

Beata Stępień-Załucka

University of Rzeszów, Poland

e-mail: beata@kpmz.pl

ORCID: 0000-0003-1802-680X

THE CONSTITUTIONAL RIGHT TO PRIVACY AND THE OPERATION OF ALGORITHMS VERIFYING ELECTORAL PREFERENCES FROM THE FACE

Abstract

New technologies bring not only many opportunities but also many risks. Some of them we have already got used to, while others still pose a challenge. The latter undoubtedly includes constantly evolving algorithms. Every day we learn about new possibilities for their application. Unfortunately, these possibilities or applications do not always go hand in hand with the existing rights and freedoms and increasingly pose a threat of their infringement. Recently, research results have been published on the recognition of individuals' voting preferences from their faces by an algorithm. Such a possibility in application carries the risk of violation of constitutional rights, including the right to privacy. In this paper, this problem will be developed. First, the essence of the right to privacy will be examined and then, based on the research on facial recognition biometrics, I will present the scope and consequences of its violation.

KEYWORDS

privacy rights, algorithms, face recognition, new technologies

SŁOWA KLUCZOWE

prawo do prywatności, algorytmy, rozpoznawanie twarzy, nowe technologie

1. INTRODUCTION

The 21st century is already considered a breakthrough period in the use of artificial intelligence and algorithms. The most popular ones concern positioning, they are currently used when we want to read news or do shopping on the Internet. With some bitterness, however, it should be said that they have become commonplace, i.e. we know that they exist and we know a certain outline of how they work. However, there are also algorithms whose functioning is completely beyond our knowledge. In other words, we know that they exist, but we do not know how they work. An example of this type of algorithm is the one which uses facial biometrics to determine political preferences. Its operation raises many questions and doubts. These are related, firstly, to the scope of operation of this algorithm and, secondly, to the implementation of constitutional rights and freedoms, including, above all, the constitutional right to privacy. Therefore, in this article, I will try to find an answer to the question of whether the functioning of this kind of algorithm allows the realisation of the right to privacy and whether nowadays, based on the activities of algorithms, we can talk about privacy at all.

2. THE RIGHT TO PRIVACY

The research area thus outlined firstly compels us to define the constitutional right to privacy.

The evolution of the right to privacy dates back to the article “Right to Privacy”. Its authors were two scholars viz. Samuel D. Warren and L. D. Brandeis, who first used this term in 1890 and defined the framework of this right.¹ It should be noted, however, that, first of all, these scientists described the negative aspect of this right, i.e. the right to be left alone, and secondly, that privacy had already existed before this text² appeared, whereas the idea of the right to

¹ S. D. Warren, L. D. Brandeis, *The Right to Privacy*, “Harvard Law Review” 1890, Vol. IV, No. 5, https://groups.csail.mit.edu/mac/classes/6.805/articles/pivacy/Privacy_brand_warr2.html.

² W. Brzozowski, *Prawo do prywatności*, (in:) W. Brzozowski, A. Krzywoń, M. Wiącek (eds.), *Prawa człowieka*, W. Brzozowski, A. Krzywoń, M. Wiącek, Warszawa 2019, p. 174.

protect the sphere of private life had been developing successively, unevenly in all countries.³

In Poland, it was also evolving gradually, starting with the Constitution of the 3rd of May,⁴ through the March Constitution,⁵ the April Constitution⁶ and the Constitution of the People's Republic of Poland (after changes introduced by the Act of 14 February 1976, Journal of Laws No. 7, item 36 with amendments).⁷

At present, the Constitution of the Republic of Poland of 1997, stipulates the right to privacy in Article 47 stating that "Everyone has the right to protection of his private life, family life, honour and good name, and the right to decide about his personal life. In addition to the above obligation to respect and protect privacy and prohibiting interference with this right, is the provision of Article 51 of the Constitution of the Republic of Poland, containing information autonomy."⁸

So what is this right to privacy? Constitutional regulation has not led to the development of a uniform definition of the right to privacy in science. It is identified with the guarantee of freedom and equality, but it is also perceived as a tool to protect one's identity and dignity against discrimination, unauthorised interference in the private sphere of an individual, abuse, or reductionism.⁹ Besides, as far

³ K. Kakarenko, J. Sobczak, *Odpowiedzialność za przestępstwa popełnione w sieci a kwestia prywatności*, (in:) K. Chałubińska-Jentkiewicz, K. Kakarenko, J. Sobczak (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, pp. 2-3.

⁴ The 3rd of May Constitution, referring to the earlier legal tradition, guaranteed religious freedom and personal freedom - the latter, however, limited only to the noble state. M. Wild, *Komentarz do art. 47 Konstytucji RP*, (in:) M. Safjan, L. Bosek, (eds.), *Konstytucja RP*, Vol. I, Warszawa 2016, p. 1163.

⁵ The March Constitution guaranteed in Article 95 "complete protection of life, liberty and property" without distinction of origin, nationality, language or race. It also indicated the conditions for limiting personal liberty (Article 97), certified freedom of movement (Article 101), the secrecy of correspondence and letters (Article 106) and freedom of conscience and religion (Article 111). M. Wild, *Komentarz do art. 47 Konstytucji RP...*, p. 1163.

⁶ The April Constitution guaranteed personal freedom and the inviolability of the dwelling and the secrecy of correspondence (Article 68, paragraph 2), "the possibility of developing their personal values and freedom of conscience, speech and association" (Article 5(2)). M. Wild, *Komentarz do art. 47 Konstytucji RP...*, p. 1163.

⁷ In the case of the Constitution of the People's Republic of Poland, the foundations for the protection of the right to privacy can be traced back to the amendments introduced by the Law of 14 February 1976, Journal of Laws No. 7, item 36 with changes, concerning freedom of conscience and religion (Art. 82(1)), inviolability and personal freedom (Art. 87(1)), inviolability of dwellings and secrecy of correspondence (art. 87(2)). At the same time, it should be noted that these changes in the period of the People's Republic of Poland were theoretical, not practical, and their implementation did not take place until the 1990s. More on the evolution of the right to privacy. M. Wild, *Komentarz do art. 47 Konstytucji RP...*, p. 1163.

⁸ M. Karpiuk, *Konstytucyjne prawo do ochrony prywatności i jego ograniczenie ze względu na bezpieczeństwo państwa. Przykład informacji niejawnych*, (in:) K. Chałubińska-Jentkiewicz, K. Kakarenko, J. Sobczak (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, pp. 2-3.

⁹ M. Sitek, *Prawa (potrzeby człowieka) w ponowoczesności*, Warszawa 2016, p. 181.

as dignity is concerned, both academia¹⁰ and the jurisprudence of the Constitutional Tribunal emphasise the fact that the protection of privacy and informational autonomy is a consequence of the protection of inherent and inalienable human dignity, which was explicitly expressed by the Constitutional Tribunal in one of its justifications.¹¹

This lack of uniform definition of the right to privacy results from the fact that privacy is defined in many ways. Besides, in the literature, there is a view that it is such a broad notion that in determining its essence one should concentrate on distinguishing its various forms and contexts in which privacy is endangered rather than on a strict rule.¹² Therefore, as a rule, it should be assumed that in a narrow sense, the term is understood as a state within the framework of which an individual decides on the scope and extent of the information made available and also communicated to other persons. On the other hand, in a broad context, it is a state in which an individual makes concrete decisions concerning himself, excluding the interference of third parties.¹³ Hence, in the doctrine, we can find definitions which speak about the right of an individual to decide and control the disclosure of information about oneself.¹⁴ Writing about the right to privacy, L. Garlicki points out that it is a collective notion, covering quite a wide spectrum of rights, the core of which is the sphere of autonomy and identity of an individual. In other words, it is the personal space of each individual, to which he can allow access to other persons or deny that access to them. This space concerns: the sphere of sexuality, knowledge of origin, reputation, information about addictions and health, housing as well as communication with the environment.¹⁵

The considerations presented so far make it possible to define the object of privacy protection in various aspects of human life, which include the protection of the integrity and inviolability of this good in particular through the protection of life, health, and human dignity. Moreover, this protection also includes the expectation of the individual that without his or her consent other persons will

¹⁰ M. Karpiuk, *Konstytucyjne...*, p. 199.

¹¹ "The protection of privacy and informational autonomy is a consequence of the protection of inherent and inalienable human dignity" (Art. 30 Constitution), Decision of the Constitutional Court of 30 July 2014, K 23/11, Journal of Laws of 2014, item 1055.

¹² K. Łakomic, *Prawo do ochrony prywatności w kontekście informacji o stanie zdrowia. Autoreferat rozprawy doktorskiej, napisanej pod kierunkiem prof. dr hab. Marka Zubika*, p. 4, <https://www.wpia.uw.edu.pl/uploads/media/5d98c8180784c/autoreferat.pdf?v1> (accessed 1 September 2021).

¹³ J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych*, p. 153, https://repozytorium.uni.wroc.pl/Content/52920/PDF/09_Jakub_Rzucidlo.pdf (accessed 1 September 2021); P. Sarnecki, *Komentarz do art. 47*, (in:) L. Garlicki, M. Zubik (eds.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2006, Vol. II, p. 248.

¹⁴ K. Badźmirowska-Masłowska, *Wizerunek dziecka w Internecie a zagrożenia prawa do prywatności*, (in:) K. Chałubińska-Jentkiewicz, K. Kakarenko, J. Sobczak (ed.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, p. 54.

¹⁵ W. Brzozowski, *Prawo do prywatności...*, p. 174.

not acquire knowledge of the spheres of activity of the individual which he or she does not want to disclose to them.¹⁶ The essence of this right lies, therefore, in the fact that it is the individual himself who determines when, how, and to what extent information about him is made available to others.¹⁷ Moreover, the dimension of access to this information is also important. The sphere of private life will thus include circumstances in relation to which the primacy of the individual's interest should be assumed over the public interest. Consequently, in the case of the right to privacy, there is a presumption of primacy of the right of the individual to be left alone over the public interest or the interest of other entities.¹⁸

On the basis of the foregoing, it may be stated with conviction that privacy is a good of special constitutional value¹⁹ and the right to privacy may be regarded as a general clause on the basis of which the individual finds protection both in his relations with other individuals and with the State. Privacy is a sphere which should not be exposed to external interference, and the individual himself, as a result of his autonomy, has the right to set limits on the accessibility of his personal life to other outsiders.²⁰

The importance and significance of the right to privacy mean that it enjoys special protection. It is confirmed by the fact that, in accordance with Article 233 para. 1 of the Constitution, this right is inviolable under martial law and a state of emergency.²¹ Consequently, no circumstances, not even exceptional or extreme ones, allow the legislator to relax the prerequisites the fulfilment of which would entitle him to invade the sphere of private life, without exposing himself to the charge of unconstitutional arbitrariness.²²

It is important to add that the right to privacy is not a right that enjoys absolute constitutional protection. In Article 31 para. 3 of the Constitution, the legislator has determined the premises on the basis of which this right may be subject to limitations.²³ It is important, however, that such limitations may be established only by statute and only when they are necessary in a democratic state under the

¹⁶ J. Tackowska-Olszewska, *Autonomia informacyjna jednostki a zarządzanie cyfrową tożsamością. Granice autokreacji*, (in:) K. Chałubińska-Jentkiewicz, K. Kakarenko, J. Sobczak (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, p. 45.

¹⁷ K. Łakomiec, *Prawo do...*, p. 4.

¹⁸ J. Tackowska-Olszewska, *Autonomia...*, p. 45.

¹⁹ J. Uliasz, *Konstytucyjna ochrona prywatności w świetle międzynarodowych standardów*, Rzeszów, 2018, p. 26.

²⁰ M. Karpiuk, *Konstytucyjne...*, pp. 2-3. Cf. P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008, p. 116.

²¹ R. Piotrowski, *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne*, (in:) A. Mednis (ed.), *Prywatność a jawność – Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016, p. 19.

²² Decisions of the Constitutional Court of 20 June 2005, K 4/04 OTK –A 2005, No. 6, item 64.; 20 March 2006, K. 17 /05 OTK-A 2006, No. 3, item 30.

²³ M. Florczak-Wątor, *Komentarz do art. 47 Konstytucji RP*; (in:) P. Tuleja (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2019, pp. 169-170.

rule of law for reasons of security, public order, or the protection of the environment, health, and public morals or the freedoms and rights of others, on condition that they may not affect the essence of the rights and freedoms.²⁴ An example of a restriction of the right to privacy based on one of the above grounds may be the need to ensure security. Indeed, security is a component of the public interest and if necessary security cannot be guaranteed, the right to privacy will give way to it. In other words, the right to privacy will be reduced in favour of security and the private interest will be subordinated to the public interest, taking into account the principle of proportionality.²⁵ As a reminder, it should be added that this principle protects constitutional rights and freedoms from undue interference by the legislator. This is done on the basis of a kind of proportionality test, which consists in answering the following questions:

- 1) whether the introduced regulation serves and is necessary for the formation of the legal order,
- 2) whether the goal intended by the legislator is possible to achieve without infringing the legal standards that define the essence of the rights it regulates,
- 3) whether the regulation is necessary for the protection of the interest of a specific constitutional value with which it is connected, and finally,
- 4) whether the introduction of the regulation is in proportion to the burden it imposes on the citizen.²⁶

3. FACIAL BIOMETRICS AS A NEW TECHNOLOGY

Biometrics is the science that deals with the identification and verification of the identity of individuals on the basis of their physical, physiological or behavioural characteristics, called biometrics. Biometric methods use personal – unique, permanent, and measurable – characteristics for this purpose.²⁷ Biometrics are based, for example, on face, retina or fingerprint scanning and recognition, which have become part of the everyday use of new technologies. Biometrics

²⁴ L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2019, p. 120.

²⁵ M. Karpiuk, *Prawo do prywatności w warunkach nowych technologii*, (in:) K. Chałubińska-Jentkiewicz, M. Karpiuk (eds.), *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, pp. 321-322.

²⁶ B. Banaszak, *Prawo konstytucyjne*, Warszawa 2015, p. 379.

²⁷ T. Mendyk-Krajewska, *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, p. 35, http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z54_03.pdf (accessed 1 September 2021); Y. Liu, Identifying Legal Concerns in the Biometric Context, "Journal of International Commercial Law and Technology" 2008, Vol. 3, Issue 1, p. 45 in.; E.J Kindt, *Biometric applications and the data protection legislation. The legal review and the proportionality test*, "Daten-schutz und Datensicherheit" 2007, Vol. 31, Issue, 3, pp. 166-170.

are used to unlock smartphones, iPads, and computers; finger biometrics are part of the passport procedure.²⁸

In addition, in most European countries there has been a rapid increase in the number of cameras in the public domain for video surveillance. This is also related to biometrics and is now seen as a remedy for certain social problems (especially hooliganism) and as an effective tool for catching criminals by recognising faces and automatically matching them with suspects. As a result, over the years monitoring has become an essential component of crime prevention.²⁹

It is, therefore, safe to say that biometrics has become a widely used means of verifying a person's identity. This has been made possible by the new technologies that have evolved in the last decade. Thus, biometric techniques have become reliable means of authentication. Face recognition technology has gained the most popularity. It allows for discreet and easy verification³⁰ and is a non-invasive and contactless way of identifying a person.³¹

This kind of verification is made either on the basis of revealed or undisclosed, hidden activity. The essence of an undisclosed activity lies in the fact that the verification of an individual is carried out without the individual's knowledge and consent. In both cases, verification is carried out using an increasing number of algorithms. Thus, it is possible that an individual is not even aware that at a given moment he or she is being verified by an algorithm that creates an "image" of the individual, "following" his or her facial expressions and gestures against his or her knowledge and will. This image is a collection of information about the subject, which is verified by the algorithm.³² Currently, such an image of a person can be created by an algorithm in the field of voting preferences.

²⁸ T. Wanat, *Akceptowalność automatycznego rozpoznawania twarzy nabywców w handlu detalicznym*, "Handel Wewnętrzny" 2015, No. 3(356), p. 306.

²⁹ L. D. Adkins, *Biometrics: Weighing Convenience and National Security against Your Privacy*, "Michigan Telecommunications and Technology Law Review" 2007, Vol. 13, Issue 2, p. 456; *Biometrics in Large-Scale IT. Recent trends, current performance capabilities, recommendations for the near future*, <https://www.eulisa.europa.eu/Publications/Reports/Biometrics%20in%20Large-Scale%20IT.pdf> (accessed 1 September 2021); Ł. Szwejka, *Rola monitoringu wizyjnego w prewencji kryminalnej*, "Społeczeństwo i Rodzina" 2016, No. 47 (2), pp 80–93, https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/37900/szwejka_rola_monitoringu_wizyjnego_w_prewencji_kryminalnej_2016.pdf?isAllowed=y&sequence=136 (accessed 1 September 2021); J. Szwiercz, P. Matczak, A. Dąbrowski, A. Wójtowicz, *Monitoring wizyjny i jego wpływ na straty spowodowane przestępczością. Przykłady z wybranych polskich miast*, "Studia z Polityki Publicznej. Public Policy Studies" 2020, No. 7 (25), p. 51 *et seq.*; *Biometrics: the state of the art in public safety*, "Nec Public Safety Whitepaper", https://mex.nec.com/es_MX/safety/pdf/wp_biometrics.pdf (accessed 1 September 2021).

³⁰ Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, *Privacy-Preserving Face Recognition*, https://www.researchgate.net/publication/221655685_Privacy-Preserving_Face_Recognition (accessed 1 September 2021).

³¹ T. Wanat, *Akceptowalność...*, p. 306.

³² Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, *Privacy-Preserving...*

Namely, the results of research in the field of verification of voting preferences of individuals by an algorithm have been made public in the literature. The created algorithm can verify political orientation only on the basis of photos.

What's more, the study found that the algorithm is not wrong in more than 70 percent of cases. The study was divided into two stages. In the first stage, the algorithm "was learning". This learning process consisted in the collection of data, i.e. the algorithm studied the face, scanned its features, and coded the support declared by the person studied for a liberal or a conservative. In other words, the algorithm was learning the facial characteristics of people who support liberals and conservatives, and in this way learned how to recognise a person who supports liberals or a person who supports conservatives. The next stage of the study was the self-verification of persons and their political views by the algorithm. Based on the collected data, the algorithm was tasked with determining the political views of individuals from dating and Facebook profiles being shown only one profile. In this way, over a million photos were analysed, on the basis of which the algorithm correctly identified the political views of as many as 72 percent of people.³³ It should be emphasised, however, that the study used single photos of people. Thus, the algorithm assigned political views to the verified person on the basis of only one profile of the person. Therefore, it can be assumed that based on a larger number of photos of the verified person, the accuracy with which the algorithm would determine his or her political preferences would be higher. It is, therefore, safe to say that the potential of the algorithm was not fully exploited in the study. This means that perhaps in the near future, we will see similar studies with more precise results, perhaps even oscillating around the 90 percent effectiveness of the algorithm.

4. THE PERFORMANCE OF A FACIAL ALGORITHM RECOGNISING POLITICAL PREFERENCES IN THE CONTEXT OF THE RIGHT TO PRIVACY

The next question remains: what do these research results mean in practice and, above all, what is their significance for the realisation of the constitutionally guaranteed right to privacy? The answer to the above may come as a surprise. As unbelievable it may seem, by unlocking a phone through face ID we can make available data concerning our electoral preferences. What is most controversial, however, is that people being polled by this type of algorithm may be completely

³³ M. Kosiński, *Facial recognition technology can expose political orientation from naturalistic facial images*, "Nature. Scientific Reports" 2021, Vol. 11, article number 100, <https://www.nature.com/articles/s41598-020-79310-1#Sec2> (accessed 1 September 2021).

unaware that their political preferences are being verified at any given time. This means that we can submit data on support for the party we favour, the party whose views we identify with, not only without being aware of it but even with clear objections to this kind of action. Such a situation is particularly dangerous from the perspective of the implementation of the right to privacy. This is because in such conditions this right cannot be realised effectively, and the operation of an algorithm of this kind directly violates it. The question is: when confronted with such advanced technology, can we still talk about privacy at all?

Unfortunately, when confronted with technology, we still seem to be helpless. This helplessness results from two fundamental issues. Firstly, there is a lack of knowledge about how algorithms work and how the data they collect is used. Secondly, there is a lack of legal regulation which defines the framework within which algorithms operate on the web.

In this matter, it means that such an algorithm operating on the web and recognising people's voting preferences from their faces will deprive an individual of his or her sphere of autonomy, a personal space that is reserved only for that individual. The individual, when confronted with the operation of such an algorithm without his or her consent, will be stripped of information in a sphere that not only he or she does not have to disclose if he or she does not want to, but which is reserved exclusively for him or her. And it is up to each individual to decide whether or not to share it. In other words, the operation of such an algorithm would constitute an unauthorised external interference in the right to privacy, and learning about one's electoral preferences by unauthorised persons may have the same consequences as a breach of the principle of the secrecy of the ballot. Namely, as M. Chmaj writes, depriving the individual – voter of certainty that no positive or negative consequences will occur in relation to him or her.³⁴ At the same time, it should be remembered that data on electoral preferences is special. Their use by unauthorised persons may have even more far-reaching consequences, posing a direct threat to democracy. This is due to the fact that a facial recognition algorithm in combination with an algorithm responsible for positioning data on the web can send an individual to specific websites with information discrediting the party the individual supports or confirming the individual's preferred choice of party.

Additional justification for the above thesis may be found in the fact that it has been widely acknowledged by science that it is contrary to the right to privacy and freedom of data positioning on the web. It needs to be reminded that an individual's privacy is infringed in the network not only when a particular person is individualised and identified by name and surname, but also when he or she is

³⁴ M. Chmaj, *Zasady polskiego prawa wyborczego*, (in:) *System wyborczy w Rzeczypospolitej Polskiej*, M. Chmaj, W. Skrzydło, Warszawa 2008, p. 51.

individualised on the basis of being singled out as a result of activity in the digital environment.³⁵

Moreover, an extra-constitutional light may be shed on this issue by the position of the European Commission Commissioner M. Vestager of February 2021, who, on the basis of the possibilities offered by algorithms connected with face recognition by city cameras, and on the basis of the experience of events in Hong Kong and the way the police there identify protesters, stated that remote verification of faces is illegal and violates the law of the European Union. As a result, a legislative solution is to be prepared at the European level in the near future.³⁶

5. SUMMARY

Summing up the above considerations, I would like to express a certain reflection that we are usually afraid of what is unknown and we are only just getting to know algorithms and their possibilities. However, this learning process and use must be accompanied by legislation that will secure the implementation of fundamental constitutional rights, as well as other rights and freedoms. This is all the more so because nowadays there is no guarantee that algorithms of this kind are not at work, as the scientific world has already found a technical solution to protect individuals from abuse arising from violation of the right to privacy through facial recognition of voting preferences. The scientific answer to this algorithm is a program – a different algorithm – which, by means of strongly enhanced privacy, allows only basic data to be recognised and not to be unauthorisedly processed by different kinds of algorithms.³⁷

However, no matter how uncertain the performance of these types of algorithms is, it remains certain that facial recognition of political preferences of verified individuals violates the constitutionally guaranteed right to privacy and, what is more, constitutes a threat to the essence and functioning of democracy not only in Poland, but also worldwide.

³⁵ W. Lis, *Zjawisko profilowania jako przejaw naruszenia prawa do prywatności w środowisku cyfrowym*, (in:) K. Chałubińska-Jentkiewicz, K. Kakarenko, J. Sobczak (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, p. 177.

³⁶ Komisja Europejska: *zdalne rozpoznawanie twarzy łamie prawo*, <https://www.telepolis.pl/tech/prawo-finanse-statystyki/komisja-europejska-zdalne-rozpoznawanie-twarzy-lamie-prawo> (accessed 1 September 2021).

³⁷ Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, *Privacy-Preserving...*

REFERENCES

- Adkins L. D., *Biometrics: Weighing Convenience and National Security against Your Privacy*, "Michigan Telecommunications and Technology Law Review" 2007, Vol. 13, Issue 2
- Badźmirowska-Masłowska K., *Wizerunek dziecka w Internecie a zagrożenia prawa do prywatności*, (in:) K. Chałubińska-Jentkiewicz (ed.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017
- Banaszak B., *Prawo konstytucyjne*, Warszawa 2015
- Biometrics: the state of the art in public safety*, "Nec Public Safety Whitepaper", https://mex.nec.com/es_MX/safety/pdf/wp_biometrics.pdf (accessed 1 Septemeber 2021)
- Biometrics in Large-Scale IT. Recent trends, current performance capabilities, recommendations for the *near future*, <https://www.eulisa.europa.eu/Publications/Reports/Biometrics%20in%20Large-Scale%20IT.pdf> (accessed 1 September 2021)
- Brzozowski W., *Prawo do prywatności*, (in:) *Prawa człowieka*, Brzozowski W., Kerzywoń A., Wiącek M., Warszawa 2019
- Chmaj M., *Zasady polskiego prawa wyborczego*, (in:) *System wyborczy w Rzeczypospolitej Polskiej*, Chmaj M., Skrzydło W., Warszawa 2008
- Erkin Z., Franz M., Guajardo J., Katzenbeisser S., Lagendijk I., Toft T., *Privacy-Preserving Face Recognition*, https://www.researchgate.net/publication/221655685_Privacy-Preserving_Face_Recognition (accessed 1 September 2021)
- Florczak-Wątor M., *Komentarz do art. 47 Konstytucji RP*, (in:) Tuleja P. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2019
- Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2019
- Kakarenko K., Sobczak J., *Odpowiedzialność za przestępstwa popełnione w sieci a kwestia prywatności*, (in:) Chałubińska-Jentkiewicz K., Kakarenko K., Sobczak J. (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017
- Karpiuk M., *Konstytucyjne prawo do ochrony prywatności i jego ograniczenie ze względu na bezpieczeństwo państwa. Przykład informacji niejawnych*, (in:) Chałubińska-Jentkiewicz K., Kakarenko K., Sobczak J. (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017
- Karpiuk M., *Prawo do prywatności w warunkach nowych technologii*, (in:) Chałubińska-Jentkiewicz K., Karpiuk M. (eds.), *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015
- Mendyk-Krajewska T., *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z54_03.pdf (accessed 1 Septemeber 2021)
- Lis W., *Zjawisko profilowania jako przejaw naruszenia prawa do prywatności w środowisku cyfrowym*, (in:) Chałubińska-Jentkiewicz K., Kakarenko K., Sobczak J. (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017
- Łakomiec K., *Prawo do ochrony prywatności w kontekście informacji o stanie zdrowia* Autoreferat rozprawy doktorskiej, napisanej pod kierunkiem prof. dr hab. Marka Zu-

- bika, <https://www.wpia.uw.edu.pl/uploads/media/5d98c8180784e/autoreferat.pdf?v1> (accessed 1 September 2021)
- Piotrowski R., *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne*, (in:) Arwid Mednis (ed.), *Prywatność a jawność – Bilans 25 lecia i perspektywy na przyszłość*, Warszawa 2016, p. 19
- Rzucidło J., *Prawo do prywatności i ochrona danych osobowych*, https://repozytorium.uni.wroc.pl/Content/52920/PDF/09_Jakub_Rzucidlo.pdf (accessed 1 September 2021)
- Sarnecki P., *Komentarz do art. 47*, (in:) Garlicki L., Zubik M. (eds.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2006, Vol. II
- Sitek M., *Prawa (potrzeby człowieka) w ponowoczesności*, Warszawa 2016
- Taczowska-Olszewska J., *Autonomia informacyjna jednostki a zarządzanie cyfrową tożsamością. Granice autokreacji*, (in:) Chałubińska-Jentkiewicz K., Kakarenko K., Sobczak J. (eds.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017
- Szwejką Ł., *Rola monitoringu wizyjnego w prewencji kryminalnej*, “Społeczeństwo i Rodzina” 2016, nr 47 (2), https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/37900/szwejka_rola_monitoringu_wizyjnego_w_prewencji_kryminalnej_2016.pdf?isAllowed=y&sequence=136 (accessed 1 September 2021)
- Szwiercz J., Matczak P., Dąbrowski A., Wójtowicz A., *Monitoring wizyjny i jego wpływ na straty spowodowane przestępczością. Przykłady z wybranych polskich miast*, “Studia z Polityki Publicznej 2020, No. 7 (25)
- Uliasz J., *Konstytucyjna ochrona prywatności w świetle międzynarodowych standardów*, Rzeszów 2018
- Warren S.D., Brandeis L. D., *The Right to Privacy*, “Harvard Law Review” 1890, Vol. IV, No. 5, https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (accessed 1 September 2021)
- Wild M., *Komentarz do art. 47 Konstytucji RP*, (in:) Safjan M., Bosek L. (eds.), *Konstytucja RP*, Vol. I, Warszawa 2016
- Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008
- Wanat T., *Akceptowalność automatycznego rozpoznawania twarzy nabywców w handlu detalicznym*, “Handel Wewnętrzny” 2015, No. 3 (356), <https://www.telepolis.pl/tech/prawo-finanse-statystyki/komisja-europejska-zdalne-rozpoznawanie-twarzy-lamie-prawo> (accessed 1 September 2021)