

OPTIONS FOR MONITORING OF SPACES PUBLICLY INACCESSIBLE IN THE CONTEXT OF PROTECTION OF PERSONAL DATA AND PERSONAL RIGHTS²⁴

PaedDr. Zuzana Kurucová, PhD.

Institute of Theory and History of State and Social-Science disciplines, Faculty of Law PEU

doc. JUDr. Marcela Tittlová, PhD.

Institute of Public law, Faculty Law PEU

ABSTRACT

The submitted article devotes to the protection of personal data, the protection of personal rights in connection to the use of monitoring devices – camera systems. It analyses legal regulation valid and effective up to 25.5.2018, namely the selected parts, which are assessed in view of suitability and sufficient protection of personal data of data subjects. Several of its parts are subject to scrutiny. Subsequently, the attention is given to the legal regulation effective from 25.5.2018, which is a response to the adoption of a Regulation of the European Parliament and of the Council 2016/679 of 27 April 2016 on protection of personal data of natural persons. Even though the original regulation is subjected to a relatively strong criticism, this new regulation does not contain even those guarantees, which are contained by the still effective act. Within this context, the conclusion contains the formulated specific recommendations and proposals to a significantly more effective protection of personal data of data subjects with regard to the used monitoring devices – camera systems.

KEYWORDS

monitoring devices, options for monitoring of publicly inaccessible spaces, options of using the information obtained.

JEL CLASSIFICATION

K10, K20, K30.

INTRODUCTION

Under the Article 1 of the Slovak Constitution, the Slovak Republic has the nature of a separate, legal, sovereign, democratic state. This framework, but also other provisions allow to deduce that it is a state that honours fundamental human rights and freedoms of citizens and human beings (regardless of their nationality), as required from such states by many European and international documents. In the end, their content is reflected in many provisions in the Slovak legal order, from

²⁴ This study was supported by the Agency for promotion of research and development on the basis of the Contract No. APVV-16-0521

the Constitution up to the specific legislation. This is the reflection of co-existence and belonging of Slovakia to transnational grouping, but also to many international ones and at the same time the obligation to incorporate some of the adopted acts in full or in terms of achieving the purpose, which is thereby pursued.

A particularly sensitive issue arising not only in the national context, but also in the European context is the protection of privacy. This is understood very widely in terms of partial authorizations, which are subsumed thereunder.²⁵ Besides the protection of family life, secrecy of communicated, sent messages, it is also protection of personality and protection of personal data, which are subsumed under the protection of privacy.²⁶ It is important to understand the provision in Article 8 of the European Convention for the protection of human rights and fundamental freedoms within this context, i.e. that everyone has the right to have his/her private and family life respected, to respect his/her home, his/her correspondence, but these rights are not absolute. It is possible to interfere with the rights under conditions set out in Article 8(2) of this document. The key condition is the legality of this interference, i.e. is that the interference with the right to privacy is in accordance with law and for the purposes that are directly defined. This requirement of legal interference with the right to privacy and at the same time reasons for which this is possible are also reflected in the Constitution of the SR. Equally, if personality rights are concerned, their interference and limitation is only possible under the Article 13 of Constitution if the law so provides (permits under certain conditions). In connection therewith, the provisions of Civil Code in §12 specify that the documents of personal nature, video images, video and audio recordings relating to a natural person or expressions of personal nature can be created and subsequently used only with his/her consent. Exception to this rule is the existence of the so-called legal, statutory licenses, which shall be governed by the provisions of the Civil Code. Use of these statements and recordings without the consent of the data subject (their creation and use) shall be possible for specific purposes within their meaning.

Protection of personal data is a very delicate issue. It is a very personal question. Information related to a person, its specific knowledge that characterize this person have become a very sensitive, carefully followed and regulated issue over the last years. As a component part of the right to protection of privacy, it is important to define the concept of “personal data” itself and what has such a nature. The rules and obligations of how to handle them unwind from this subsequently. Whereas these data about the various aspects and parts of life of people, are of fundamental importance, they are carefully protected and obligations, under which the data may be obtained, handled, treated, stored and in the end also used, are consistently regulated

Camera systems, or systems to monitor persons in various situations and for different purposes, have become very important in the last years and will progressively become a more and more expanding means of protection and prevention. This is both a tool that is being used as a means of preventing criminal behaviour, crime, but at the same time it is a tool that allows some control (e.g. for business entities) of how certain activities are carried out, whether they are taking place in accordance with the internal rules and legal standards (e.g. banks monitoring specific banking activities and their course). They are also a means representing certain degree of protection of rights for natural persons as non-business entities, as well as for the business subjects (natural persons and legal persons). Gradually they have therefore become more and more expanded means whether in the publicly accessible spaces, but also in a publicly inaccessible, i.e. non-public spaces. It is only natural that their use brings about interference with the right to privacy and also the conflict with a lot of data having personal nature about each individual (personal data). On the one hand, we are

²⁵ Tittlová, M.: Zákon o ochrane súkromia pred odpočúvaním. Comment. Bratislava: Wolters Kluwer, 2017, p. 31 et seq.

²⁶ Ivor, J.: Monitorovanie obydliá kamerovým systémom a jeho využitie na účely trestného konania. In Zborník príspevkov z medzinárodnej vedeckej konferencie „Teoretické a praktické problémy využívania informačno-technických prostriedkov, FP PEVŠ, Bratislava, 2017, p. 83 - 84 et seq.

focusing on the possibility of personal data protection in the submitted article, and the possibilities for their use from the point of view of camera systems according to the still effective regulation and legal regulation effective from 25.5.2018 on the other. We have analysed and assessed, compared these regulations and have formulated concrete conclusions and recommendations in the end of this scientific work.

1. LEGAL REGULATION EFFECTIVE UP TO 25.5.2018

On 30 May 2014, the full wording of the Act No. 122/2013 Coll. on protection of personal data was published in the Collection of Acts of the Slovak Republic as an official publishing medium. This complete wording was published under the No. 136/2014 Coll. and it summarised several amendments of the original act into one newly designated regulation (indicated with a new number, but the original name). These are legal regulations establishing principles and rules on protection of personal data also in the context of options to use the camera recordings as monitoring means. It is a legal regulation which was effective until 25.5.2018. Already before this date a new act on protection of personal data, the Act No. 18/2018 Coll., has been adopted. The original above-mentioned regulation (its full wording) still remained in force and effect until it took effect, i.e. until 25 May 2018, and for this reason we are devoting to the options in this respect.

Directly the subject-matter of the Act notes (§ 1) that the provisions of this Act regulate the protection of rights, which is provided to natural persons against unauthorised interference with private life of such persons, including processing of their personal data. They are laying down a series of rights and obligations including liability, which shall be determined when processing personal data of natural persons. It is decisive what is considered to be personal data. Provision of § 4(1) specifies that the personal data shall be considered *the data concerning the identified or identifiable natural person, where such a person is the one who can be identified either directly or indirectly, in particular on the basis of a generally applicable identifier or on the basis of one or more characteristics or characters that form the physical, physiological, psychological, mental, economic, cultural or social identity.*

The use of camera systems, their legality, and indeed the legitimacy of use, is a very sensitive subject also in the context of this Act. It is precisely because of requirements for the protection of personal data under this Act. This is not the only act that introduces such requirements. It is necessary to take into account the directive of the European Parliament and of the Council 95/46/EC on the protection of personal data, which is incorporated in our legal order, i.e. our legal regulation is in compliance therewith. Here it is necessary to outline the provision of § 15 (7) of the Act, which provides for monitoring possibilities of public or larger space, which is accessible to the public. This provision regulates the conditions under which it is possible to monitor publicly accessible spaces with camera systems and the conditions under which this monitoring is possible. The legislator sets out a number of requirements that must be met in order to use the monitoring devices (camera systems), namely the condition that:²⁷

- a.) the space is publicly accessible,
- b.) the space can only be monitored to achieve the defined purpose,
- c.) this space is clearly marked as space that is monitored.

These conditions shall be considered cumulative, i.e. all of them must be met simultaneously in order to interfere with the right to privacy by the use of the monitoring devices and at the same time to record the personal data of persons. The legislator makes the legality of intervention and recording of personal data with these means subject to these conditions. *A contrario*, if one of the following conditions is not met, then it is an illegal intervention in the right to privacy and illegal

²⁷ Tittlová, M.: Korupcia (vybrané kriminologické a trestnoprávne aspekty). Bratislava: Wolters Kluwer, 2015, p. 146 et seq.

recording, collection of personal data. The legislator links the conditions for the use of such resources and possible collection and subsequent processing of personal data to conditions that are clearly formulated and at the same time, many of their aspects are also legally defined for its purposes.

To point a.) The legislator requires that spaces and plots of land to be monitored in this way must be accessible to public. Their use in the private spaces without access of a wide and in advance unidentified group of individuals is therefore excluded. As a rule, these are parks, means of transport (their interior is monitored), business premises of banks, for example. The provision of § 4 (3)(j) defines which premises are considered to be publicly accessible and legal under this Act and for its purposes. Spaces accessible to public are those, which *can be freely entered and where one can freely stay without a time limit or in the specified time, where other restrictions, if any, are met by the person and do not affect the entry and free movement in the space, or it is a space defined by a special act.*

To point b.) Monitoring is not for its own sake, i.e. its purpose is precisely defined in the present provision. Therefore, if a particular entity, e.g. a business entity wishes to monitor certain space which is public, the reasons for this activity must be subsumed under those defined in this provision. In particular, premises publicly accessible can be monitored on condition that this is done for the following purposes (alternative reasons):

- Protection of public order and safety,
- Detection of criminality,
- Breaches of state security,
- Protection of property or health.

To point c.) Publicly accessible spaces can be monitored (for the above stated purposes) to reach the above mentioned objectives only on condition that they are clearly marked. The space itself must be clearly sufficiently visibly marked as a monitored space usually at the entrance, but also inside the space itself. It is important that the legislator expresses the condition for visible marking of the space. Required marking must be sufficiently visible, and it must clearly and unambiguously state that the space is being monitored. As a general rule, it is at the entrance to the space, whether in the form of a verbal inscription in the official language, or a camera pictogram on a plate. It is important, and for this reason, if any person does not understand the official languages he/she has the option to figure it out from the camera pictogram and to find out that the space is monitored. The legislature does not impose any requirements as regards the size or method of notification. It only states that the space has to be marked clearly. Specific subjects using these means therefore have the option to choose a specific way of notification via clear marking. As a general rule, this is done by using a verbal inscription and the above shown camera pictogram on a plate at the entrance to the spaces which are subject to this monitoring. Consequently, it is considered that the persons who are thus notified, enter the spaces with the knowledge that their personal data are collected and may be processed for legal purposes. It is assumed that if they do not agree with this intervention in their guaranteed rights, they will not enter the spaces and plots of land, or that they leave them.

The operation of camera systems naturally means that the personal data of persons will be processed by means of monitoring devices.²⁸ Most commonly people's faces, figures, several expressions of personalities are recorded.

The legislator further states that such recordings, which were recorded after meeting the conditions stated above, although they are interference with the right to privacy, they record personal data of

²⁸ Ivor, J.: Monitorovanie obydľia kamerovým systémom a jeho využitie na účely trestného konania. In Zborník príspevkov z medzinárodnej vedeckej konferencie „Teoretické a praktické problémy využívania informačno-technických prostriedkov, FP PEVŠ, Bratislava, 2017, s. 84 - 85

subjects and this of various nature, even without their express consent, are useful for the purposes of criminal and administrative procedures. If these monitoring conditions are met, individuals cannot claim protection of their rights (personalities, personal data) against their recording, storage and use, as these are legal interventions.

The present regulation, nor the previous directly included the term “monitoring”. The partial lack of this regulation has been replaced by legal theory. Monitoring shall be considered to be a way of tracking, namely tracking by monitoring device, i.e. the camera, resulting in creation of a video.

In the event that no facts are discovered, for which the recorded data could be used, the legislator sets out the requirement in the § 17(7) that after 15 days of storage these obtained recordings shall be destroyed. Their use is possible in the process of inferring legal accountability, therefore their usefulness is bound solely to the use of evidence in administrative or criminal proceedings. If these cannot be used, the legislator lays down an obligation to the operator to destroy them within 15 days of obtaining them.

As it turned out also in our state, the use of camera systems is widespread. And it is not only our case, but also abroad. This is both the result of options provided by the camera systems (their use can gain very valuable knowledge about activities of persons and also identify them), but also of a strong information progress and development of monitoring devices. The fact is that this amendment includes the options for monitoring of public areas after meeting the legal conditions. As directly stated in § 2(3), the amendment of this act does not apply to personal data, which are:

- a.) processed by a natural person for their own use within the scope of exclusively personal or home activities, in particular keeping of personal directory or correspondence,
- b.) have been obtained randomly without prior determination of purpose and means of processing, without the intention of being further processed in a consolidated system under specific criteria and are not further systematically processed.

Questionable, therefore, are the options of use of the recordings that have been acquired by private individuals in non-public spaces. These are relatively simple cases that are currently strongly expanded – monitoring of homes as the private space (house, flat). One can see that the legal regulation does not apply to them, but there is no other legal regulation, which would deal with these cases. Thus it comes to an intensive interference with the right to privacy, personal rights; and the use of monitoring devices naturally results in recording of personal data. The nature of those systems and their use is the same as in the public spaces – interference with the right to privacy, recording of personal data. The only difference is that these spaces are not publicly accessible, but private. The Civil Code requires consent of the data subject with making of recordings and portraits and their use, and so this regulation cannot be applied here either.

With regard to the use of monitoring devices and collection of personal data in the publicly inaccessible spaces, it is important to define these private premises – the *homes*. Yet it is a term that is subject to protection and guarantees as from the national, but also from the international and European point of view. For example, Article 8 of the Convention contains guarantees of protection of private and family life, home and correspondence. In connection with these guarantees, the Article 21(1) of the Slovak Constitution also contains formulation that the home is inviolable. Without the consent of the person living in it, it is not possible to enter it. An interesting definition is also offered by the Criminal Code, which stipulates in §122(5) that for law enforcement purposes

home means a house, apartment or any other space that is used for housing, including those premises and plots of land belonging thereto, if they are closed as part of the home.²⁹

Certain rules for monitoring private spaces were found in the Methodological guidance of the Office for the protection of personal data No. 5/2016 called the “Monitoring of publicly inaccessible spaces”. The above guideline comes from the year 2016 and one can see that the solution to this problem was missing for a relatively long time. It is still questionable, whether the form of methodological guidance is suitable for these purposes. This guideline states that monitoring of publicly inaccessible spaces, private premises and property (home) is not the case of monitoring private property and spaces, which are used for business purposes. These are, as a general rule, spaces delimited with fence, green, fencing and so on. If such a space is to be monitored, it is necessary to take the nature of the monitored spaces and their extent into account. It is possible to distinguish between several cases when only non-public spaces are monitored (only the space of a house or flat), or when the private space (courtyard, house), as well as part of public space (pavement, part of road, etc.) is monitored. If exclusively private space is monitored, the Office for the protection of personal data proceeds in accordance with § 3(2)(a) of the Act on the protection of personal data – i.e. the activities to which the provisions of this Act do not apply. In view of this, the person carrying out monitoring has no notification obligation against the Office. On the other hand, if a private home is monitored, it is a private-law relationship being subject to private regulation – persons making these recordings must respect the rules on the protection of personal rights under § 12(1) and (2) of the Civil Code (requiring the consent of the data subject with its making and use)³⁰. It is only natural that if a private space is monitored, so only that person can monitor the space who has sufficient legal relationship thereto. One cannot monitor the other person's homes, adjacent parcels and so on. If this happened and such recordings would be published, e.g. on the Internet, on social networks and etc., persons recorded therein can demand protection of personality within the meaning of this civil regulation. In the case where exclusively own space is monitored, or a space to which the recorder has certain rights, the unauthorised intrusion – breaking-in by a certain person constitutes an offence. Such a record is usable as evidence in criminal proceedings (and also in administrative procedures), under § 10(3)(c) of the currently applicable Act on the protection of personal data. This provision makes it possible to process personal data without consent of the data subject, if this is necessary to protect life, health or property of the data subject. The letter g) is also applicable. It states that personal data can be processed without the consent of the person, if this is *necessary for the protection of the rights and the interests of an operator or a third party protected by law, in particular personal data processed in the framework of assets, financial or other interests of the operator and personal data processed for the purpose of securing the safety of the operator by cameras or similar systems; this shall not apply where such processing of personal data is outweighed by the fundamental rights and freedoms of data subjects, which are subject to protection under the Act*. There is however a certain conflict between the interests protected by law – protection of personal data and personality of potential offender and the interests of persons in the home which was intruded illegally. We can only agree that the rights of individuals end where the rights of other persons begin³¹ and the protection of their rights (personal data and personality) cannot be invoked by someone who has infringed the rights of other persons. In this case, the person who has intruded the home of another person without authorisation cannot invoke its protection, as the person violated the right of another person. It is necessary to actively speak out for the protection of the rights of this person (whose home was intruded without authorisation) and to sacrifice the personal rights and recording and using the recordings with its personal data without its consent in favour of its protection. Such recordings can be used in criminal proceedings as evidence, although this is not explicitly

²⁹ Čentés, J. a kol.: Criminal Code. Large comment. IIIrd updated release. Bratislava: EUROKÓDEX, 2016, p. 412 et seq.

³⁰ Lazar J. et al.: Substantive civil law 1st and 2nd volume. Bratislava: IURIS LIBRI, 2014. p. 93 et seq.

³¹ Jtk 10/2012

mentioned by law.³² Spaces publicly available can be monitored after meeting the legal conditions, and therefore recordings containing personal data of the data subjects can be obtained (recorded), kept and used, and such recordings can be used as evidence in criminal and administrative proceedings; in case of recordings from the monitoring of non-public spaces there is nothing stated about such usability.

From the above context it is clear that monitoring of public and private spaces and processing of personal data in this way, and the use of such recordings is not quite appropriately and sufficiently addressed in the Act. While monitoring of public spaces is addressed by the legislator at the level of the Act, cases of private spaces monitoring are not mentioned at all together with recording or overlapping with public spaces (pavements, parts of road, etc.). The monitoring with camera systems in vehicles is also not addressed legally. The Office for the protection of personal data is trying to deal with these issues by methodological guidelines, but important issues should be addressed directly in the act and significantly more comprehensively and in more details.

2. LEGAL REGULATION EFFECTIVE FROM 25.5.2018

New legislation on the protection of personal data took effect on 25.5.2018, in particular the Act No. 18/2018 Coll. on the protection of personal data and on amendments to certain acts (the new act). Its existence in our legal order is the expression or result of the fact that the European Union has adopted the Regulation of the European Parliament and of the Council 2016/679 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, repealing the Directive 95/46EC (on the protection of personal data). In view of the nature of the regulation, as the act of secondary law, this is directly effective and applicable in the territories of all Member States.³³ There was no need to adopt this regulation by a separate act. With regard to the existence of legal provisions in our state, the legislator has decided not to repeal them, but to transpose the text of the regulation into national law in the form of legal wording – a new act on the protection of personal data.

Right in the introduction of this part it should be said that the legislator often literally transposes European acts in our country and this without any more concrete and a more detailed consideration. In the case of directives it is not an appropriate procedure, in the case of regulation it is in principle the only appropriate procedure. It has to be noted that this legal regulation differs in many ways from the original. It differs more substantially also in matters of use of monitoring devices in relation to public spaces. While the previous legal regulation was evaluated as insufficient in matters of this monitoring and processing of personal data in the context of their use in many ways, this new legal regulation is even briefer and does not explicitly outline neither the above indicated monitoring of public spaces. Assessment of cases where the monitoring is used and personal data are processed by monitoring devices in private (non-public) premises, if they take up public spaces (pavements, parts of road), is not at all resolved; it does not address the use of vehicle cameras and recording of data by their use (on the road, pavement – what type of space it is actually? – public, private?), and the like. Since this is a reflection of regulation, this provision copies the text as it was adopted by the European Parliament and the Council. Previous European regulation was adopted by way of a directive, so it allowed the Member States to take various means to achieve the objective of the protection of personal data. In relation to the protection of personal data as from 25.5.2018 and in fact already now a range of issues remained unsolved. These are covered partly by the Methodological guidance, but we have already indicated that this is not the entirely suitable form of

³² Ivor, J.: Monitorovanie obydľia kamerovým systémom a jeho využitie na účely trestného konania. In Zborník príspevkov z medzinárodnej vedeckej konferencie „Teoretické a praktické problémy využívania informačno-technických prostriedkov, FP PEVŠ, Bratislava, 2017, p. 85 - 86

³³ Siman, M., Slašťan, M.: Primárne právo EÚ. Bratislava: EUROKÓDEX, 2012, p. 43 et seq.

regulation of such important issues. Clearly there is a space for further legislative action of the legislator and resolution of these fundamental issues in terms of both protection of the rights of data subjects, operators of camera systems (in houses, flats, family houses, if they record a part of public spaces, in vehicles in the form of vehicle cameras), as well as from the point of view of personal data protection, protection of the personality of individuals.

One can only outline that the new regulation also defines the essential points of personal data protection. Thus under § 2 of the new act, personal data are the *data relating to an identified natural person or identifiable natural person, which can be identified either directly or indirectly, in particular on the basis of generally applicable identifier, other identifier, such as the first name, surname, and the identification number, location data, or on-line ID, or on the basis of one or more characteristics or characters that form his/her physical identity, physiological identity, genetic identity, psychological identity, mental identity, economic identity, cultural identity or social identity.*

Also here (§ 3(5) of the new act) it is stated that its provisions shall not apply to the processing of personal data by means of natural persons in their personal activities, home activities. It does not define in any way what is a personal activity or home activity of a natural person, and so it is slightly polemical, whether it includes, for example, the use of motor vehicles and the camera systems built-in in the vehicles.

The only thing that the new act requires in relation to processing of personal data is that it can be processed only in legal manner so as not to violate the fundamental rights of data subjects (§ 6 of the new act). In addition to the requirement of legality, there are no other requirements defined, for example, recording and processing of personal data by monitoring devices in public spaces, contained in the previous. The legislator formulates principles of use in the new regulation, e.g. the principle of purpose limitation for processing of personal data, the correctness principle, minimising of personal data, the principle of integrity and confidentiality and the principle of responsibility. Legality of personal data processing is subject to some legal bases in § 13(1) in the new regulation; the use of camera systems and processing of personal data in this way is thus perhaps possible only under point (d), (e) or (f):

- processing of personal data is inevitable for the protection of life, health or property of the data subject or other natural person (d).
- processing of personal data is inevitable for the performance of a task carried out in the public interest or in the exercise of public authority conferred on the operator (e), or
- processing of personal data is inevitable for the purposes of legitimate interests of an operator or a third party, except for cases where the interests or rights of the data subjects which require protection of personal data prevail over those interests, in particular if the data subject is a child; this legal basis does not apply to the processing of personal data by public authorities in the performance of their tasks (f).

This is an analogy to the original regulation, i.e. that processing of personal data is possible even without consent of the data subject, if this is necessary to protect life, health, property of that person or any other person. Without the consent, the cases can be addressed where the personal data are processed for the purpose of protecting the interests of the person or a third party – this can be the case of use of monitoring devices in homes (in the house, flat), where the interest of person being burgled clearly predominates over the interest of the offender in the protection of personal data and the protection of personality.

This application is partially complicated by the fact that this Act does not apply to personal and home activities. And it is not clear what is included in them. The question is, what is processing of personal data for the purposes of home activities, i.e. whether these are the monitoring systems in

homes, houses, flats, in publicly inaccessible spaces, or not, whether it may be making of personal lists of debtors with their identification data, and the like. This formulation was taken over from the previous regulation, i.e. the Act valid and effective at the moment, where it is stated that these are personal lists, e.g. keeping of personal directory and the like. The legislator, however does not define it any closer in this regulation. If yes – and also these systems are a home activity, the Act does not apply to them under §3. If this is not a home activity, the Act applies to this activity, and thus allows to process the personal data.

Overall, this regulation can be assessed as yet a more problematic from the point of view of options to process personal data in connection with the use of camera systems and the use of recordings thus obtained. Naturally, there are methodological guidances of the Office for the protection of personal data, but their content rather relates to the original regulation and these have yet not been updated. The problem is that if the Office publishes some guidelines, it will remove them in 1-2 days from their site, because their application or substantive wording proves to be problematic. This does not add to legal certainty in this already complicated area.

3. CONCLUSIONS AND PROPOSALS *DE LEGE FERENDA*

With effect from 25.5.2018, the Act No. 18/2018 Coll. on protection of personal data and on amendments to certain acts becomes the effective part of our legal order. It is a reaction to the adoption of new EU regulation on the protection of personal data, as a consequence of the Slovak Republic being a part of the EU. This regulation replaces the still effective Act on the protection of personal data (full wording of the Act No. 136/2014 Coll.).

This original Act regulated the options for processing and the use of personal data obtained by the use of monitoring devices after meeting the legal conditions (in publicly accessible places). It partly addressed the processing of personal data without the consent of the data subject in places which are purely private (monitoring devices in the houses, flats), if they record only the private area. The new act links the processing of personal data only to the requirement of legality and pursued legitimate purpose – under Article 13(1)(d), (e) and (f). As we have already indicated, the regulation does not solve several aspects of personal data processing in the context of camera systems use. After the analysis of the original regulation and also the new one that has entered into effect on 25.05.2018, the following modifications, additions or amendments to this regulation are advisable. Their implementation will promote protection of personal data when using camera systems (monitoring devices) and at the same time allows to protect the rights of persons using these systems. Setting out of conditions, under which it will be possible to process the personal data, clearly specifies the cases where the personal data can be processed even without the consent of the data subject, where it will be possible to intervene in its personality rights for the purposes of achieving higher and legitimate objective – the protection of rights and the interests of personal data processor protected by law. This will prevent many problematic cases, where the solution is not supported by law, or not supported by a clear legal formulation, and depends on the assessment of the actual entity assessing it. We can therefore recommend the following:

- a.) Methodical guidances of the Office for the protection of personal data that still exist and are still attached to the original regulation must be updated.
- b.) It is not possible that the Office for the protection of personal data publishes a guidance on one day and removes it on the second day because it found out that its application is problematic; these are phenomena that violate the principle of legal certainty.
- c.) These methodological guidelines should only solve the methodology for processing of personal data and not the options, how and under what conditions the personal data should be processed and used; under which conditions to interfere with the guaranteed rights; these are crucial issues that should be addressed at the level of legal provisions.

d.) The option of personal data processing must be regulated – how they should be recorded, processed and used, if these are public spaces; the current legal regulation could serve as an inspiration. It provides legal requirements for this procedure clearly and precisely; if the space to be monitored for specific purposes is accessible to public, monitoring should be indicated clearly and precisely, then this procedure is legal and also without the consent of the person, his/her personal data can be processed and used as evidence in criminal proceedings and administrative proceedings when deducing legal liability.

e.) The conditions, under which the recordings obtained in the context of the home monitoring (solely private spaces of the house, flat, etc.) can be used, must be clearly defined; the new act does not quite accurately define what is to be understood by processing for personal or home activities, and whether these are also camera systems in houses and flats; they can primarily be intended only for monitoring of children (home nannies) or they may record unlawful activity of a person within the personal life; it should be clearly defined at the level of law that processing of personal data for home and personal activities is something different (making of personal directory), but not the use of monitoring devices in the privacy; it should be directly determined by law that these are not home activities, and therefore that the application of the new act is not excluded; subsequently such recordings can be used, although the personal data are processed without the consent of the data subject for the reason referred to in § 13(1)(f).

f.) The use of vehicle cameras should be defined by law; i.e. that the processing of personal data in this form is possible even without the consent of the data subject and that such recordings may also be used without its consent in the proceedings assessing the claims, administrative and criminal claims; these systems have to increase road safety and assist in resolving minor offences, criminal offences and insurance claims; they should help to establish clearly the driver at fault in case of an accident and other key aspects; it is inconceivable that such a significant means is not supported in our legal provisions, and it should be definitely introduced that personal data may be processed and the recordings used also without the consent of the data subject for the purposes of responsibility relationships and solutions of insurance events; it is inconceivable that these fundamental questions are solved by a methodological guidance.

g.) It is necessary to resolve the processing of personal data, when a private space is monitored but it also captures a part of public space; as there are different individuals moving here, it is necessary to require meeting of conditions to be laid down for monitoring of public spaces in such case, so that every person was informed that this space is monitored and was aware that his/her personal data may be processed; in addition, this will support the usability of such recordings in administrative or criminal proceedings in responsibility relationships.

REFERENCES

- Čentěš, J. et al.: Criminal Code. Large comment. IIIrd updated release. Bratislava: EUROKÓDEX, 2016.
- Ivor, J.: Monitorovanie obydľia kamerovým systémom a jeho využitie na účely trestného konania. In Zborník príspevkov z medzinárodnej vedeckej konferencie „Teoretické a praktické problémy využívania informačno-technických prostriedkov, FP PEVŠ, Bratislava, 2017.
- Ivor J.: Monitorovanie osôb ako dôkazný prostriedok v trestnom konaní In: Ochrana osobných údajov: zborník z celoštátneho seminára s medzinárodnou účasťou, Akadémia Policajného zboru, Bratislava, 2007.
- Lazar J. et al.: Substantive civil law 1st and 2nd volume. Bratislava: IURIS LIBRI, 2014.
- Siman, M., Slašťan, M.: Primárne právo EÚ. Bratislava: EUROIURIS, 2012.
- The Constitution of the Slovak Republic No. 460/1992 Coll., as amended by constitutional laws.
- The European Convention for the protection of human rights and fundamental freedoms as amended by additional protocols.
- Civil Code No. 40/1963 Coll. as amended

Full wording of the Act on protection of personal data No. 136/2014 Coll.

The Act No. 18/2018 Coll. on protection of personal data and on amendments to certain acts, as amended.

Methodical guidance of the Office for the protection of personal data No. 5/2016 named “Monitoring of premises inaccessible to public”.

Jtk 10/2012.