Case Note

On Private Persons Monitoring the Public Space

*Hielke Hijmans**

Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, Judgment of 11 December 2014, Opinion Advocate General Jääskinen of 10 July 2014.

I. Facts

This preliminary ruling finds its factual background in a camera that was installed and used by a Czech resident, Mr Ryneš, under the eaves of his family home. As the referring court points out, the reason for Mr Ryneš to install and use the camera was to protect the property, health and life of his family and himself. Earlier both Mr Ryneš and his family had been attacked by persons who could not be identified.[1]

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. Only Mr Ryneš had direct access to the system and the recorded data.[2]

One night, 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[3]. One of the suspects asked for confirmation that Mr Ryneš's surveillance system was legitimate.[4]

As a result it was found that Mr Ryneš was to be a considered a data controller who had not complied with the Czech data protection law. Mr Ryneš contested that decision, with the result that a Czech Court (the Nejvyšší správní soud) decided by decision of 20 March 2013 to refer the following question to the Court of Justice of the European Union ("the Court") for a preliminary ruling: 'Can the operation of a camera system installed on a family home for the purposes of protecting the property, health and life of the owners of the home 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 ..., even though such a system monitors also a public space?'

II. Judgment

The judgment of the Court gives an interpretation of the material scope of Directive 95/46/EC[5] ("the Directive"), where private persons process personal data in connection with a personal or household activity. Article 3(2) of the Directive exempts processing in the course of a *purely*[6] personal or household activity" from its scope.

The Court rules that the processing by the camera used by Mr Ryneš does not fall within this exception: "[The] operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision."[7] The deci-

* Associated researcher of the Free University Brussels (VUB) and the University of Amsterdam; Office of the European Data Protection Supervisor (Brussels), until 1 July 2014 as Head of Unit for Policy and Consultations, currently on sabbatical.

1 Paras 13 and 14 of the judgment.

2 Para 13 of the judgment.

3 Para 15 of the judgment.

4 Para 16 of the judgment.

5 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, OJ L 281/31.

6 Italics added by author.

7 Para 35 of the judgment.

sive element is that the camera also monitors a public space.

It comes to this conclusion through the following reasoning.

First, the Court addresses the terms "personal data" and "processing of personal data" in relation to images taken by video cameras. Personal data covers "any information relating to an identified or identifiable natural person, an identifiable person being one who can be identified, directly or indirectly, in particular by reference ... to one or more factors specific to his physical ... identity"[8] . This includes images of a person recorded by a camera, inasmuch as it makes it possible to identify the person concerned[9]. Processing of personal data covers in principle video surveillance of persons; the Court refers to recitals 15 and 16 of the Directive as confirmation of this presumption[10]. If the recording is stored on a continuous recording device — in this case the hard disk drive — it constitutes processing[11].

Second, the Court interprets the term 'in the course of a purely personal or household activity' by highlighting the fundamental rights' nature of the protection offered by the Directive, with a reference to its two recent landmark cases, *Digital Rights Ireland and Seitlinger* [12] and *Google Spain and Google* [13] confirming a high level of protection. Derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Consequently the exception under Article 3(2) must be narrowly construed[14].

Third, the insertion of 'purely' in relation to a personal or household activity, means that the exception does not relate simply to a personal or household activity[15]. For the exception to apply, the processing must be carried out in the purely personal or household setting of the person processing the data. As the advocate general has stated the link must be "exclusive".[16]

Fourth, the exception may cover correspondence and the keeping of address books, even if they incidentally concern or may concern the private life of other persons.[17] However, this is not the case where video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data[18].

Finally, the Court adds as an *obiter dictum* that the processing at stake – within the scope of the Directive – may be allowed by the Directive, taking into account legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself. The Court refers in this context to Articles 7(f), 11(2), and 13(1)(d) and (g) of the Directive[19].

This *obiter dictum* can be understood as stating that Mr Ryneš may have a legitimate interest for processing these data by his camera system, that it may be disproportionate to inform the persons whose data are captured and that the objective of the processing may concur with objectives recognised by the Directive, in particular the combat of criminal offences (mentioned in Article 13(1)(d)) and the protection of the data subject (mentioned in Article 13(1)(g)).

Arguments for this understanding of the *obiter dictum* can be found in the opinion of the advocate general, who also makes an interesting observation linking this *obiter dictum* with the scope of the Directive. He states that it would be "illogical to argue that, in order to protect Mr Ryneš' fundamental rights, it is appropriate to leave unapplied an EU directive which is specifically intended to strike a fair balance between Mr Ryneš' rights and the rights of other natural persons, namely, the people affected by the processing of personal data."[20]

III. Comments

The judgment confirms that the Court of Justice of the EU takes data protection particularly serious, in line with *Digital Rights Ireland (C-293/12) and*

8 Para 21 of the judgment.

9 Para 22 of the judgment.

10 The Court seems to use an a contrario reasoning based on recital 16. Recital 16 states that the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of the Directive, when it takes place for law enforcement purposes.

11 Paras 24 and 25 of the judgment.

12 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.

13 Case C-131/12, Google Spain and Google Inc, EU:C:2014:317.

14 Paras 27-29 of the judgment.

15 Para 30 of the judgment.

16 Opinion Advocate General Jääskinen, at 53.

17 The Court takes these examples from recital 11 of the Directive.

18 Paras 32 and 33 of the judgment.

19 Para 34 of the judgment.

20 Opinion Advocate General Jääskinen, at 66.

Seitlinger[21] and with *Google Spain and Google*[22]. Both cases were discussed in the first issue of European Data Privacy Law Review[23]. This approach of the Court is expressed in a systematic reference to the Charter of the Fundamental Rights of the Union, in relation to the interpretation of the Directive. An interesting element in the present case is that the Court only refers to Article 7 of the Charter (the right to privacy) and not to Article 8 of the Charter (the right to data protection), whereas in earlier cases it referred to both rights. This links to the ongoing academic discussion whether data protection is merely a subset of privacy, or that it delivers additional protection because it also covers situations outside the scope of privacy.[24] Although this case note is not the place to elaborate on this academic discussion an argument could be made that the Court, by assessing the Directive only in light of Article 7 of the Charter, takes the approach that data protection indeed is a subset of privacy. The Directive puts in place a legal system for the processing of personal data, but its aim is to (better) protect privacy. I admit, it could also be argued that this is a conclusion that gives too much emphasis to a practical approach of the Court, in this specific case.

Let me continue by discussing the elements of the reasoning of the Court. The Court confirms that where images are taken by video cameras, this falls within the terms "personal data" and "processing of personal data". This is a logical finding, in line with the intentionally wide scope of data protection rules in the Directive. In a technologically developing society the importance of the term "identifiable" in relation to personal data has gained relevance. Data protection deals increasingly with identifiable (so not yet "identified") persons. Video surveillance is a clear example[25]. The whole purpose of it is to capture data of not yet identified persons, in order to identify them in later stage. Equally, the material scope of the Directive includes increasingly covers all data processing. Article 3(1) of the Directive limits the scope of the Directive in relation to manual processing. Manual processing only falls within the scope of the Directive, if the data form part of a filing system or are intended to form part of a filing system. Obviously, this limitation becomes less relevant in our digitalised world.

The wide or wider scope of the Directive is also fully in line with the elevation of data protection to a fundamental right after the entry into force of the Lisbon Treaty, giving everyone the right to the protection of his or her personal data. A limitation of the scope of the protection by secondary EU law would not be in line with this right included in Article 16(1) TFEU and Article 8(1) Charter, because secondary EU law cannot limit a right of an individual allotted to him of her by primary EU law.

This all links to the main element of the judgment, the interpretation by the Court of the so called "household exception" of Article 3(2) of the Directive, which includes purely personal activities and is a limitation of the scope that must be narrowly construed[26]. The interpretation of this limitation has gained relevance in light of developments in the information society. This is the result of the wider scope of application of the Directive as such, but also of the fact that the interpretation of the household exception becomes more difficult.

The dividing line of what is confined to the private house or intimate sphere of an individual and what comes into the public environment is blurring. Information shared by individuals on social media is an obvious example. There is no precise demarcation line between posting or sharing of information on a social network site as a purely personal and as a (partly) public activity. Since the circle of friends with whom information is shared can be particularly wide[27] the difference with expression views on

21 Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238.

22 Case C-131/12, Google Spain and Google Inc, EU:C:2014:317.

23 Tijmen Wisman, Privacy: Alive and Kicking, European Data Protection Law Review 1/2015: pp. 80-84; Herke Kranenborg, Google and the Right to Be Forgotten, European Data Protection Law Review 1/2015: pp. 70-79.

24 Kokott and Sobotta in Data protection anno 2014: how to restore trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), Hielke Hijmans and Herke Kranenborg (eds), Intersentia 2014, p.83; Lynskey, Deconstructing Data Protection: The 'added-value of a right to data protection in the EU legal order, International and Comparative Law Quarterly / Volume 63 / Issue 03 / July 2014, pp 569-597; Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", published in the "Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013.

25 Example 14 in Article 29 Data Protection Working Party, Opinion 4/2007 on "the concept of personal data " – WP 136.

26 This reasoning does not necessarily apply to the other limitation of the scope of the Directive, in its Article 3(2), excluding the former second and third pillars of the EU Treaty. These pillars are (supposed to be) covered by other instruments of EU law, whereas within the domain of the household exception no data protection is provided.

27 See European Data Protection Supervisor, Opinion of 7 March 2012 on the data protection reform package, at 90-93.

public parts of internet is flu. Many of these situations will be covered by the Directive, as a result of the narrow interpretation of the limitation of the scope of data protection.

With CCTV-cameras, we see this same issue, as the present case shows. On the one hand, one can argue that the camera used by Mr Ryneš is a household activity. To be more specific, its purpose is to protect the household. It could be argued that the substance of the activity is linked to the personal sphere or the household of Mr Ryneš. This link is even more evident than in the case of sharing of information on social media. On the other hand, in order to protect the household areas around this household needed to be monitored. The effect of the activity is not limited to the personal sphere or the household. The Court uses the term "setting"[28]: the setting is wider.

In my view, this makes perfect sense, especially taking into account that the right to data protection is as said a right the data subject directly derives from primary EU law.

Furthermore, the judgment also gives indications whether this type of monitoring by video cameras is allowed under EU data protection law. In its *obiter dictum* the Court sketches the circumstances making this type of processing of personal data legitimate under EU law. It also gives indications how processing on the basis of the legitimate interest ground of Article 7(f) of the Directive could work out in practice[29]. Two elements stand out: first, in judging the legitimacy of the interest of Mr Ryneš the Court gives importance to the fact that his interest concurs with the public interests recognised under Article 13 of the Directive. Arguably, the protection of the security of his household by an individual is considered to be part of the public interest of security. Second, the Court indicates that there is no need to inform the data subjects of the monitoring. This indication raises the question whether it would indeed involve a disproportionate effort for Mr Ryneš to inform. Informing people – for instance through a general warning somewhere near his home – would possibly also have a preventive effect on those intending to disturb the security of his home.

Finally, the judgment can be used as an incentive to elaborate a bit more widely on technologies, capturing images of individuals in the public space. CCTV cameras are an example of this specific case, but one could also think of Google Street View, facial recognition built in smartphones or a technology that is highly topical, the private use of drones[30].

This provokes two questions. The first question is the extent to which individuals may expect that in the public space their privacy is protected. Privacy is a wide concept that is not limited to the sphere of the private home[31]. However, this does not mean that individuals may expect the same level of privacy in the public space where images are increasingly captured. It is not evident to what extent individuals have a claim against those who take image for instance of people having a drink on a public terrace or visit a public event. The second question is to what extent individuals are entitled to capture images of other individuals, for instance through CCTV cameras or smartphones? What is their legitimate interest under Article 7(f) of the Directive?

In Ryneš the Court only gives a partial answer. Individuals are data controllers, they may have a legitimate interest in processing personal data in a public space. However, what remains is a grey zone where it is not clear what is allowed under EU data protection law and what is not allowed.

---

28 Para 33 of the Judgment.

29 On Article 7(f), see Joined cases C-468/10 and C-469/10, ASNEF and FECEMD, EU:C:2011:777, at 39-40Further read: Article 29 Data Protection Working Party WP 217, 9 April 2014 Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".

30 See European Data Protection Supervisor, Opinion of 26 November 2014 on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner".

31 Further read: P. de Hert and S. Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in Reinventing data protection?, S. Gutwirth, et al. (eds), Springer 2009, at II.1.