The Expanding Scope of the Data Protection Directive: The Exception for a "Purely Personal or Household Activity"

Case Comment: C-212/13 *Ryneš v Úrad pro ochranu osobních údaju*

Oliver Butler[1]

Introduction

This case note comments on the judgment of the Court of Justice of the European Union (CJEU) in C-212/13 *Ryneš v Úrad pro ochranu osobních údaju*.[2] It argues that the CJEU has imposed a spatial logic on the interpretation of the exception for data processing "in the course of a purely personal or household activity": Article 3(2) of the Data Protection Directive 1995. It criticises that spatial logic as both too broad and too narrow. Too broad because the logic of the decision potentially captures many other forms of video-based recording and too narrow because it appears to exclude data protection from CCTV in the purely private setting, ignoring circumstances where individuals from outside the household might legitimately enter and be subject to intrusive monitoring. It examines the consequences of that logic for UK data protection law and guidance issued by the UK Information Commissioner's Office (ICO). This note argues that the implications of the reasoning in *Ryneš* could extend beyond these narrower changes and represent part of wider expansion of data protection through the interpretation of the CJEU, which has pursued a course of broad interpretation for provisions of the Directive and narrow interpretations of its exceptions. The note questions the desirability of this extension.

Ryneš

The CJEU gave its judgment in *Ryneš* on 11 December 2014 following a preliminary reference under Article 267 TFEU. The case attracted considerable interest from Member States. It concerned the appropriate interpretation of Article 3(2) of the Data Protection Directive 95/46/EC:

> "This Directive shall not apply to the processing of personal data… By a natural person in the course of a purely personal or household activity."

Ryneš had installed a fixed-position, visual-only camera system, which stored the visual data recorded to a hard drive on a continuous loop, without any ability to view the data in real-time via a monitor. This meant that data was only held until it was overwritten by new data placed on the hard drive and could only be accessed by Ryneš after the event. The camera recorded the entrance to his home, the public footpath and the entrance to the house opposite his home. Only Ryneš had direct access to the system and the data it contained. His only reason for operating the equipment was to protect the property, health and life of his family and himself, following attacks by persons unknown. Recordings of a later attack were subsequently disclosed to the police and used in criminal proceedings against vandals, who in turn made a complaint to the Czech Data Protection Office, the Úrad pro ochranu osobních údaju. The Czech Data Protection Office found that the surveillance system installed by Ryneš breached a number of

[1]PhD Student, University of Cambridge. This note develops arguments made in a presentation at the 2015 Winchester Conference on Trust, Risk, Information and Law, which had an overall theme of "the privacy arms race". I am grateful to Marion Oswald for inviting me to give that presentation, to Judith Townend for inviting me to turn the presentation into a longer piece, and David Erdos for his comments on the draft. All errors are my own.

[2][2014] ECR 0.

provisions of the Czech law implementing the 1995 Directive, including requirements to register as a data controller with the Data Protection Office. Ryneš challenged that decision.

The national court referred the following question to the CJEU for a preliminary ruling:

> "Can the operation of a camera system installed on a family home for the purposes of the protection of 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 also monitors a public space?"

Judgment of the CJEU

The CJEU held, without difficulty, that the system amounted to the automatic processing of personal data.[3] It reiterated, citing previous case law, that Directive 95/46 is intended to ensure a high level of protection of the fundamental rights and freedoms of natural persons and derogations and limitations in relation to the protection of personal data must apply only in so far as they are strictly necessary.[4] Accordingly, the exception provided for in the second indent of Article 3(2) had to be narrowly construed.[5] The CJEU was further encouraged to pursue a narrow definition, firstly, by the protection of privacy and data protection in the EU Charter and, secondly, by the very wording of the provision itself, which said that only "purely" personal or household activities were excluded.[6] In answer to the preliminary question, the CJEU held that:

> "To the extent that video surveillance such as that at issue in the main proceedings *covers, even partially, a public space* and is accordingly directed outwards from the *private setting* of the person processing the data in that matter, it cannot be regarded as an activity which is a 'purely personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46."[7]

A Spatial Logic

In focussing on the nature of the "setting" rather than whether the "activity" is personal or household in nature, the CJEU has imposed a spatial logic on the meaning of the exemption. Although I do not deny that the nature of the location in which an activity takes place may colour whether it is properly a purely personal activity, the CJEU held that even partial coverage of a public space would prevent CCTV from being a purely personal or household activity. The apparent logic is that video recording (and potentially also photographic recording more generally)[8] cannot be regarded as an activity which is "purely personal or household" for the purpose of exemption under Article 3(2) if that recording covers, even partially, a public space. The judgment does not make it clear to what extent this approach extends beyond CCTV or what characteristics of CCTV limit the reasoning to it, save that the case acknowledges that personal

[3] Paragraph 25.
[4] Paragraphs 27 and 28.
[5] Paragraph 29.
[6] Paragraph 30.
[7] Paragraph 33, emphasis added.
[8] Although there was no real discussion of photographic recording more generally in the judgment.

correspondence and records of addresses fall within the definition of a purely personal or household activity.[9]

A different definition without this spatial logic is possible. The CJEU could simply have held that, by its nature, the *activity* of CCTV surveillance to *identify persons unknown* cannot be a purely personal or household activity, irrespective of the nature of the setting in which it takes place. The practice and growth of CCTV surveillance is not a purely personal or household activity, like keeping correspondence or holding records of addresses. It is an intrusive means of collecting potentially extensive information about data subjects.

As it stands, the definition is both too broad and too narrow. Too broad, because the logic of video recording outwards the private setting potentially removes many other personal or household activities from the scope of the exemption and too narrow because the logic of the decision suggests that CCTV covering only private land for personal security purposes may be exempt, even if its purpose is to record information about persons unknown or other persons from outside the private setting who enter it under licence or by right.

Opinion of Advocate General Jääskinen

Advocate General Jääskinen, in his Opinion, rejected the idea that the personal or household nature of an activity could rest on the purpose of the relevant data processing. He rejected that notion as too subjective and therefore difficult to objectively verify. Confusingly, he considered such purposes to be sufficiently objective and verifiable to be of use when assessing the lawfulness of the processing itself:

> "In my view, the scope of an EU legal instrument cannot depend on the subjective purpose of an interested party – in this case, the data controller – since that purpose is neither objectively verifiable by reference to external factors nor relevant with respect to the data subjects whose rights and interests are affected by the activity in question…
>
> On the other hand, the purpose of the processing may come into play when its lawfulness is assessed. The scope of the Directive must therefore be established on the basis of objective criteria."[10]

It is difficult to understand why facts relating to the purpose of an activity are objective and verifiable for assessing lawfulness within the scheme of the 1995 Directive but are subjective and unverifiable for the purpose of determining whether an exemption to the 1995 Directive exists. The purpose of a particular activity as a fact is capable of determination to the same extent irrespective of which part of the Directive is then applied to that fact.

The Advocate General went on, however, to consider the definition of personal and household in terms which do not limit personal activities to a private setting in which they take place:

> "In my view, 'personal' activities under the second indent of Article 3(2) of Directive 95/46 are activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others. These activities may,

[9] The Court did accept at paragraph 32 that, in light of Recital 12 of the Preamble to the Directive, correspondence and the keeping of address books would be within the exception "even if they incidentally concern or may concern the private life of other persons." Recital 12 states "… there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence or the holding of records of addresses".

[10] AG Opinion, paragraphs 46 and 47.

> however, take place outside the home. 'Household' activities are linked to family life and normally take place at a person's home or in other places shared with family members, such as second homes, hotel rooms or private cars. All such activities have a link with the protection of private life as provided for under Article 7 of the Charter."[11]

The Advocate General did, however, agree that "it is true — as the UK Government contends — that the protection of the inviolability of a private dwelling and the protection of that dwelling against theft and illegal access are activities which are essential for each household and, for that reason, activities that can be regarded as household activities."[12]

He rejected the idea that protection of the home through CCTV beyond the home could be a purely personal or household activity however as:

> "video surveillance which covers a public space cannot be considered to be a *purely household* activity, because it covers persons who have no connection with the family in question and who wish to remain anonymous."[13]

The CJEU went further than the Advocate General by imposing a spatial logic on the meaning of a purely personal or household activity that would be absent under the Advocate General's definition of personal activities.

C-101/01 Lindqvist

Little guidance can be drawn from the only other EU case to consider the application of Article 3(2): C-101 *Lindqvist*, as it dealt only with the dissemination of personal information to an indefinite number of people via the internet.[14] In that case, Lindqvist had published various pieces of personal and sensitive personal data about her co-workers at a church to a personal website which, at her request, had been linked to a national Church's website. Following objections, she was prosecuted by the relevant data protection authority and challenged the decision, on the ground, among other things, that the information was processing in the course of a purely personal or household activity. The court rejected that argument and held that:

> "As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses.
>
> That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people."[15]

Implications: The Data Protection Act 1998

[11] AG Opinion, paragraph 51.
[12] AG Opinion, paragraph 55.
[13] AG Opinion, paragraph 56, emphasis in original.
[14] [2003] ECR I-12971.
[15] Paragraphs 46 and 47. Serious doubts can be raised as to whether the ICO's guidance on social networking and online forums is compatible with *Lindqvist*. See ICO Guidance, Social Networking and Online Forums – When does the DPA apply?, at paragraph 42.

The spatial logic in *Ryneš* runs contrary to the purpose-orientated approach of UK implementation of the 1995 Directive. This has several implications for the UK.

Article 3(2) of the 1995 Directive was implemented in the UK by the Data Protection Act 1998, section 36. Section 36 provides that:

> "Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection principles and the provisions of Parts II and III."

This provision has only been addressed briefly by the UK courts and there is little relevant case law. *Ryneš* has some important implications for the interpretation and application of this provision. First, section 36 is framed in terms of purpose rather than activity, as per the terms of Article 3(2), or the nature of the setting, as per the spatial logic in *Ryneš*. Given the rejection a purpose-driven interpretation in the Advocate General's Opinion and the adoption of a spatial rather than a purpose-oriented understanding of activities, there must be doubt about whether it is safe to rely on the plain meaning of the words of section 36. Secondly, both family and recreational purposes appear to be elaborations on the meaning of personal or household activities. It is no longer safe to rely on these elaborations without more. For example, it is no longer clear that recreational video recording outward the private setting would remain within the exemption, given the logic of *Ryneš*.

Implications: ICO Guidance

The application of Article 3(2) has mainly been through guidance and practice developed by the ICO. The implications of *Ryneš*, therefore, are most acute in relation to that guidance. This section considers the ICO guidance beyond CCTV which has potentially been cast into doubt by the decision in *Ryneš*.[16]

Unmanned Aerial Systems

ICO guidance on unmanned aerial systems (UAS) or drones provides that:

> "A distinction should be drawn between those individuals who can be considered as *'hobbyists'* and are therefore generally using their device for *domestic purposes*, and those individuals or organisations who use the device for *professional or commercial purposes*. Where UAS are used for *non-domestic purposes*, operators will need to comply with data protection obligations and it will be good practice for domestic users to be aware of the potential privacy intrusion which the use of UAS can cause to make sure they're used in a responsible manner."[17]

The ICO guidance relies on a purpose-orientated approach to the Article 3(2) exemption, distinguishing between domestic and non-domestic purposes for the relevant data collection. This approach was criticised in the Advocate General's Opinion and not adopted by the CJEU. Instead, the spatial logic applied to CCTV might equally come to be applied to video recording from drones, which, when recording outward a private setting, present a significant threat to the privacy of third parties. It is possible that a similar conclusion would be reached for drones as for CCTV, contrary to the existing ICO guidance.

[16] See ICO Guidance: In the picture: A data protection code of practice for surveillance cameras and personal information.

[17] Page 30, emphasis added.

Implications: Schools

ICO Guidance: Taking Photographs in Schools states that "photos taken purely for personal use are exempt from the [Data Protection Act 1998] DPA" and gives two examples:

> "A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the DPA does not apply."
>
> "Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the DPA does not apply."[18]
>
> There are significant differences between the intrusiveness of CCTV and its threat to data protection and personal photography or video recording. However, it is not clear to what extent the fact that such recording outward the private setting will render photography or video-recording other than "purely" personal. Certainly, many third parties, including children, are the subject of data processing where school performances are recorded. It may be questioned how far such facts really are from *Ryneš*.

Implications: Wearable Technology

Although wearable technology has not been the subject of formal ICO guidance, the ICO has nevertheless posted comment on its news blog. The relevant passage reads:

> "If you are using a wearable technology for your own use then you are unlikely to be breaching the Act. This is because the Act includes an exemption for the collection of personal information for domestic purposes. But if you were to one day decide that you'd like to start using this information for other purposes outside of your personal use, for example to support a local campaign or to start a business, then this exemption would no longer apply."[19]

The guidance, in common with UK implementation in the Data Protection Act 1998 and other ICO guidance, takes a purpose-orientated approach to determining which activities are purely personal or household (here referred to as domestic) activities. However, many items of wearable technology, for example body worn cameras like the increasingly popular video recording devices built into cyclist's helmets, will involve the collection of data about individuals outward the private setting in an manner analogous to the CCTV in *Ryneš*. We may therefore question to what extent such technology can escape the spatial logic of *Ryneš*.

Justice for Mr Ryneš?

One of the troubling aspects of this case is the fact that Mr Ryneš was prosecuted for using CCTV to protect his home from criminals following a complaint made by the very criminals his CCTV helped to convict. There is certainly some discomfort in this, which may drive one to consider that the defence of one's home is a household activity par excellence. It should, of course, be noted that the effect of the decision is to regulate the relevant CCTV, not to ban it, and the effect of the decision would have remained the same if Ryneš had happened to be a less meritorious defendant.

---

[18] ICO Guidance: Taking Photographs in Schools, page 2.

[19] Andrew Paterson, Senior Technology Officer, ICO, Wearable Technology – the future of privacy, 26 June 2014, https://iconewsblog.wordpress.com/2014/06/26/wearable-technology-the-future-of-privacy/.

There is also, however, a discomfort in that an uncertain area of the law was interpreted in a way that left Ryneš exposed to criminal sanction under the national implementing law. Now that the law is clarified, such a discomfort would no longer exist in the case of those who neglect their data protection duties, although the consistency of ICO guidance with the CJEU jurisprudence is potentially a continuing cause for concern.

Injustice was, however, avoided for Mr Rynešin the resolution of the national litigation following the reference to the CJEU.[20] The Czech Supreme Administrative Court held that because the implementing legislation was vague and the practice of the Data Protection Office inconsistent, criminal punishment would violate his rights under Article 7 of the European Convention on Human Rights.[21] Accordingly, Ryneš was not found criminally liable for his CCTV system, although the law was now clarified by the judgment so that future individuals in his position would be criminally liable.

Questioning the spatial logic

The inclusion of private CCTV surveillance systems outward, even partially, of the private setting is to be welcomed. The technology represents an invasive and broad potential collection of personal and sensitive personal data about individuals.

However, one may question the need for a spatial logic. Further, we might question the clarity of the division between the private and public setting. There remain unanswered questions which may give rise to future litigation.

Should CCTV be exempt in the purely private setting, as *Ryneš* seems to suggest, even where that space may be entered by individuals from outside the household who enter under licenses, such as cleaners or plumbers or guests of the household, or implied licenses, such as those making postal deliveries which require an approach of the house through the private setting of a front garden or driveway, or by statutory right, such as the myriad of government officials who have such powers? Is it appropriate that data protection is exempted in that space even where the purpose is the surveillance of third parties? The Advocate General took the view that CCTV surveillance was a "household activity" in the private setting, but is it always purely so? The Opinion is silent on the point.

There are also questions about the wider application of the principles expressed in *Ryneš*. The Advocate General foresaw this difficulty and sought to avoid it in his Opinion:

> "By contrast, the legal questions associated with recordings made using mobile phones, camcorders or digital cameras are of a different nature, and so will not be addressed in this Opinion."[22]

It is not clear that that the application of the spatial logic beyond CCTV can so easily be avoided. The CJEU did not deny the applicability of the spatial logic beyond CCTV but was silent on its application beyond CCTV. Google glass and its equivalents present similar problems of intrusiveness and third party impact. So do body-worn recording devices and other wearable technology outward the private setting. Drones, smart phone and other cameras and video recording devices, or smart watches can all be intrusive. The internet of things will increase the

[20] I am grateful to Mr Vít Zvánovec of the Czech Data Protection Office for bringing this case to my attention.
[21] sp. zn. 1 As 113/2012–133, paragraphs 68 to 71. The decision can be found at: http://www.nssoud.cz/files/SOUDNI_VYKON/2012/0113_1As__1200133_20150225164111_prevedeno.pdf.
[22] AG Opinion, paragraph 30.

opportunities for surveillance in and around the private setting. More everyday concerns for the *Ryneš* decision relate to the extent to which tourists may take photographs or video in public spaces or hobbyists may record video for personal enjoyment.

Conclusion: Expanding EU Data Protection?

The theme of the 2015 Winchester Conference on Trust, Risk, Information and Law was the "privacy arms race."*Ryneš* certainly falls within a broader set of judgments by the CJEU that have expanded the scope of the 1995 Directive. I would, however, be more cautious about characterising this as part of an "arms race" rather than a trend which reflects broader concerns about data protection in Europe as a result of rapid technological change and increasing revelations of data protection breaches.

Despite signs that the text of Article 3(2) might not survive into the General Data Protection Regulation,[23] Article 2(2)(d) of the consolidated text of the draft General Data Protection Regulation, which reached political agreement in December 2015, has maintained the exemption for the processing of personal data "by a natural person in the course of a purely personal or household activity".[24] The judgment in *Ryneš* is therefore likely to remain relevant in the interpretation of the scope of EU data protection law.

The spatial logic on Article 3(2) adopted in relation to CCTV in *Ryneš*, if applied consistently to other video-recording equipment would suggest that many personal or household activities cannot be "purely" personal or household for the purposes of the exemption. Its full implications may make data protection a concern for any technology-using private individual. This would represent a much broader scope for the 1995 Directive than existed under the purpose-oriented implementation and regulatory understanding that proceeded *Ryneš* in the UK. The judgment leaves many questions unanswered. We might also consider the extent to which there will be an enforcement gap in practice between the scope of data protection regulation and the matters that regulators actually tackle. We might ask whether there will be a wilful blindness to the natural implications of the reasoning in *Ryneš* or whether the decision will be confined to CCTV. Finally, and most importantly, we should ask whether the effect of *Ryneš* is to create an exemption that regulates too much in public spaces and too little in the private setting.

[23] See Commission Proposal for a General Data Protection Directive (2012)

[24] See Extraordinary Meeting of the LIBE Committee, 17 December 2015: http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884