyd., Lublin 2009,

Misztal-KoneckaJ. , G. Tylec (2012), Ewolucja Prawa Polskiego pod wpływem Technologii Informatycznych, wyd. Wydawnictwo KUL, Lublin

Oniszczuk J.(2004), Konstytucja Rzeczypospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego na początku XXI w., 1 wyd., Kraków.

Rojszczak M., (2019) Geneza prawnej ochrony prywatności [w:] Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warszawa.

Rojszczak M.(2018), Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji, PiP, nr 10

Rojszczak M.(2019) Prawo Unii Europejskiej jako narzędzie podnoszenia standardów w obszarze prywatności w cyberprzestrzeni [w:] Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warszawa

Sakowicz A. (2006) , Prywatność jako samoistne dobro prawne (per se), PiP, nr 1

https://krd.pl/getattachment/4dcfac955-ee35-41b8-9ec5-2d768019c044/Jak-Polacy-korzystaja-z-telefonu-i-Internetu-w-cza.aspx?disposition=attachment

http://ww2.senat.pl/k7/dok/sejm/072/3553.pdf

http:/orka.sejm.gov.pl/Druki8ka.nsf/0/996CE307123D03FEC12583FA0069E8F2/%24File/3451.pdf

https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010

https://stalking.com.pl/2016/08/12/uporczywe-nekanie-statystyka-za-lata-2015-2016/

https://sip.lex.pl/#/monograph/369454046/8?keyword=prywatno%C5%9B%C4%87&tocHit=1&cm=SREST]

WSFiP conducts research and educates students in the following fields:

Finance and Accounting
- Treasure Administration
- Banking
- Corporate Finance
- Accountancy
- Accounting and Finance in Public Sector Institutions
- Corporate Accounting and Controlling
- Audit
- Management and Finance in Real Estate

Law
- this program gives strong legal foundations to undertake further professional training for judges, prosecutors, atorneys, notaries, bailiffs.

Administration
- Fiscal Administration
- Local Government Administration

Logistics
- this program gives good preparation for work in logistics companies as well as in other economic and administrative units.

Cyberspace and Social Communication
- Communication and Image Creations
- Safety in the Cyberspace

Internal Security
- Administration and Management in Security
- Security and Public Order
- Security and Development in Euro-region
- Security of Information and Information Systems
- Security in Business
- Criminology and Investigative Studies
- Criminology and Forensics
- Protection of People and Property
- Public Order Agencies

Information Technology
- Databases and Net Systems
- Computer Graphics and Multimedia Techniques
- Design of Applications for Mobile Devices
- IT Services in Public Administration Units

Postgraduate courses
- Administrative studies
- Fiscal Administration
- Law and management in health service