Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 16–29.

The Right to Informational Self-Determination in the Context of Selected Judicial Decisions and Practical Background[1]

Andrea Erdősová*

* Andrea Erdősová, JUDr., PhD, Paneuropean University in Bratislava, Faculty of Law, Institute of International Law. (e-mail: andrea.erdosova@paneurouni.com)

Abstract: It is essential to address in particular the comprehensive prevention of breaches of the right to informational self-determination and whether the persons concerned are aware that they "voluntarily agree" to pass on their identity information to third parties. It is alarming nowadays what amount of private data are available at their disposal for companies or private persons regarding other persons and how easy it seems to obtain this data. In today's information age and the era of more advanced use of artificial intelligence, it will be more necessary than in the past to define what the individual intended, what he agreed with, and what he eventually approved as data privacy.

In order to ensure the protection of the individual and his/her privacy, it is therefore necessary to respond to and refine the existing sources of law, especially to establish codes of ethics taking into account the modern technological and social development.

Keywords: ethics; informational self-determination; the right to privacy; personality rights; European Court of Human Rights; findings of the Constitutional Court; case law

1. Introduction

Primarily, the right of the informational self-determination originates in guaranteeing the freedom and dignity of individuals in relation to public authorities. Today, state power is not the only threat to law. Nowadays it seems easy for different subjects to gather without a problem huge amounts of information about individuals, especially for those such as Google, Facebook, Instagram, or Twitter. It might not be satisfactory to just consider how to protect someone effectively from the power handled by public authorities.

In order to ensure the protection of the individual and his/her privacy, it was therefore necessary to respond to and refine the existing legislation in this area, in particular at the European Union law level.[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) is one of the "new" means of protecting the privacy of individuals.[3] In the context of the protection of informational self-determination, the whole regulation is an important instrument for the protection of the right to

privacy, in particular through the so-called *Right to erasure ('right to be forgotten')* in Article 17 of the Regulation, which consists in the rights of the data subject[4] to obtain the deletion of personal data relating to him from the controller[5] without undue delay. The controller is then obliged to delete such personal data without undue delay if one of the enumerated reasons is fulfilled, allowing the data subject to request the deletion of his personal data published on the Internet (with or without his knowledge).

To what extent it is an effective means in the current technological development and possibilities of data and information backup on other media, it seems more than questionable. Therefore, we perceive these means rather than the mechanisms of derangement of one's own information identity, where, particularly in disputes concerning the protection of personality, the court will thus be able to see by consenting, verifying and examining what the individual has agreed to interfere to his/her right to privacy. Last but not least, today, more than in the past, it is also necessary to set general ethical boundaries of permissible interference from the perspective of exploitation of the artificial intelligence.[6]

2. The Meaning of Informational Self-Determination

The term "right to informational self-determination" (informationelles Selbstbestimmungsrecht) originated in the Federal Republic of Germany and its author is the Federal Constitutional Court (Bundesverfassungsgericht), which derived this right from Article 2(1) 12 in conjunction with Article 1(2) of the Constitution of Germany.[7] The term "self-determination" generally means the right to autonomy and independence. The essence of the right to informational self-determination is therefore the right of every individual to control information from his/her privacy so that he/she decides what facts about his/her surroundings will get known, who has them and how they will be used.

The Constitutional Court of the Slovak Republic knows this term, although it is used only very sporadically, i.a. judgment of the Constitutional Court of the Slovak Republic of 29 April 2015, no. PL. ÚS 10/2014-78, where its paragraph 89 defines as follows:

"The case law of foreign constitutional courts also takes a similar approach to privacy. For example, the Federal Constitutional Court of Germany, through the right to informational self-determination guarantees protection not only of the content of the information to be moved, but also protects the external circumstances in which it is carried out; location, time, subscribers, type and mode of communication, because knowing the circumstances of the communication made, in conjunction with other data, may itself indicate the content of the communication itself, and by examining and analysing this data, individual subscriber profiles can be constructed out of the communication.

[e.g. Decision of 27.7.2005, BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung) or 27.2.2008, BVerfGE 120, 274 (Grundrecht auf Computerschutz)]."

The ruling in question was a proposal by a group of Members of the National Council stating that the contested provisions of the Electronic Communications Act impose an obligation on electronic communications providers to keep traffic data, location data and

data of communicating parties from the date of communication for 6 months in the case of Internet connection, e-mail and Internet telephony, and for 12 months for other types of communication.

In the view of the group of deputies, "the introduction of the obligation to retain data pursuant to the above provisions constitutes a noticeable interference with private life, as it is a blanket surveillance of all Slovak citizens, regardless of their integrity and honesty. Every day, every person in Slovakia is obliged to record who he was calling, who he sent text messages and emails, when he did, where he was, what phone or service he used, how long the communication in question took, and many others. By combining this information, we can describe the movement of every citizen in Slovakia who uses a mobile phone or the Internet, predicting their behavior, circle of acquaintances, hobbies, health, sexuality, or other personal data and secrets [...] it is possible to compile the perfect personality, communication and movement profile of an individual, revealing a number of essential characteristics of his identity and behavior, in other words, reveal a substantial part of his privacy."

In its proposal, the group of deputies also points out that "according to the case-law of the ECHR", interference with private life "e-mail and telephone calls (ECtHR judgment in Klaas v. Germany), as well as finding telephone numbers of telephone persons or storing information that the person was calling with a person, all of them have to be considered as keeping the control or check over the mail and its content. It is irrelevant whether the data retained has been used or disclosed in any way (in particular the ECtHR judgment in Copland v. The United Kingdom). Infringement of fundamental rights, and hence private life, means not only immediate intervention (e.g. familiarisation with stored data), but also measures taken by public authorities from which it is foreseeable that they will result in a restriction of fundamental rights and freedoms".

According to the proposers, the contested provisions of the Electronic Communications Act "are in direct contradiction with the principle that fundamental rights and freedoms must be respected in substance and meaning, and restrictions can only be applied to a stated objective (Article 13(4) of the Constitution)". They further state that "the merits of any interference with fundamental rights and freedoms in a democratic and legal state are assessed on the basis of the cumulative fulfilment of three basic criteria, namely the legality, legitimacy and proportionality of such interference (Constitutional Court Findings, file no. I. ÚS 117/07, PL. ÚS 23/06, PL. ÚS 3/09, PL. ÚS 3/00, PL. ÚS 67/07)".

In a part of this petition, the Constitutional Court of the Slovak Republic granted the proposal about the breach of law.

Also i.a. in the decision of the Constitutional Court of the Czech Republic under no. Pl. ÚS 24/10, in which the court assessed the constitutionality of § 97 par. 3 and 4 of Act no. 127/2005 Coll. on electronic communications regulating the obligation of legal or natural persons providing a public communications network or publicly available electronic communications service to store traffic or location data, this court adopted and used the term "informational self-determination" as a doctrine contained in the above-mentioned Federal Constitutional Court decision and informational self-determination as follows:

"The primary function of the right to respect for private life is to provide space for the development and self-realisation of an individual personality. In addition to the traditional definition of privacy in its spatial dimension (protection of the dwelling in the broader sense of the word) and in the context of autonomous existence and public power undisturbed in social relations (marriage, family, society), the right to respect for private life fundamental decision – decided freely by the individual. In other words, the right to privacy also guarantees the right of the individual to decide at his/her own discretion to what extent, in what manner and under what circumstances should the facts and information about his/her personal privacy be made available to other entities. This is an aspect of the right to privacy in the form of the right to informational self-determination; guaranteed by Article 10 paragraph 3 of the Charter."

Pars pro toto two findings of the two constitutional courts serve as an example of the use of a term which, despite its extraordinary timeliness and, so to speak, material significance in disputes concerning the protection of personality and privacy, has still not been frequently used as a terminus technicus. This is peculiar, pointing out that in today's information age and the era of more advanced use of artificial intelligence, it will be more necessary than in the past to define what the individual intended, what he agreed with, and what he eventually approved as data privacy. In our view, this is also a key aspect of shifting the burden of proof to the operators, or creators or sponsors of the algorithms involved in setting up and using a wealth of information and data from our privacy.

However, even the national doctrine of the general courts does not leave the right to informational self-determination unnoticed. According to the order of the Supreme Court of the Slovak Republic (Order of the Supreme Court of the Slovak Republic of 18 February 2010, ref. No. 3 Cdo 137/2008), the right to privacy lies in the right of a natural person to decide independently whether and to what extend should the facts from his private life be made available to others or made public. The violation of the right to privacy is not only the unauthorised acquisition of knowledge about the privacy of a natural person, but also the unauthorised dissemination of this knowledge. The unauthorised interference with the right to privacy may significantly reduce dignity or seriousness in society, but this is not the only right required to demonstrate the seriousness of the harm to a natural person. Consequently, there is no procedural obligation to prove to the injured party that the unlawful interference had the effect of reducing his seriousness and dignity in society.

3. Strasbourg Doctrine

Although the European Court of Human Rights also does not directly and expressis verbis address the issue of self-determination, the basis of its earlier case law can still be used to answer the question of which data, information an individual has authorised or where was his legitimate expectations about the use and spread of these information, to what extent, location, time and for which range of recipients.

Paradigmatic in this context is the case of Max Rufus Mosley, Mosley v. United Kingdom,[8] who is known to the public as ex-president of the International Automobile Federation (FIA).

Briefly, on March 30, 2008, Sunday's newspaper *News of the World* published an article on the front page entitled "F1 chief had perverted Nazi orgies with five prostitutes". Ex-president of the International Automobile Federation was exposed as a secret sadomasochistic sexual pervert. The published text continued by describing the event and adding a few photos taken from a video recorded by one of the sex orgy participants, and the recording was pre-ordered and paid for. In addition, the extract from the record as well as the relevant photographs were accessible on the newspaper's website, where potential candidates could further disseminate them.

In the proceedings against the publisher of the tabloid, the complainant did not in fact object that the sexual sadomasochistic act had not occurred as was clear from the recordings and the text, but openly admitted that he had been professing this kind of sexual practice for years, but denied background act simulation with Nazi content. He alleged that the media had unlawfully interfered with his privacy, on the grounds that his private life was his personal affair and that the newspaper publisher had no relevant evidence, except for the presence of uniforms, a strange German accent in his speech and connotations to his father's fascist past and the direct relation of sexual orgies to Nazi ideology.

He requested that the footage of the video be immediately downloaded from the newspaper website. The applicant was successful in the national proceedings for the protection of his personal rights and was awarded damages of GBP 60,000 and GBP 420,000 with respect to costs. Mosley argued that the State failed to fulfil its positive responsibilities and had ensured a general obligation for publishers or journalists to seek prior consent from the person concerned.

In so doing, the complainant demanded that the ECtHR determine that newspaper publishers be required to notify the person concerned of the planned media coverage three days before publishing information that infringes the privacy of persons. Thus, the ECtHR also assessed the practical impact of the complainant's claim and found that there was no general obligation to pre-notify as such in any of the Member States' legal systems. On the other hand, some Member States require the data subject's consent to the publication of material relating to family life,[9] although in many cases they provide for exceptions to the publication of information relating to "public interest" issues (paragraph 62).

In paragraph 128 of the ECtHR, referring to the national decision, it recalled that any prior consent would not have any effect other than a penalty for not respecting it. A regulatory or civil sanction in the form of a fine would probably be a small incentive to avoid publication without the prior consent of the person concerned. This is all the more necessary to prevent the prohibition of publishing the article in question in the press because the person concerned has not given his consent to its publication. Moreover, as the ECtHR pointed out, these obstacles can also lead to censorship. The threat of criminal sanctions or punitive penalties may have a freezing effect in the field of political reporting and investigative journalism concerning the highly protected values of the Convention.

Information and video footage of Max Mosley were seen by hundreds of recipients and they had the opportunity to spread them further. Therefore, the response to the request to download video footage and prevent access to information was as follows: "The court must always be cautious when considering the real facts and the limits of what can be achieved [...]. However, in order to limit access to information by court order, it must be

remembered that information is so widely and generally accessible on public domains that such a court command would have practically no meaning. In traditional terminology, such a measure would be labelled "brutum fulmen". It is not appropriate for the court to make only blank gestures (paragraphs 34–35)."

For these reasons, the Chamber decided that Article 8 of the Convention had not been infringed in that case. In addition, what can be seen as the scope of the legitimate requirement can be summarised from one of the three decisions in the case of Caroline von Hannover, in concreto Hannover v. Germany, no. 59320/00.[10]

It can be inferred from the judgment in question that, although there is a public demand – in the case of a commercial interest in magazines – for the publication of photographs and articles, in the present case, everyone, even if known to the public, must have a "legitimate expectation" of protecting and respecting their private lives.

The judgment of the ECtHR on the basis of a complaint from the Princess of Monaco, Caroline von Hannover, is not only pointedly defining the so-called personality protection of "relative" (quasi) public persons, but it is also a sort of navigation system in the endless sea of the details of the private life searched from the prominent people. It will serve the press in a number of cases to distinguish between legitimate and well-known processing and further dissemination of information and details from the privacy of "celebrities". As J. Herczeg pointed out: "[...] the readers of the boulevard will not lose their stories, as the media behavior of these persons will also be important for assessing whether or not the intervention is justified. But in other words, one's own behavior will set the limits of legal privacy."[11]

This also applies, mutatis mutandis, to cases of confidentiality of data from the private sphere of a natural person subject to professional secrecy. Legal theory has clarified that "[...] when a patient himself publishes in the press or other mass media his own health condition stating the facts subject to confidentiality by the doctor, or when the patient himself discloses certain facts subject to confidentiality, and so they will exclude them from their personal privacy".[12]

On the other hand, Reid's legal opinion commenting on the ECtHR's judicial practice in this context cannot be overlooked. In its view, the mere fact that an individual is in a public place or that his personal data is publicly accessible to others on public domains does not necessarily preclude the application of Article 8 of the Convention. Like the person's legitimate expectations regarding their protected sphere of privacy, although significant, they are not necessarily the only determining factor in assessing the legitimacy of an intervention.[13] This also applies, mutatis mutandis, to the voluntary disclosure of information or guarantees of its later use.[14]

4. Informational Self-Determination of Minors in the Context of One Case

The situation where there is currently an Internet connection in virtually every home, even in the streets of cities, is making it even more difficult by the lack of general legal knowledge of what data are collected in the Internet environment, how they are used and to

what extent they are kept. The issue is also addressed by relevant psychological concerns, according to which a group of minors approaching adulthood are not even partially aware of the importance of protecting their privacy and informational self-determination and the consequences of its ill-considered sharing with third parties in cyberspace.

In addition, it is very common to find that the parents of minors also violate their right to informational self-determination by sharing their photographs or by publishing them in public places. This question was also addressed by the Supreme Court of the Czech Republic in its order of 12 December 2012, file no. 30 Cdo 3770/2011, which unequivocally ruled that unauthorised interference with the right to informational self-determination of a child could also be carried out by a legal representative, stating: "Protection under Section 11 of the Civil Code also includes images of a minor of "celebrities" who capture his daily and private activities for which there is no public interest, even if his or her legal representative is motivated by an incentive to attract public attention to himself or herself. [...] The appellant's argument that the consent of the legal guardian to the public dissemination of photographs and articles on minors that capture and map the child's privacy precludes the unlawful interference must be rejected. Article 16 of the Convention on the Rights of the Child[15] affords the child protection against arbitrary interference with his or her privacy, without distinction from where they are carried out. In other words, a child has the right to protection from arbitrary interference with his/her privacy, even if carried out by legal representatives (holders of parental responsibility)."

The right to informational self-determination is also related to monitoring the behaviour of individuals, which is no longer a dystopia, but an increasingly current reality, where there are certain algorithms of systems, of which the most familiar is the so-called "cookies". Modern software, however, cannot only read the behaviour and decision-making processes of an individual, but also over time his or her consumer preferences, thoughts, and motivations, giving rise to very interesting and relevant information for data collection. Worse, however, is the risk of interference with the right to privacy, in particular the right to informational self-determination, where the individual does not even know not only what data are collected about him/her, but also where and for what purposes he or she continues to use it. Installations of industrial cameras may also be another way of disrupting the individual's self-determination.

5. Industrial Cameras in a Legislative and Practical Framework

The emergence and existence of the first industrial cameras is associated with monitoring missile test launches in Nazi Germany in 1942. By technical improvement, we now have not only a larger number of camera systems but also an increase in the number of objects monitored by them. These are, for example, security cameras, which follow us when shopping, in underground garages, cameras at the entrance to the pub together with appropriate software, which can identify among the visitors known so-called "troublemakers", furthermore, those that recognise vehicle licence plates, but also camera surveillance through other devices that we accept on a voluntary basis, but eventually become an

undesirable burden. These include laptops, phones, tablets, game consoles, the Internet, video servers and viral videos.

In the United States, there has recently been a debate on the introduction of cameras with face recognition software,[16] which is mainly used by police forces in several countries. Cops are allowed i.a. to take a picture of a person with a mobile phone and immediately identify their identity and eventual criminal record or other personal information from various accessible databases. A very turbulent case of the right to privacy is the so called "Street View", which under this technology was designed in 2007 to monitor populated parts of the world.

It was tracking in about 12 countries collecting emails, passwords, photos and other personal information.[17] Related to this was a system creating a mapping of an increasing number of states through the so-called google maps, which also retrieves images captured by people in public places which allows them to find themselves online. This way, it is also possible to take a look at dwellings and private spaces. This may potentially undermine the right to privacy and, in these circumstances, the unauthorised use of personal data. The biggest commotion was caused by the maps in Italy, where they captured a high-ranking politician coming out of a public house.[18]

In many of the disputes that Google has encountered in connection with this technology, it has been argued that WIFI communication channels have allowed this data to be retrieved, making it publicly available to society. Finally, even in disputes where Google lost, monetary sanctions were negligibly small compared to the company's regularly high profits. In the context of privacy invasions through surveillance, or rather espionage,[19] there has to be mentioned the media-narrated case of Snowden's testimony, according to which there is a secret PRISM anti-terrorism program that allegedly allows the U.S. National Security Agency and the Federal Bureau of Investigation to retrieve texts, photographs or video-mails, chats, social networking, and phone calls around the world.[20]

We have a number of cases of violations of the right to privacy through camera systems, both at home and close to the border. Not long ago, the media resonated the case of a journalist from the Czech Republic, who protected his property against vandals with his own CCTV system, but CCTV did not allow the perpetrators to be detained and accused as evidence in court and acquitted the perpetrators. The damaged journalist was eventually sanctioned by the Office for Personal Data Protection of the Czech Republic for unannounced installation of the camera and unauthorised collection of personal data. On the basis of an analogous case, the Supreme Administrative Court of the Czech Republic even referred a question to the Court of Justice of the European Union.[21]

6. Public Versus Private

Finally, the right to informational self-determination is also a question of what information should be and for what purpose part of the monitoring, even if a person has not directly elected it, but the interest in monitoring has exceeded private interests and is rather perceived in the public good.

In one such case, the Regional Court in Brno upheld the lawsuit against the decision to place the camera on the ground floor of an apartment building at the entrance so as to capture the persons entering and leaving the house, thereby identifying the property better and in the aim to prevent stealing mailboxes. The court has rightfully held that by placing the camera at the entrance to the house against the plaintiff's will, the defendants rightfully infringed his right to privacy as a personality right within the meaning of Section 11 of Act No. 40/1964 Coll. Civil Code, as amended, hereinafter referred to as OZčr, as well as unlawful interference with the applicant's right to protection against unauthorised acquisition and collection of pictorial records pursuant to § 12 para. 1 OZčr.[22]

Since no legal licence has been given for this intervention and the installation of a CCTV system requires the consent of all residents of the apartment building, the court pursuant to § 13 para. 1 OZčr prohibited the acquisition and collection of video recordings and ordered the defendants to dismantle it. However, in this and similar cases, the problem is mainly focused on obtaining monitoring consent, as other cases assess cases in which the subject feels affected by the monitoring and therefore disagrees with the capture of premises owned or exercised by other related rights.

Pursuant to the aforementioned legislation, it would be necessary not only to obtain the consent of all potentially affected persons before installing a CCTV system, but also to place a visible space monitoring sign. If all residents of the dwelling house were to agree in unison, then it would seem difficult to assert that the monitoring affected the rights of visitors or other persons who found themselves in the dwelling without having a legal relationship with it. Assuming, of course, that the monitoring of this space could have anticipated what was clearly indicated. This obligation also creates space for labelling without being linked to an active system, i.e. it is only an assembly of non-functioning dummy devices.

However, they logically do not establish any real violations of law and their importance lies in the territory of purely preventive security measures. If we rely on the case law of the European Court of Human Rights, we find a number of explanations for what is considered a home, even though the concept of home is generally autonomous and according to the text of the European Convention on Human Rights[23] it can only be defined with great difficulty. In principle, it is a space that is a physically defined area where private and family life develops. However impersonal we would consider prima facie, for example, a hotel room, in the case of a homeless person who was paid for accommodation by the local authorities, it became home during his stay.[24]

However, the Court is not concerned with extending the right to home through the right to acquire or own property, but to place protection in respect of home without being able to undermine the right to use it. In particular, the intervention of competent authorities by confiscation, control or secret surveillance is prevented.[25] In Friedl v. Austria case decision, the Commission considered essential that the taking of photographs and the subsequent recording in the investigation file infringed the right to privacy, irrespective of the interests of a private or public nature behind the pictures taken.[26]

The Court has stated on several occasions that the mere fact that an individual is in the public domain or that data about him is widely available on public domains does not

automatically exempt from the application of Article 8 of the Convention. The Court accepts that there are a number of factors which may be considered in assessing whether there has been an infringement of the right to privacy.

The individual's reasonable expectations of possible interference with his or her privacy are certainly essential facts, but not exclusive. The same applies to the information provided by the parties concerned (right to informational self-determination).[27] To the same extent, it applies to e-mails and the Internet used at the workplace which are part of private autonomy, provided that the employee has not been notified by the employer on the possible monitoring of its manifestations.[28]

Finally, persons who are being prosecuted must not be excluded from the protection of privacy.[29] It can therefore be settled in the ECtHR case law that insofar as the purpose of obtaining information is to protect the public interest, whether it is the right to public information or the protection of collective security. Interference with the right to respect for private life are going to be considered less strictly than searching for information and details from private life. For this reason, the control of the exercise of a public function, the task of which is, for example, to maintain security and order in public places, also implies an obligation to suffer the capture of video recordings from the intervention.[30]

At the same time, it is clear from that judgment that the powers of public officials, in particular exercised in public and in contact with the public, may, and should be, directly subject to a control regime, which is an exercise of the right to information. Naturally, questions falling within the scope of the fundamental right to privacy of a natural person are not subject to such a legal regime. It is also necessary to carefully differentiate whether the attacks carried out in the sphere of personality rights were really directed against individuals or against the state authority of which they are representative.

"Given the above-mentioned differences between the State authority and the natural persons of which it is composed, it can be concluded that if an intervention is directed against a particular authority of the State, it cannot be inferred from this that such interference affects the personality rights of the natural persons of which a government body is composed, which does not mean that the authority concerned is also hit by this interference."[31]

The need for obtaining and storing information is generally not disputed as long as it is carried out under the auspices of a police investigation or security guarantee and is clearly based on legitimate objectives and is indispensable in a democratic society.[32] In addition, the necessity and procedural guarantees enjoy a wide margin of appreciation in national security measures.[33]

The question of the violation of the right to privacy in such cases has been answered in the earlier case-decision of the Commission, which in Hilton v. United Kingdom[34] has confirmed that security control per se does not affect private life, except for information pertaining to private life, which is subject to control.

It was a strictly individualised demonstration of the interference that caused direct interference with the right to privacy. However, the case law has evolved to more general assumptions, and thus, through a permanent court in particular, has established that the principle of "reasonable probability" will always be decisive in establishing whether

an individual is a subject of observation (reasonable likelihood). Indeed, it indicates that such measures are applicable to the person concerned or those that belong to the category of persons likely to be monitored. If he/she finds himself/herself in this category, then there is no longer any need to prove whether or not surveillance has or could affect private-sector attributes.[35]

In addition, the Court has established that public information falls within the scope of private life when it is systematically collected and stored in the files of the competent authorities, particularly where it relates to the distant past or is false or capable of significantly undermining a person's good repute.[36]

The perception of the existence of a specific subject is also significantly influenced by the nature of the activity per se, as was the case, for example, with Vanessa Redgrave,[37] who found a wiretapping device which, in her view, was placed by the Government. The suspicion was supported by the fact that the applicant was known both from controversial political cases and by belonging to the revolutionary party, and there existed an interest in tracking her in the past.

Another important criterion taken into account by the Court is the legality of the intervention. In this sense, judicial criteria are based on legality which refer to the presence and content of national legislation available and guarantee that the measures in question are reasonably foreseeable and protected against arbitration.[38] According to doctrine, the question of predictability is meant in terms of general guarantees of predictability of law, but this does not automatically represents that an individual will know in advance i.a. control procedures of special forces, as this could be the threat to the controls relating to national security interests. However, it must be pre-defined, what categories of people will be monitored, within what time limit, by what procedural mechanisms, how data will be further used, how they will be protected when communicating them to third parties, and the conditions under which records can or must be destroyed.[39]

The ECtHR case law focuses in particular on examining the adequacy and effectiveness of safeguards against misuse of information. On the other hand, it is not excluded that the alert in some form will persist later, sometimes despite or without the adoption of rules on the obligation to destroy it. This raises the association to the aforementioned Max Mosley case where the Court was i.a. forced to state that even downloading video footage and preventing official later distribution after the recording appeared on public domains does not prevent its misuse. Despite all this, forcing publishers, journalists to ask for prior approval of the publication leads to nothing and it solely can present nothing or means only an empty gesture.[40]

7. Conclusion

A few of these cases map out circumstances of the use of the institute of the right to informational self-determination, and although we see that it appears sporadically in both national and European Court of Human Rights rulings, we consider this could be one of the criteria for assessing both the rate of participation of a person affected by the rights of personality and the subsequent determination of the amount of non-material harm.

As can be seen from the text followed, informational self-determination is not always a question of delimiting the private sphere, and the autonomy of the individual in this context may be outweighed by the public interest, fulfilling the purpose of the public good, i.a. trying to maintain security, or preventing unrest, or a certain preventive-deterrent effect while maintaining public order.

References

1 This contribution is the result of the project implementation grant by the APVV No. 16-0588.
2 See more i.a. Elena Júdová, Ochrana slabšej strany – porovnanie európskeho a slovenského medzinárodného práva súkromného [Protection of the Weaker Party – Comparison between European and Slovak Private International Law], 17–31, in *Acta Iuridica Olomucensia,* vol. 9, no. 1 (2014).
3 Lilla Garayová, Regulácia voľného pohybu osôb v kontexte protiteroristických opatrení v EÚ [The Regulation of the Free Movement of Persons in the Context of Counter-terrorism Measures], 80–86, *Paneurópske právnické listy,* no. 1 (2018).
4 The expression "data subject" according to Article 4(1) of the regulation states that "personal data" means any information relating to an identified or identifiable natural person ("data subject"), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
5 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
6 See the document drafted by a panel of experts at the request of the European Commission (DG Research and Innovation) which aims at raising awareness in the scientific community, and in particular with beneficiaries of EU research and innovation projects. It does not constitute official EU guidance; the document was adopted on November 14, 2018, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf (accessed 8 August 2019).
7 Ruling of the German Constitutional Court defining informational self-determination, http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintText&Name=bv065001 (accessed 8 August 2019).
8 Mosley v. United Kingdom, judgment of 10 May 2011, no. 48009/08, Complaints valid September 15, 2011.
9 Lilla Garayová, Odhad vplyvu Brexitu na voľný pohyb osôb [The Estimated Impact of Brexit on the Free Movement of Persons and Data], 51–62, in *Voľný pohyb osôb a vnútorný trh Európskej únie: vedecký zborník* (Bratislava, Paneurópska vysoká škola, 2018).
10 Hannover v. Germany, judgment of 24 June, 2004, no. 59320/00.
11 Jiří Herczeg, Případ Caroline von Hannover – zveřejnění fotografií ze soukromí prominentů, 877–880, in *Právní rozhledy,* no. 23 (2004).
12 Karel Knap et al., *Ochrana osobnosti podle občanského práva,* 4th substantially revised and supplemented edition, 24 (Linde Praha, 2004).
13 To this we associate, mutatis mutandis, the case of Friedl v. Austria, judgment of 31 January 1995, no. 15225/89, in which the Court did not find a violation of Article 8 of the Convention, even though the police photographed the complainant, but during a public demonstration and they remained anonymous without mentioning the name of the photographers.
14 Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights,* 3rd edition, 483 (London, Sweet & Maxwell Ltd., 2008).
15 *Convention on the Rights of the Child,* adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49, www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed 8 August 2019).
16 *Technológia rozpoznania tváre a GDPR,* 9 March 2011, https://blog.canex.sk/2019/12/19/technologia-rozpoznavania-tvare-a-gdpr/ (accessed 8 August 2019).
17 Judgment of the Federal Supreme Court on Google Street View: Decisions on the processing of personal data, published August 2013, www.edoeb.admin.ch/datenschutz/00683/00690/00694/01109/index.html?lang=en; compare with David Streitfeld, Court Says Privacy Case Can Proceed Vs. Google, 11 September 2013, www.nytimes.com/2013/09/11/technology/court-says-privacy-case-can-proceed-vs-google.html (accessed 8 August 2019).

18 *Pohlad do zákulisia Google StreetView,* 1 November 2012, www.wesolyaniolek.com/pohlad-do-zakulisia-google-streetview/ (accessed 8 August 2019).
19 Lilla Garayová, *Spoločnosť proti terorizmu?* [Torture as a Just Means of Preventing Terrorism?] 360–364 (Plzeň, Aleš Čeněk, 2016).
20 *Super veľký brat? Fakty a mýty o tajnom programe PRISM,* 11 June 2013, https://zpravy.aktualne.cz/zahranici/supervelky-bratr-fakta-a-myty-o-tajnem-programu-prism/r~i:article:782171/ (accessed 8 August 2019).
21 *Nejvyšší správní soud: Nejvyšší správní soud položil předběžnou otázku Soudnímu dvoru Evropské unie* [The Supreme Administrative Court referred the question to the Court of Justice of the European Union for a preliminary ruling], 22 April 2013, www.nssoud.cz/Nejvyssi-spravni-soud-polozil-predbeznou-otazku-Soudnimu-dvoru-Evropskeunie/art/956 (accessed 8 August 2019).
22 See also *Ako GDPR nahliada na používanie kamerových systémov* [How GDPR views the use of camera systems], www.isecure.sk/sk/aktuality/monitorovanie-kamerovym-systemom-z-pohladu-gdpr.html (accessed 22 August 2019).
23 Convention for the Protection of Human Rights and Fundamental Freedoms, podpísaný 4. novembra 1950 v Ríme, hereinafter referred to as "Convention", O'Rourke v. United Kingdom, decision about admissibility 2001, no. 39022/97; see also David John Harris, Michael O'Boyle, Edward Bates, Carla Buckley, *Law of the European Convention on Human Rights,* 2nd edition, 380 (Oxford, Oxford University Press, 2009); Friedl v. Austria, 1995, no. 15225/89, compare with X. v. U.K., 9702/82 or Murray v. U.K., par. 84, 85, concerning data collection, fingerprints and photos by the police, also Chave née Jullien v. France, no. 14461/88, for obtaining and storing medical records or DNAs and Marper v. U.K., 2008, no. 30562/04 and 30566/04; Lupker v. Netherlands, 1992, no. 18385/91; Copland v. U.K., 2007, no. 62617/00, par. 42; Sciacca v. Italy, 2005, no. 50774/99, par. 29.
24 O'Rourke v. U.K., decision on admissibility by 2001, no. 39022/97.
25 David John Harris, Michael O'Boyle, Edward Bates, Carla Buckley, *Law of the European Convention on Human Rights,* 2nd edition, 380 (Oxford, Oxford University Press, 2009).
26 Compare with case X. v. U.K., 9702/82 or Murray v. U.K., par. 84, 85.
27 Lupker v. Netherland, by 7 December 1992, no. 18385/91.
28 Copland v. U.K., by 3 April 2007, no. 62617/00, par. 42.
29 Sciacca v. Italy, by 11 November 2005, no. 50774/99, par. 29.
30 See also the judgment of the Constitutional Court of the Slovak Republic of 5 January 2001, rec. II ÚS 44 / 00-133: "According to the legal opinion of the Constitutional Court, the exercise of his/her statutory duty of service by a public official – an employee of the municipal police – cannot be considered a part of the fundamental right to privacy or a manifestation of personal nature (pursuant to § 11 of the Civil Code) [...] these are diametrically opposed issues of the public and not the private sphere, which cannot in any way be considered a part of their fundamental right to privacy."
31 Judgment of the Supreme Court of the Slovak Republic of 27 March 2001, rec. no. M Cdo 46/2000.
32 Leander v. Sweden, of 26 March 1987, no. 9248/81, par. 49.
33 Ibid. par. 59.
34 Hilton v. U.K., of 6 July 1988, no. 12015/86.
35 Compare with Halford v. U.K. of 25 June 1997, no. 20605/92.
36 Rotaru v. Romania, 4.5.2000, č. sť. 28341/95 ods. 43–44.
37 Redgrave v. U.K., of 1 September 1993, no. 20271/92.
38 Lilla Garayová, Sources of EU Law, 59–62, in Andrea Erdősová, Lilla Garayová, Peter Potásch (eds.), *Selected Sources of Law – Past and Current Perspectives* (Bratislava, Paneurópska vysoká škola, 2019).
39 Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights,* 3rd edition, 563 (London, Sweet & Maxwell Ltd., 2008).
40 Mosley v. U.K., of 10 May 2011, no. 48009/08, par. 34–35.