THE *RYNEŠ* CASE AND LIABILITY FOR INVASION OF PRIVACY IN THE 21ST CENTURY

Zdeněk Kühn *

Summary: New technologies combined with the internet have fundamentally altered our ability to have control over the diffusion of information and its impact on human behaviour. This paper explains this change as well as the transformation of the concept of privacy itself. The main part of the paper analyses the case law relating to local activities such as CCTV cameras in private buildings which serve to protect the property of the camera system operators. The author defends the regulation of privacy against the intrusions of providers of telecommunications and data services and corporations such as Google and Facebook. This should be exercised by the law of the EU because autonomous domestic regulation would endanger the free movement of services across the EU. Moreover, it would be difficult for separate national regulation to be successful in fighting global corporations like Google. On the other hand, there is not much sense in the European regulation of activities that are local by their very nature, such as the use of CCTV cameras in private buildings to protect the camera system operators' property.

1 Introduction

New technologies combined with the internet have substantially changed the way we conceive our world. They have fundamentally altered our ability to have control over the diffusion of information about ourselves. These new technologies include omnipresent smartphones and cameras, whether stationary, attached to buildings, or installed in cars to film the course of a journey. Then there is the recent trend of cameras carried by drones and similar devices, or the still quite rare system of Google Glasses (a camera installed in glasses).[1] Such devices

* The author (https://orcid.org/0000-0001-6952-3561) is Professor of Jurisprudence at the Charles University Law School and a Judge of the Supreme Administrative Court of the Czech Republic (SAC). The author acted as the judge-rapporteur in the *Ryneš* case. All opinions expressed in this paper are those of the author and not of the institutions he has represented. The author would like to express his gratitude to the participants at the Dubrovnik Conference in 2016 for their valuable comments. Errors in this paper are solely the responsibility of its author. This paper was written as part of the project of the Grant Agency of the Czech Republic Reg No 16-22016S entitled 'Legal Transactions and Legal Responsibility of Juristic Persons'. DOI: 10.3935/cyelp.14.2018.302.

[1] Google, the producer of Google Glasses, has attempted to make them similar to smartphones. See <https://plus.google.com/+GoogleGlass/posts/axcPPGjVFrb> accessed 21 July 2016. However, they are still at the prototype stage and further development is expected.

enable their user to post the recorded content on the internet within seconds. Recordings are often made for this very purpose, ie to be transmitted via web services. Even recordings made by cameras whose original purposes are different (typically security cameras protecting buildings, apartments and other property against vandalism, burglary or theft) may subsequently be posted on the internet, usually via various social networks, in order to trace offenders.[2]

Similar video or audio recordings are just a small piece of the mosaic of the fundamental transformation of the concept of privacy at the beginning of the third millennium. Such records by themselves, left somewhere on isolated data media devices or carriers, or placed on the internet but essentially undetectable, would not significantly alter or modify the protection of privacy. The argument regarding the protection of privacy is rather that the internet, in particular browsers such as Google and communication servers such as Facebook or Twitter, represents not only an increasing quantity of publicly available information intervening in the privacy of the people concerned but primarily a change in the paradigm of the concept of the protection of privacy.

This paper analyses the transforming modes of privacy. First, it explains the transformation of the invasion of privacy in the internet era and changes in the concept of privacy itself. The main part of the paper analyses the case law relating to local activities, such as CCTV cameras in private buildings which protect the property of the camera system operators (for the *Ryneš* case, see below). The author concludes that the regulation of privacy against intrusions by telecommunications and data service providers and corporations such as Google and Facebook is justified. It should be exercised by the law of the EU because autonomous domestic regulation would endanger the free movement of services across the EU. Moreover, separate national regulation in fighting global corporations like Google is not likely to be successful. On the other hand, there is not much sense in European regulation of activities that are local by their very nature, such as CCTV cameras in private buildings to protect the property of the camera system operators. The author explains that regulation under public law becomes toothless in such cases, and sanctioning becomes selective and essentially random. In addition, such regulation has the potential to further alienate ordinary citizens from the law.

[2] See the judgment of the SAC in *e-kolo.cz*, No 3 As 118/2015-34 of 8 June 2016. The owner of an electrical bike shop posted a photo of the thief on Facebook and, as a result, the thief was traced and caught. Subsequently, the owner was punished for the invasion of the thief's privacy.

2 Privacy before the internet and in the internet era

The meaning of the legal notion of protection of privacy has been and remains the subject of many definitions and concepts. One aspect of protection of privacy is particularly relevant for the purposes of this paper, and that is the possibility of an individual deciding what information about his or her life should become public. Frederick Schauer in his pioneering article on this topic succinctly summarised that the protection of privacy also presumes 'the power to control the facts about one's life'.[3] A similar attitude has been taken by R Posner in his economic analysis of law. He emphasises the aspects of the right to privacy relating to the control of individuals over the spreading of information about themselves.[4]

It is indisputable that the internet has changed the way in which we think about human conduct. It has fundamentally altered the possibility of controlling the spread of information and its impact on human behaviour. For example, an employer may, through a simple search via an internet browser, obtain a volume of information on a job applicant which would have taken a lot of money and the work of a detective agency at the end of the 1990s. Although most of this information has always been part of the public domain, what has dramatically changed is its availability due to a new medium which contains such information. Of course, the internet existed at the end of the 1990s. However, it did not contain as much information as it does today, mainly because a sophisticated browser like Google did not exist. Google and similar web browsers can, within a few seconds and in response to a relevant question, identify and show data (texts, pictures, videos, etc) which two decades ago would only have been made available through the continuous surveillance of the person concerned and by questioning their acquaintances, etc.[5] Such simple access to information of a certain type, although not always accurate, is unprecedented in the history of mankind.

The right to privacy has undergone a substantial change during the last two decades. The change may be described as both a quantitative and qualitative change. At the same time, the very concept of privacy has been subject to a significant transformation.[6] The differences in the types of interference in privacy are clear when we compare the time before the

---

[3] F Schauer, 'Internet Privacy and the Public-Private Distinction' (1998) 38 Jurimetrics 555, 556.

[4] R Posner, 'Privacy' in P Newman (ed), *The New Palgrave Dictionary of Economics and the Law 3* (Palgrave Macmillan 2004) 103-104.

[5] On the Google system, see the excellent article by O Tene, 'What Google Knows: Privacy and Internet Search Engines' [2008] Utah Law Review 1433.

[6] See for example Schauer (n 3) 557ff.

internet with the internet era.[7] The modes of intervention in privacy before the internet and Google were essentially physical: home searches, breaching mail secrecy, surveillance of an individual, interception, etc. Actors were usually the government, including the police or other state agencies, as well as printed or electronic media (radio and TV). Such interference was rare and each act of intervention could be perceived by the individual concerned, as it could be identified relatively easily.

The opposite can be seen in the internet era. The injured is often unaware of such interference, and although attacks may be quite frequent, each separate attack itself is usually not intensive. Intensive interference generally occurs as a result of traces we ourselves or third persons leave on the internet (our own speeches transmitted via social media and discussion forums; messages from individuals impersonating us; reports on us, whether taken from reliable or less reliable sources; photos and videos we or someone else have posted on a website; insults and fabrications regarding particular individuals on forums, etc). In theory, clandestine defamation was close to this kind of interference even before the internet was launched, but the range of potential addressees was drastically different.

During the internet era, the government and classical media rarely intervene. Should the state play any role, it is because we seek, successfully or unsuccessfully, its protection against such interference. However, in most cases we simply ignore such interference with our privacy, or we are even unaware of it.

The change in quantity lies primarily in the fact that the number of occurrences of the invasion of privacy has dramatically increased in the internet era. There are often denunciatory or false statements regarding particular individuals in various website discussions. With an increasing number of such statements and lies, the individual loses the possibility of defending themselves efficiently against such interventions. It should be admitted that the impact of defamation expressed during a discussion on an obscure blog is much smaller than that of a defamatory statement expressed during the prime time news on a national TV channel. Libellous and slanderous statements on the internet become a legal issue as soon as a large number of them are published and an ordinary internet user would be exposed to them on the initial pages they retrieve with any standard search engine when obtaining information on the person concerned.

This is linked to so-called autocomplete widgets, which are a very popular tool in all search engines. When users type the first letters of a word or phrase they are searching for, Google Autocomplete suggests a

[7] See for example FH Cate, 'Principles of Internet Privacy' (2000) 32 Connecticut Law Review 877, 877-878.

list of the most frequently searched for expressions beginning with the typed letters. It may happen that, through an autocomplete widget, Google or any other browser suggests information on the individual being looked up that is not positive about them.[8]

The whole issue has become more complicated with the fact that the role of traditional media is dramatically declining this century, while the importance of internet information is significantly rising. However, such a development is not always beneficial.

The biggest changes seem to affect the younger Facebook generation, which more or less covers people born after 1989. The large volume of personal information that users of social networks are willing to publish and make available to third persons is striking. Such information can be removed from the internet only with significant difficulty. Browsers keep older versions of websites irrespective of whether a particular website has been fundamentally changed later.[9] The content of individual internet websites is frequently copied and used by other internet websites over which the user of the original site has no control. Should a young person publish inappropriate material in his or her youth on the internet, there is essentially no chance of removing it later even after a very long time when the originally thoughtless youngster may have become a respectable official. Whilst human memory is rather short, the internet remembers forever.

3 The advantage of regulating activities of cross-border significance through European Union legislation

For a substantial period of their existence, all these phenomena were not subject to any intervention from the law. They were independent of the state and its authorities, and the business interests of individual operators of web search engines were the main driver in their development. Originally, the state was an inactive and helpless observer. An initiative to begin regulation under public law was primarily instigated by the fact that the unregulated processing of information by large corporations such as Google or Facebook might dramatically impinge upon the rights of people. However, data generated in this manner have started to be a tempting source of information for the police and other state authorities. It is not in the interests of the state to prevent the generating of such data

[8] Compare judgment no VI ZR 269/12 of the German Federal Supreme Court of 25 June 2013. In this case, the plaintiff complained that Google had suggested in connection with his name the words 'fraud' and 'scientology'. The Federal Supreme Court concluded that people affected in a similar way have the right to demand the elimination of the disputed combination or phrase.

[9] However, it should be noted that Facebook prevents its rival Google from searching through sites inside Facebook.

and metadata but to subject the process to firm rules. In recent years, the state has reacted to these phenomena. It has tried to set certain rules and restrictions under which the data accessed from the internet may be stored in databases.

Since the internet ignores borders and large corporations such as Google and Facebook run their businesses globally, it seems logical in Europe to have these phenomena regulated by the law of the European Union.[10] This is done mainly through the GDPR of 2016, which in 2018 replaced the earlier Data Protection Directive.[11] The GDPR is generally based on the presumption that the collection of data essentially requires the consent of the users concerned (subject to many exceptions, of course). However, such consent can be given by ticking a particular box by means of which the user agrees with the general terms and conditions of the website operator, regardless of whether they have read the conditions (and most users do not). As a result, such consent is fictitious in most cases.[12] On the other hand, if users really read through the terms and dislike them, very soon they come to the conclusion that there is no alternative, since the terms and conditions of other websites are comparable if not worse.

The regulation of the retention of data by providers of publicly available electronic communication services or public communications networks by means of the legislation of the European Union should be

[10] The Charter of Fundamental Rights of the EU of 2000 considers these issues and constitutionally regulates them in some detail. Under Article 8 of the EU Charter, every person has the right to the protection of his or her personal data (para 1). 'Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.' Charter of Fundamental Rights of the European Union [2000] OJ C364/01, para 2.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[12] See recital 32 of the GDPR: 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.' 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) (Text with EEA relevance) [2016] OJ L119/1.

considered reasonable. Providers of internet and telecommunications services, and various web search engines, etc operate their businesses across individual Member States. Inconsistent regulation would represent a real obstacle to the free movement of services within the EU. For example, different regulation of 'the right to be forgotten' in internet browsers across Europe would not only restrict the free movement of services but also cause an unequal position among the citizens of different EU Member States.[13] Moreover, we should realise that only common European regulation and not the autonomous regulation of, for example, a small country such as the Czech Republic can work against giants such as Vodafone, Telefónica, T-Mobile, Orange, Facebook or Google.

What makes little sense is the European regulation of activities regarding the publication of personal data which have no global or European impact or significance. Operating a static security camera under the roof of a family house and storing such recordings on a hard disk is an activity that is purely local. Even the fact that the operator of such a camera may possibly place the recordings on the internet (typically in order to trace the perpetrator of a crime) does not suggest that such an activity deserves the attention of the law of the European Union. It is difficult to assume that, in the words of the GDPR, such differences in the protection of personal data regarding these activities may prevent the free flow of personal data throughout the Union.[14]

---

[13] See *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317. For the first time, the Court of Justice (controversially) formulated the European principle of 'the right to be forgotten'. The CJEU, in relation to Directive 95/46/EC, the predecessor of the GDPR, stated that the activity of a search engine as a provider of content which consists of finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as the 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data. The operator of a search engine must be regarded as the 'controller' in respect of the processing of the personal data within the meaning of this provision. The operator of an internet browser has a duty, under certain circumstances, to erase the inclusion in the list of results displayed following a search made on the basis of a user's name of the links to web pages published lawfully by third parties and containing true information relating to the user personally. The operator has a duty to do so even in cases when the name or the information have not been erased from the respective websites or their publication was lawful. However, further details of requirements are rather cumbersome, and as such their practical application can be quite hard. It should be noted that the largest browser operators try to observe the conclusions of the *Google Spain* judgment. The case itself has attracted extraordinary attention on the part of jurisprudence. See, for example, Dan Jerker B Svantesson, 'The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach' (2015) EUI Working Papers, RSCAS 2015/45 <http://cadmus.eui.eu/bitstream/handle/1814/36317/RSCAS_2015_45.pdf?sequence=1> accessed 1 September 2018, which attempts to point out one of many deficiencies in the judgment, namely the still insufficiently elaborated issue of the applicability of EU law to cases that are global by nature.

[14] GDPR (n 12) recital, para 9.

4 The *Ryneš* case

It is one thing to protect personal data in the course of processing information with an internet browser whose different regulation within the EU may have a negative impact upon the free movement of services, or the collecting of data by providers of telecommunications services (internet providers, phone operators, etc). However, operating a residential camera system[15] or posting a photo from such a system on Facebook is a totally different issue.[16]

Mr Ryneš was a resident of a small Czech city who had faced harassment by unknown perpetrators over a number of years, perhaps related to his activity as a local journalist. He had been beaten up several times, and his house had been attacked on many occasions prior to April 2008. His windows had been repeatedly destroyed. The police were not able to detect those responsible and advised Mr Ryneš to buy a security camera to search for those accountable for the repeated attacks. Mr Ryneš followed their advice and between October 2007 and April 2008 used a camera located under the eaves of his house. The camera was in a fixed position and could not be rotated. It recorded the entrance to his home, the public footpath and the entrance to the house opposite. The system allowed only a visual recording, which was stored on a hard disk drive. Once full capacity had been reached, the existing recording would be erased and recorded over. No monitor was installed on the recording equipment, so it was not possible for the images to be viewed in real time. Only Mr Ryneš had direct access to the system and the recorded data.

The only reason for using the camera was to protect the property, health and life of his family and himself. On the night of 6 to 7 October 2007, a window was broken at Mr Ryneš' home by a shot from a catapult. The video surveillance system in question made it possible to identify two suspects. The recording was handed over to the police and subsequently used as evidence in criminal proceedings.

However, one of the suspects questioned the lawfulness of Mr Ryneš' surveillance system. By means of its decision of 4 August 2008, the local authority for privacy protection decided that Mr Ryneš had committed offences under the privacy law, owing to the following facts: as a data controller, he had used a camera system to collect, without their consent, the personal data of persons moving along the street or entering the house opposite; the data subjects had not been informed of the processing of these personal data, the extent and purpose of such processing, the identity of the data processor, the method of processing, or the per-

[15] See *Ryneš*, C-212/13, ECLI:EU:C:2014:2428 and the subsequent judgment of the Czech SAC of 25 February 2015, No 1 As 113/2012-133.

[16] The issue considered by the SAC in *e-kolo.cz* (n 2).

sons who might have access to the data at issue; as data controller, Mr Ryneš had not complied with the requirement to report the processing in question to the relevant office.

Mr Ryneš brought an action contesting the decision, which the Prague City Court dismissed. He then lodged a cassation complaint against this judgment before the Czech Supreme Administrative Court. The Court decided to make a preliminary reference to the Court of Justice, essentially questioning whether EU law in the form of Directive 95/46 was applicable. In the Czech court's view, the operation of a camera system installed on a family home for the purpose of protecting the property, health and life of the owners of the home should be classified as the processing of personal data 'by a natural person in the course of a purely personal or household activity' for the purposes of Article 3(2) of Directive 95/46, therefore making EU law inapplicable.

In considering the *Ryneš* case, the Court of Justice of the European Union had a chance to declare that a portion of such issues would not be subject to EU law. It could have subordinated the issues under a relatively indefinitely formulated exemption from the applicability of Directive 95/46 on the protection of natural persons in relation to the processing of personal data and the free movement of such data. The referring Czech Supreme Administrative Court explicitly invited the CJEU to do so.[17] The referring court claimed that 'it should be up to every single Member State whether such situations would be subject to the legal regulation of the protection of personal data or not.'

However, the Court of Justice did not take the opportunity. Instead, its steps were rather formalistic, namely a quasi-deductive procedure as follows: the objective of Directive 95/46 is to ensure a high level of protection of basic rights and freedoms of individuals and their privacy in particular. Thus, exemptions from the protection of personal data must be narrowly construed, and therefore the exception for data processing 'in the course of purely personal or household activities' within the meaning of Article 3(2) of the Directive was not applicable, as the camera systems had covered part of a public square.[18]

Since the Court of Justice of the European Union took a formalistic approach to this case, ie ostensibly preserving the literal rule when interpreting the Directive and spicing it up with a similarly formal jargon of human rights, namely 'the more regulations – the more human rights',[19] it failed to consider the real impact of its decision upon the reality of social relations. However, the Government of the United Kingdom in its

[17] This is exactly what the question in the reference for a preliminary ruling was about. See the decision of the Czech SAC of 20 March 2013, no 1 As 113/2012-59, para 15.

[18] *Ryneš* (n 15) paras 27-33.

[19] *Ryneš* (n 15) paras 28-29.

observation of proceedings noted that if household camera systems were not exempted from European regulation, it would lead to a needless bureaucratic burden for ordinary citizens. In addition, in this context such occurrences of the invasion of privacy of Europeans which are local by nature should be regulated by domestic law. It is the relevant national legislature that is perfectly aware of the crime rates in its territory and the efficiency of national police forces in fighting crime. This is why the national legislature knows best whether, within its jurisdiction, private camera systems should be regulated by public law, or whether private law regulation would suffice (including related issues like the right to post pictures of suspects online).

The judgement of the Court of Justice in the *Ryneš* case raises many other questions, in particular what the extent of the impact of Directive 95/46 or the GDPR is. The Advocate General in his opinion in *Ryneš* stated that video surveillance of a public place is characterised by its continuous and automatic nature, irrespective of the (varying) length of time of its storage. He added that 'by contrast, the legal questions associated with recordings made using mobile phones, camcorders or digital cameras are of a different nature.'[20] However, it is not that easy. The logic of the analysed decision suggests that should a student be recording their classmates leaving university every day between 11 and 12 for one week (which would usually be stored in a cloud storage system), or should they be recording (for several weeks) on their phone or video camera the gradual changes of a particular fruit tree with random passers-by being recorded as well, all such situations would be subject to regulation by European legislation on the protection of personal data.

The indeterminacy of the impact of Directive 95/46 and the GDPR can be illustrated well by an issue not expressly considered by the Court of Justice but mentioned by the Advocate General. At the hearing, the Court of Justice tackled the matter of how cameras installed in vehicles should be treated. The Advocate General in his interpretation considered it to be clear that 'those devices which monitor public streets, including persons moving along those streets, cannot be covered by the exception and that their use is therefore fully subject to the conditions laid down in Directive 95/46.'[21] The practice of evaluating the nature and substance of such cameras dramatically differs in EU Member States. They are forbidden in some countries and lawful in others. An example of the latter is the Czech Republic; its Office for the Protection of Personal Data assumes (contrary to the abovementioned opinion of the Advocate General)

[20] Opinion of Advocate General Niil Jääskinen, ECLI:EU:C:2014:2072, para 30.

[21] AG Jääskinen (n 20) footnote 43.

that such cameras are not comparable to cameras attached to buildings and therefore not subject to the regulation.[22]

With the expansion of new technologies, we can ask how public law regulation can be established so that it works efficiently. If a particular product is not generally forbidden or is not regulated at the time of its purchase, eg various camera systems or Google Glasses, the public authorities have no efficient means of regulating invasion of privacy. Practical examples may illustrate the point. Mock-up camera systems or camera systems placed on a building or vehicle but not turned on and thus unused are undoubtedly outside public law regulation. The fact that we can see a camera device on a building or a vehicle does not necessarily mean that the device is active and therefore subject to regulation. Since supervisory authorities have no right to enter buildings and vehicles (cars or trucks) in order to monitor such devices, they have technically no chance of ascertaining whether the law has been violated. If there are any sanctions imposed, it usually happens *ex post* at the moment when the recording is used against the perpetrator of an alleged crime and, as a result, it is obvious that recordings were or have been made on the respective device.

The GDPR shows an awareness of these problems. Article 58(1)(f) states that each supervisory authority in the Member States has the power to obtain access to any premises of the controller and the processor, including any data processing equipment or means, in accordance with Union or Member State procedural law. This new power of national authorities is not the remedy to the mentioned problems. On the contrary, unless the authorities are equipped with Orwellian powers and employ tens of thousands of agents to inspect millions of premises where personal data could eventually be processed, the new power will remain mostly on paper. The authorities will remain reactive, responding to various sorts of informants and neighborhood disputes.

Such regulation of new technologies remains rather formal. In general, it undermines respect for the legal order and most citizens simply ignore it. Sanctions for its violation might be imposed only rarely. On the other hand, the time and energy invested in reporting a device like

[22] See the Opinion of the Office for the Protection of Personal Data No 1/2015 of March 2015, 'Operating cameras on motor vehicles recording space outside the vehicle', p 3, para 6: 'From the perspective of the Office, due to the fact that such processing is without any risk with respect to invasion of privacy and the personal data of the data subject (unlike stationary camera systems, this system is unable to record for its operator a regular overview of people and their behaviour in a particular place, and does not interfere with the right of dwelling or represent surveillance of employees at work, which is forbidden under section 316(2) of Act 262/2006 Sb, Labour Code), and, at the same time, a different use of the recording from the camera system on the motor vehicle is not presumed (eg publishing) and it need not be the subject of a preliminary search by a supervisory authority, such processing is not subject to the duty to report [according to the Czech Data Protection Law].'

a camera monitoring system to a national supervisory authority is enormous,[23] which unfortunately results in people evading the law and taking risks.[24] This is why the GDPR moving away from the duty to report in similar cases towards the control of how collected data are handled (with a particular emphasis on data breaches) is to be welcomed.

Another problem arises when an office for the protection of personal data interprets the law in such a way that it is in conflict with the natural human understanding of what is just and appropriate when protecting one's property. An infamous example of this in the Czech Republic is the protection of the 'privacy of thieves': the Office imposed a sanction upon the owner of stolen property who tried to get the property back and posted a photo of the perpetrator of the theft on Facebook in order to ascertain their identity. The SAC in the subsequent litigation confirmed the sanction imposed upon the person who protected his ownership rights and posted the photos on Facebook. According to the SAC:

> the purpose of operating camera systems for the protection of property is not (in short) making a recording for future publishing but only for the possible handing-over to the competent authorities for further action. The investigation of crimes and sentencing of perpetrators (including those committing administrative delicts) is fully within the competence of state bodies.

If a person posts a photo of a thief on Facebook, it is considered not to be necessary for the protection of their rights or interests as protected by the law.[25]

---

[23] For example, the instructions on the website of the Czech Office for the Protection of Personal Data are far from being user friendly. Some forms are so complicated that only a person with the mixed competences of an IT specialist, lawyer and personal data protection specialist is able to fill them in correctly.

[24] Under the old directive, the procedure to discharge the duty to report a camera system easily became a bureaucratic ritual. The Czech Office in practice could hardly review, for example, whether the decision of the owners of a residential building to place a camera system on their building in reaction to vandalism or theft on the premises was proportional. It is difficult to accept the idea of the Office to substitute the decision of the owners of residential units on whether installing a camera system on their property was necessary with its own authoritative decision that due to the circumstances the owners should and could protect their property in a different manner. The Czech Office even reviewed technical details such as from what angle a camera may record common areas in the building or where cameras may be installed. Decision of the Czech Office for the Protection of Personal Data No 1/2016 of January 2016, 'Locating camera systems in residential buildings'.

[25] See *e-kolo.cz* (n 2). Interestingly, the new head of the Czech Office, Ivana Janů, appointed in 2015, denounced the earlier decision of her agency and promised that in future a different decision-making path would be taken by the agency. See the press statement of the Office: 'ÚOOÚ by pokutu v případu ekolo.cz znovu neudělil' ['The Office would not impose a fine in the ekolo case anymore'] 4 October 2017 <www.uoou.cz/uoou-by-pokutu-v-pripadu-ekolo-cz-znovu-neudelil/d-27149> accessed 1 September 2018.

5 Conclusion

The law on the protection of personal data as developed by the EU has a great ambition because it tries to cover the scope of both purely local activities and the practice of corporate giants. Consequently, the amount of corresponding rules is enormous and their application has become a new field for specialised lawyers. Likewise, specialised national agencies struggle and often change their interpretation of the law. This was the single most important reason why Mr Ryneš finally won his case before the Czech SAC. Over time, the Office has changed its interpretation of the limits of the scope of EU law with respect to domestic household camera systems. Originally, it claimed jurisdiction over these issues. However, it later expressly stated that it would not deal with these issues because they were beyond its power and subject to the 'household exception' of EU law. Taking into account the legitimate expectation of Mr Ryneš as a household owner, the SAC ruled in his favour. [26] Besides, added complication in the legal system and a lack of foresight in EU law further weakens legal certainty and the trust of EU citizens in the law.

All these problems lead to the conclusion that regulation under public law should not spend its energy tilting at windmills, ie it should not be designed to protect privacy in situations where new technologies invade it by their very nature. Public law regulation is meaningful if there is an apparent disproportion in the negotiating position between a client and the provider of services, and where – due to the limited capability of an ordinary person of understanding all the specificities of internet services – there is no informed consent to all the aspects of the services provided, such as when using Google, Seznam, Twitter, MyHeritage[27] or Facebook. A dispute involving an inhabitant of a residential house who feels restricted due to his neighbour having placed a camera on the neighbouring building need not and should not be solved by public law. It is private law which provides a sufficient number of possibilities of how to protect ourselves against the abuses of such cameras.

[26] *Ryneš* (n 15) part VD.

[27] MyHeritage is a global online service whose basic version is free of charge. It helps people create their family tree. MyHeritage makes commercial transactions with the data uploaded by client users, with only paying clients having access to the data of third persons. In the first half of 2016, MyHeritage launched a new service collecting DNA samples from its clients.