scripted

Volume 11, Issue 1, April 2014

THE DATA RETENTION DIRECTIVE NEVER EXISTED

Judith Rauhofer, Daithí Mac Síthigh[*]

Abstract

Analysis of the decision of the Court of Justice of the European Union in Joined Cases C-293/12 (*Digital Rights Ireland*) and C-412/12 (*Kärntner Landesregierung*), on the validity of the Data Retention Directive.

DOI: 10.2966/scrip.110114.118

[*] Lecturers, School of Law, University of Edinburgh. Many thanks to Prof. Chris Himsworth and Prof. Niamh Nic Shuibhne for comments.

1. Introduction

The Court of Justice of the European Union (ECJ) has ruled that the 2006 Data Retention Directive[1] is invalid.[2] The basis of invalidity was the exceeding of the limits imposed by the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter of Fundamental Rights (Charter). The decision was in respect of two joined preliminary references, one from Ireland and the other from Austria.

The decision is a significant step in the development of the ECJ's jurisprudence with regard to the protection of fundamental rights. This is the first time that the ECJ has declared not just individual provisions but an entire legal instrument invalid for violations of Charter rights. Despite suggestions from the Advocate General that the legislature be given an opportunity to amend the law, the invalidity is absolute and immediate. A closer inspection of the court's reasoning also provides fresh insights into the court's interpretation of the right to privacy (Article 7, Charter) and the relatively new right to data protection (Article 8, Charter), and scope for further development on the relationship between surveillance and freedom of expression (Article 11, Charter).

In this short note, we will consider significant aspects of the decision, and discuss the ways in which it may have an impact on the specific issue of data retention and on wider questions of fundamental rights in the European Union.

2. Context

2.1 The Directive

The Directive provided that member states must adopt laws requiring communications service providers (CSPs) to retain certain types of traffic, subscriber and location data generated by users of their service (Article 6). The retention period is between six and twenty-four months, although member states may opt for longer periods where they face "particular circumstances warranting an extension for a limited period" (Article 12(1)).

Some aspects of data retention are left to the member states. The retained data is to be available for the purposes of the investigation, detection and prosecution of serious crime, although there is no definition of "serious crime" in the Directive. As such, member states will adopt their own threshold for when data can be used. Neither does the Directive regulate the conditions for access by public authorities and law enforcement authorities of the member states.

---

[1] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[2] Cases C-293/12 (*Digital Rights Ireland*) and C-412/12 (*Kärntner Landesregierung*).

2.2 Procedural history

This case was not the first review of the Directive by the ECJ. The Irish Government had unsuccessfully challenged the legal basis, in a case determined by the ECJ in 2009.[3] The result on that occasion was that the Directive was held to have been appropriately made on the basis of article 95 (now article 114 of the Treaty on the Functioning of the European Union (TFEU)) as an internal market measure. Fundamental rights were not considered in the 2009 decision.

The same government then found itself the subject of further proceedings in Ireland. Campaign group Digital Rights Ireland brought an application for judicial review of the Directive before the High Court of Ireland. The court made a preliminary reference to the ECJ, setting out questions on the compatibility of the Directive with Article 5(4) of the Treaty on European Union (TEU) (necessity and proportionality), and with a range of rights protected by the EU Charter of Fundamental Rights. In 2012, an action was brought before the Austrian Constitutional Court by the state government of Carinthia and over 11,000 individual applicants. The applicants claimed that the Austrian law transposing the Directive infringed their rights under Article 8 of the Charter. Again, a preliminary reference was made. The ECJ joined the two cases together in 2013.

Advocate General Cruz Villalón gave his Opinion in December 2013, in which he concluded that the Data Retention Directive is, as a whole, incompatible with Article 52(1) of the Charter, since the limitations on the exercise of fundamental rights it contains are not accompanied by the necessary principles for governing the guarantees needed to regulate access to the data and their use. He recommended that the ECJ find that the Directive is invalid, but that the effects of that finding should be suspended pending adoption by the EU of the measures necessary to remedy the invalidity.

3. Decision of the Court of Justice of the European Union

The court treated the various questions of the referring courts as a request to examine the validity of the Data Retention Directive in the light of Articles 7, 8 and 11 of the Charter. It found that all three rights were capable of being engaged.

3.1 Which rights are engaged?

It found that the retention of communications data pursuant to Articles 3 to 5 of the Directive, for the purpose of possible access to them by the competent national authorities, directly and specifically affects private life. It based its conclusion on the fact that communications data "as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out and the social environments frequented by them".[4] As a result, it found that the Directive fell within the scope of Article 7 of the Charter. The data retention requirement imposed by Articles 3 and 6 of the Data

---

[3] *Ireland v European Parliament,* [2009] ECR I-593.

[4] *Digital Rights Ireland*, note 2 above, at [27].

Retention Directive constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter. As the Advocate General already pointed out in his opinion, such a retention requirement derogates from the system of protection of the right to privacy established by the Data Protection Directive[5] and the E-Privacy Directive.[6] In addition, the access of the competent national authorities to the retained data constitutes a further interference with that fundamental right.

In finding that the Directive was within the scope of article 7, the court drew upon its own case law, including *Volker und Markus Schecke and Eifert*[7] and *Österreichischer Rundfunk*,[8] and that of the European Court of Human Rights, in particular *S. and Marper v the United Kingdom*.[9] The court made it clear that both the retention of and access to personal data (in this case communications data) constitutes an interference with the right to privacy. This is important as proponents of data retention have long argued that the mere retention of data should be regarded as a lesser type of interference and should therefore not enjoy the full protection provided for by Article 7. However, the ECJ follows the ECtHR in emphasising the engagement of fundamental rights, and found that "[t]he retention of data for the purpose of possible access to them by the competent national authorities […] directly and specifically affects private life".[10]

The court also made it clear that the mere *retention* of communications data constitutes the *processing* of personal data within the meaning of Article 8 of the Charter and, therefore, necessarily has to satisfy the data protection requirements arising out of that Article. This assessment differs from the Advocate General's view, who had argued that the Article 7 right applied to the collection and retention of data, while the Article 8 right covered its subsequent use. Since the Directive was not concerned with the latter, the Advocate General did not think that Article 8 needed to be examined. Although the court's reliance on article 8 has not added much to its own interpretation of that relatively new right (many EU legal scholars would have preferred a more precise delineation between the scope of Article 7 and Article 8), it can fairly be said that, in general, the retention of personal data constitutes an act of processing and that Article 8 is therefore engaged – a finding of relevance across the European data protection system.

The ECJ furthermore acknowledged the potential impact data retention could have on individuals' exercise of the freedom of expression guaranteed by Article 11 of the Charter. Although the court ultimately did not see a need to examine the validity of the Directive in the light of Article 11, it found that it was not inconceivable that the retention of the data in question might have an effect on Internet users' use of means of electronic communication. At a time when certain, important cases are perceived as

---

[5] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[6] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[7] [2010] ECR I-11063.

[8] [2003] ECR I-4989.

[9] (2009) 48 EHRR 50.

[10] *Digital Rights Ireland*, note 2 above, at [29].

turning on a conflict between the ECHR/Charter articles on expression and on privacy, even the recognition that a law on data presents an arguable challenge to the vindication of the right to freedom of expression is important. The court draws upon the established formulation of "chilling effects" as threats to the freedom of expression, providing opportunities to future litigants to formulate Charter claims in a range of different fashions.

3.2 Was there interference, and was that interference in pursuit of a legitimate objective?

Having established the relevance and engagement of the rights, the court went on to hold that the interference with the rights in Articles 7 and 8 was not justified. Initially, though, the court declined to find that the *essence* of either right was adversely affected. Its basis for this finding was the non-application of the Directive to the content of electronic communications (in respect of article 7) and requirements for data protection and data security (in respect of article 8).

However, the court made it clear that it considered the Directive to constitute a particularly serious *interference* with those rights, highlighting in particular "the important role played by the protection of personal data in the light of the fundamental right to respect for private life"[11], and the likely impact on individuals' perception of surveillance. In a particularly evocative formulation, the court explained the issue as follows: "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance". This particular finding strongly echoes observations made by the German Constitutional Court in its 1984 "Census" decision, where it had stressed the importance of a right to informational self-determination as a facilitator for the exercise of other fundamental rights.[12] In particular, the Constitutional Court had argued that an individual, who was unsure if information about differing behaviour is at all times noted, permanently stored, used or disclosed as information, will try not to attract attention through such behaviour.

On the other hand, this interference was in pursuit of an objective of general interest. While harmonisation of laws was clearly the aim of the Directive, the court acknowledged that its material objective is to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime and thus, ultimately, to contribute to public security. The court confirmed that the fight against international terrorism and serious crime constitutes an objective of general interest, pointing out that article 6 of the Charter includes the personal right to security.

3.3 Was the Directive a proportionate measure?

As is common in the practice of the European Court of Human Rights, the area of most dispute before the ECJ was the application of the proportionality principle, the interference and objective having been established. Notably, the court found that in

---

[11] *Digital Rights Ireland*, note 2 above, at [48].

[12] (1983) BVerfGE 65, 1.

view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life, and the extent and seriousness of the interference with that right caused by the Directive, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

The court accepted that the provisions included in the Directive were suitable to achieve the material objective. However, it ruled that while the fight against serious crime, in particular against organised crime and terrorism, is of the utmost importance, it "does not, in itself, justify a retention measure such as that established" in the Directive.[13] Advocates for privacy will see this aspect of the decision, along with the ongoing fallout from the disclosures made by Edward Snowden, as evidence that the fight against terrorism and serious crime is no longer the universal trump card it once was. Communications service providers, and others that may find themselves obliged to disclose personal data to public bodies, are now in a much stronger position if they wish to oppose such disclosure requests. This is of both political and legal significance.

In particular, the court criticised the adoption of a measure that:

- Covers, in a generalised manner, all persons and all means of electronic communication, without any differentiation, limitation or exception being made in the light of its crime-fighting objective.
- Affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions.
- Applies even to persons whose communications are subject to the obligation of professional secrecy.
- Does not require any relationship between the data to be retained and a threat to public security and which, in particular, is not subject to a temporal or geographic restriction or a restriction to persons who could, for other reasons, contribute to the prevention, detection or prosecution of serious offences.

As noted above, the Directive only harmonised certain aspects of the data retention system. The result was a mandatory EU framework governing the retention of communications data, with regulation of access to that data left to the member states. This led to significant discrepancies in the approaches employed by various members states with some, like the UK, authorising access to the data for purposes never envisaged in the Directive and to organisations unconcerned with the fight against crime and terrorism. In addition, the distinction between retention and access has allowed countries to adopt different procedural safeguards.

The court has now made it clear that it would like to see a harmonised access regime with strictly applied substantive and procedural safeguards. The Directive was criticised for failing to lay down any objective criterion or substantive and procedural conditions governing competent national authorities' access to the data and their subsequent use for the purposes of law enforcement and public security. In particular, the court stated that it would like to see conditions on restricted access to and use of

[13] *Digital Rights Ireland*, note 2 above, at [51].

data, a limitation to the number of persons authorised for such access or use, and prior review of access by an appropriate body. The lack of objective criteria for the duration of the retention period (between six and twenty-four months) was criticised, as was the absence of a distinction between different categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

The court concluded that the Directive failed the proportionality test as it does not lay down clear any precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Instead, it entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

Its criticism of the general manner in which the current Directive affected more or less the entire EU population with no regard for those citizens, whose actions would have never made them subject to any kind of criminal investigation is a clear indicator of the way in which the perception of the potential impact of surveillance on democratic structures has changed post-Snowden. In reminding the legislator that distinctions must be made and that future retention measures should ideally be limited temporally, geographically and by the type of data subject to whom they apply, the court has indicated that it would be much more comfortable with a targeted approach, even without reference to the contested terms "quick freeze" or data preservation".

3.4 Data security and transfer

In addition to its consideration of the strict legal issues under review, the court also used its decision to raise the issue of data security. It highlighted the fact that the Directive does not provide for sufficient safeguards, nor does it impose a specific obligation on member states to establish such safeguards, to ensure the effective protection of the data retained against the risk of abuse and against unlawful access and use. Specifically, the ECJ criticised how, through Article 7 in conjunction with Article 4(1), the Directive permits providers to have regard to economic considerations when determining the level of security which they apply. The Directive also fails to ensure the irreversible destruction of the data at the end of the data retention period. The court was of the view that the Directive should include safeguards that are specific and adapted to the vast *quantity* of data to be retained, the sensitive *nature* of that data, and the *risk* of unlawful access to that data (e.g. rules on security and protection).

More importantly, the court criticised that the Directive does not require the data in question to be retained within the EU. It argues that this makes it impossible to control compliance with applicable EU data protection and data security requirements. That control, which the court views as an essential component of the protection of individuals' data protection rights, must be exercised by an independent authority (Article 8(3), Charter).

Stakeholders will surely have taken note of the ECJ's comments on the need to store retained data within the EU to ensure independent oversight of compliance with applicable EU data protection and data security requirements by independent EU authorities in accordance with Article 8(3) of the Charter. It may very well be that this conclusion will prove to be a particularly explosive one, indicating as it does a

hardening of attitude with regard to international data flows. Following the Snowden allegations, it has become clear that many of the means used by EU governments and businesses to ensure that transfers of personal data to non-EU countries are lawful, do in practice enable transfers to countries like the US where those data may be accessed by public bodies on the basis of national laws that might not be compatible with the EU fundamental rights framework.

The European Parliament and the European Commission are already discussing ways in which better control can be ensured in those situations. For example, discussions are ongoing between the Commission and the US government on how the EU-US safe harbour arrangement can be improved. The Parliament inserted additional restrictions that would tighten up data exports to non-EU countries into the draft General Data Protection Regulation. The ECJ's observations with regard to the safeguards required in this area will also raise new questions with regard to other existing international arrangements, like the Agreements on the transfer of passenger names records and the financial transaction data, and inform the Commission's position with regard to future negotiations of, for example, the long awaited EU-US data protection umbrella agreement. What is clear in the light of this judgement is that the status of privacy and data protection as fundamental rights protected by the EU legal order can no longer be ignored when those discussions are held. Otherwise there is always a risk that international agreement that may take years to negotiate will fall at the final hurdle of judicial review by the EU's own court.

It is as yet unclear what this may mean for EU data controllers who may wish to transfer personal data to providers outside the EU, for example in the context of cloud computing. While the fundamental rights framework does in the first instance provide a defence against state intrusions, it could be argued that it is now entirely possible that, for example, the ECJ would also find a provision in the proposed Data Protection Regulation incompatible with Charter rights, if the EU legislator fails to include adequate safeguards designed to protect EU citizens' data from unauthorised access by third countries' governments. The implications this decision may have for the ultimate shape of the new EU data protection framework is therefore difficult to assess at this stage.

4. Implementation and impact of the decision

Although the decision is silent on this matter, a press release published by the court makes it clear that in the light of the fact that the court has not imposed any temporal limitation on the invalidity, the Directive is invalid from the date it came into force.[14] This can be distinguished from the Advocate General's advice to suspend such a declaration for a specified period,[15] which is not discussed at all by the court.

This means that there is currently no EU law mandating the retention of communications data. The European Commission has published an FAQ document, in which an optimistic tone is adopted, explaining that national legislation implementing the Directive will only have to be amended to the extent required by the court's

[14] "Press release 54/14" (8 Apr 2014) available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (accessed 14 Apr 14).

[15] *Digital Rights Ireland* (Opinion of the Advocate General) at [154-158].

decision.[16] It also highlights that member states' competence to adopt their own national data retention laws under Article 15(1) of the E-Privacy Directive remains unaffected.

While the ECJ's decision means that the Directive itself is invalid *ab initio*, the same does not necessarily apply to the national laws adopted by the member states to implement the Directive. This raises few difficulties for those countries directly involved in the current case, whose national courts are now tasked with applying the ECJ's guidance to the legal challenge before them. For example, in Austria, where the referring Constitutional Court has the right to void an Act of Parliament, it is now likely that it will do so with regard to the Austrian implementing law. The High Court of Ireland has similarly robust powers. Similarly, in countries like Germany that have not yet re-implemented the Directive after the original national Act was declared null and void by its Constitutional Court under the national fundamental rights framework, are now free from the obligation to implement. In this context it is expected that the European Commission will withdraw the legal action already brought against Germany in this regard.

However, the situation is somewhat more complicated in countries like the UK that have implemented the Directive and where communications service providers are consequently already retaining significant amounts of data on their customers. While it is generally assumed that national Parliaments will specifically have to repeal or revise national implementing laws (if courts do not do the job for them first, where constitutionally permitted), the right to adopt new measures is generally not contested provided that such measures comply with the requirements of the E-Privacy Directive. That directive permits "legislative measures providing for the retention of data for a limited period" (Article 15(1)), under certain circumstances. A measure that restricts the general obligation not to retain traffic data for longer than necessary for the providers own commercial purposes (Article 6(1) of the same Directive) must constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard one of a list of public interest purposes. In practice, this is likely to mean that any national law that mandates the retention of communications data must now operate within the framework the ECJ set out in its current decision. Whether new data retention laws are now tackled at national or EU level is of limited legal relevance, although it is an interesting political question – not least because at least one member of the European Commission reacted very differently to the official line.[17]

As far as the UK is concerned, an additional point is that of the UK's approach to implementing EU legislation on the basis of section 2(2) of the European Communities Act 1972 (ECA). Since the Data Retention (EC Directive) Regulations 2009 that implement the Directive were adopted as a statutory instrument, they constitute subordinate legislation that requires an enabling provision in order to be valid. Given that section 2(2) of the ECA only serves this function to the extent that it

---

[16] European Commission, "Frequently asked questions: the Data Retention Directive" (MEMO/14/269) available at http://europa.eu/rapid/press-release_MEMO-14-269_en.htm (accessed 14 Apr 14).

[17] See Commissioner Viviane Reding's post on Twitter (8 Apr 14): "#EU citizens+ #EU Charter of Fundamental Rights win. Guaranteeing security+ respecting #dataProtection must go hand in hand. #dataRetention" available at https://twitter.com/VivianeRedingEU/status/453449768459833344 (accessed 14 Apr 14).

authorises the implementation of an EU instrument, it may no longer be capable of doing so when that instrument, as in this case, is invalid from the date it came into force. If this were the case, it is therefore possible that the UK Regulations themselves are now without a legal basis and hence ultra vires the parent Act. If that were confirmed, the UK would have to adopt new provisions of primary legislation (a new Act or an amendment of an existing Act) if it wanted to re-introduce data retention requirements at national level.

The rejection of the contention that retention affects the essence of the rights concerned does leave the door open for both the EU and the member states to adopt some kind of data retention framework in the future, provided that that framework takes on board the points raised by the court. Member states intending to rely on the Commission's advice on the 2002 E-Privacy Directive must also be aware that the overall approach to data retention adopted by the ECJ on this occasion would be of the highest relevance if any future measures claiming to be authorised by the earlier Directive were to be challenged. Given the reliance on ECtHR decisions in the present case too, the prudent member state should hesitate before readopting provisions along the lines of the now invalid Directive.

5. Conclusion

It is difficult to overestimate the potential impact the ECJ's decision is likely to have with regard not only to the retention of communications data but also the wider field of fundamental rights protection within the EU and the member states. To this extent, the court's decision is truly capable of being a "game changer", even if it has taken a long time for a decision that some commentators had doubted since it was proposed to be properly scrutinised. However, it is currently unclear how this will play out in detail and much of this will depend not only on the legal and cultural traditions of the individual members states but also on the political pressures their governments find themselves under. For EU citizens and businesses, in particular the communications service providers that were directly affected by the now invalid retention requirement, this is likely to mean a sustained period of legal uncertainty as the various institutions both at EU and at member state level come to an agreement on how this substantive and procedural issues raised by the ECJ's decision should be resolved. At the same time, it could be argued that those substantive and procedural issues have always existed, at the very least since the EU Charter came into force, and that all that has happened is that the ECJ has now sharply removed the sticking plaster that up to now has held a creaking system together. It is to be hoped that discussions and decision-making processes to deal with the long-term fallout of this decision will be made quickly to reduce any potential damage to EU citizens, businesses and the EU project as a whole.