NEWSLETTER CVA

THE METADATA CONTROVERSY & EU LAW

In today's digital age, data is increasingly valuable and ubiquitous. From social media posts to financial transactions, we generate vast amounts of data every day. Nonetheless, the value of data is not just in its content in the traditional sense, but also in its metadata (or 'data about data')[1]. With the rise of digital technology, metadata has become a rich source of evidence in criminal investigations, particularly in cases involving cybercrime, terrorism, and financial fraud, due to the crucial contextual information it can provide.

However, the use of metadata may, at the same time, raise important issues related to privacy and personal data protection. First, metadata can be used to infer personal information about individuals. Secondly, metadata is often generated automatically by electronic devices and services, and individuals may not be aware of its collection or use, putting their personal data and privacy rights at risk. Finally, metadata has gradually been used by governments and law enforcement agencies for surveillance purposes, arguably at the expenses of civil liberties and fundamental rights.

[1] 'Metadata' usually refers to data encompassing the circumstances of communications, but excluding the latter's content (see, to this effect, the judgment of the Portuguese Constitutional Court no. 268/2022, p. 35).

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

I. The impact of the Digital Rights Ireland case on Data Retention

A. Digital Rights Ireland and the invalidity of the Data Retention Directive

In 2006, mandatory data retention was harmonised at European Union ('EU') level through Directive 2006/24/EC ('Data Retention Directive'). This directive was meant to aid law enforcement and national security agencies in investigating and preventing serious crimes. It also sought to tackle the disparity of national measures (see, in this regard, Recital 6 of the e-privacy Directive) adopted on the basis of Article 15(1) of Directive 2002/58/EC ('e-Privacy Directive'), which allowed Member States to limit the right to privacy of electronic communications, provided that they seek to safeguard national security (rectius, State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences.

However, in 2014, the Court of Justice of the European Union ('CJEU' or 'Court') declared, in the case of *Digital Rights Ireland*, the invalidity of the Data Retention Directive. Despite acknowledging that data retention genuinely satisfies objectives of general interest in the fight against serious crime, the Court found that the directive did not respect the proportionality principle, as the interference with fundamental rights was not limited to what was strictly necessary. In particular, the CJEU noted that the Data Retention Directive obliged telecommunications companies to store sensitive personal data of users for one year, including information on aspects of private and family life, such as location and contacts, without any connection to criminal activities, and without allowing users to object to this collection. Furthermore, there were no exceptions for communications covered by professional secrecy and, at the same time, there were no security measures to protect personal data.

The Data Retention Directive was thus declared invalid, as the CJEU held that it disproportionately restricted the rights to respect for private and family life and to the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('CFREU').

As a result of this ruling, the e-Privacy Directive (re)took its role as the legal basis for national legislation on data retention. Although the judgment in *Digital Rights Ireland* did not affect the validity of that Directive, the retention and use of metadata based on its Article 15(1), also considering its wording and nature (namely, "(...) when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e., the security of the State), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system"), necessarily has to conform to the requirements set out by the Court in that judgment. This flows from the fact that Member States are prohibited

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

from enforcing national legislation implementing an invalid directive, in so far as that legislation is in contradiction with the grounds for the Court's decision. In fact, judgments rendered by the CJEU have 'erga omnes' effect, hence binding the legislature, the administration and the judiciary of all Member States.

It is therefore of the utmost significance that appropriate measures are implemented to safeguard the protection of European citizens' personal data and privacy, in accordance with the CJEU's pronouncement. As a matter of fact, and as explained hereupon, the provision reinstated by the judgment in *Digital Rights Ireland* already demanded that measures restrictive of the scope of the rights and obligations provided by EU law respected the principle of proportionality.

Against this background, following the CJEU's ruling, several national courts have been called upon to rule on domestic legislation adopted to implement the Data Retention Directive. In the context of such proceedings, some courts have resorted to the preliminary ruling procedure (C-140/20, C-623/17; Joined Cases C-511/18, C-512/18 and C-520/18). In one of those cases - *Tele2 Sverige* - the CJEU confirmed that the invalidity of the Data Retention Directive indeed affected implementing national provisions allowing a generalised and undifferentiated obligation to retain metadata.

It further declared that the interpretation of the e-Privacy Directive, namely its Article 15(1), must take into consideration the importance both of the right to privacy and the right to the protection of personal data, as guaranteed by the CFREU. Besides, as the list of objectives laid down in that article is exhaustive, Member States cannot adopt measures for other purposes than those mentioned in the same provision (see para. 90 Tele2 Sverige).

This limits the right of Member States to introduce exceptions to the obligation to ensure the confidentiality of personal data. Consequently, in Member States, such as Portugal, where the legislation transposing the Data Retention Directive continued to apply following the declaration of invalidity of that directive, many criminal convictions were based on a potentially unlawful access to data.

B. The situation in Portugal following the judgment Digital Rights Ireland

The Data Retention Directive was transposed to the Portuguese legal system by Law No. 32/2008 of 17 July ('Metadata Law'). It defines 'metadata' as electronic communications traffic and location data, as well as the related data necessary to identify both the subscriber and the user, simultaneously or separately. Such data allows the identification of all data regarding electronic communications, including location, identification of the source and destination of the communication, date, time, duration of communication, type of communication, and the equipment used, with the exception of their content or contents.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

Even though no reference for a preliminary ruling has been made by Portuguese courts, as it probably should, the CJEU's judgment in *Digital Rights Ireland* did not remain unnoticed in Portugal. The National Data Protection Commission ('CNPD') issued two recommendations for the disapplication and revision of the Metadata Law in cases submitted to it (Deliberation No. 641/2017, of 09 May 2017 & Deliberation No. 1008/2017, of 18 July 2017, CNPD). Moreover, the Portuguese Ombudsperson recommended in January 2019 to the government that the Metadata Law be made conform with the requirements of the CFREU and the existing oversight gap in Portugal be addressed.

As there were no signs of willingness to change the law, the Ombudsperson initiated a case before the Portuguese Constitutional Court ('PCC' or 'Constitutional Court'), requesting it to declare that the general and indiscriminate retention of traffic and location data of subscribers and registered users for the specific purpose of investigating, detecting, and prosecuting crimes is not conformed with the Constitution of the Portuguese Republic ('CRP'), regardless of their nature.

In its Judgment No. 268/2022, the Constitutional Court declared the disconformity with the CRP, with general mandatory force, of rules contained in the Metadata Law[2]. Specifically, the PCC declared:

The unconstitutionality of Article 4 of that law, read in conjunction with Article 6, on the retention and storage of the data referred to therein, for the period of one year, was declared on the ground, inter alia, that it breached the right to informational self-determination. As the Constitutional Court stated, this right is set out in Article 35 of the CRP, which guarantees its holder the power to decide on the use and disclosure of his personal data, as well as the power to control the information available about him/her. Such right is complemented by the power to control the treatment of data and by the duty of the State to protect that right, both constitutionally established.

[2] In its judgment, the Constitutional Court rightly clarified the relationship (and the differences...) between the analysis of the conformity with EU Law of a national legislation and the analysis of constitutionality of that same legislation with the national constitution: "[...] the incompatibility of a certain national rule with EU law does not automatically lead to a judgment of unconstitutionality; on the contrary, it affects its effectiveness at the internal level, insofar as it contradicts European rules that apply simultaneously. As EU law defines it, this effect occurs regardless of the source of the conflicting rules: whether the European rule is contained in primary law (such as the CFREU, by virtue of Article 6 of the TEU) or in secondary law (such as a directive or a regulation); and whether the national rule is contained in a regulatory act, a legislative act or even in the Constitution. Therefore, showing a contradiction between the national rules in question and EU law does not allow the conclusion that they are unconstitutional. A finding of unconstitutionality - and thus the invalidity of the national rule - depends on the non-conformity of the rules under scrutiny with their hierarchically superior parameter, namely the Constitution".

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

The Constitutional Court also noted that, to exercise such control, citizens must be aware that their data have been acceded. It further held that such control must be guaranteed by an independent administrative authority, constitutionally provided – which means that the data cannot be stored in jurisdictions outside that control (this is, outside the EU territory).

Nevertheless, the storage of basic data - IP protocol addresses and other basic data like civil identity of telephone number and e-mail address holders and dynamic IP protocol addresses relating to the source of a communication -, regardless of the period foreseen of one year, would not in itself be unconstitutional had the legislator complied with the obligation to ensure that storage takes place within the territory of the European Union; which it did not.

By contrast, the Constitutional Court stated that the same does not hold true, "as regards the obligation to store traffic data, generated in relation to a specific communication, in particular location data. In this case, the compression of the fundamental right to privacy is more intense, which impacts on the proportionality of the restriction. The retention of these data is therefore manifestly excessive".

The Constitutional Court also added that, "If the measure to preserve traffic and location data in itself can be considered adequate and necessary for the purposes of public interest that it aims to safeguard, the definition of the range of subjects targeted does not exceed the limits of proportionality only insofar as it is directly aimed at situations in which the restriction on the fundamental rights in question can be considered necessary to the pursuit of the objectives of criminal action. In this context, by exceeding the limits of proportionality in the measure at issue, as regards its subjective scope, Article 18(2) of the Constitution is violated as concerns the restriction of the fundamental rights to privacy and informative self-determination (Articles 26(1) and 35(1) of the Constitution. The question of whether other elements on which the proportionality of the measure would depend (the adjustment of the retention period to that strictly necessary for the purposes to be achieved; and the imposition of security conditions for the respective storage) are fulfilled by the regulation under scrutiny loses relevance".

The Constitutional Court then ruled that, by combining Articles 4 and 6 of Law no. 32/2008, in question, the obligation to collect and store the personal data listed therein for a period of one year, constrains, at the very least, the rights to the respect intimacy and private life, free development of personality and informative self-determination.

The Court also examined article 9 of the Metadata Law, regarding the transmission of stored data to the competent authorities for investigation, detection and repression of serious crimes. Considering that it does not provide for notification to the targeted individuals whose data have been accessed by criminal investigation authorities, to the extent that such communication is not likely to compromise investigations or the life or physical integrity of

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

third parties, there is a breach of the principle of proportionality for restricting the rights to privacy, secrecy of communications, and effective judicial protection. The right of someone to be aware of the treatment given to his personal data is in itself inalienable.

The Constitutional Court accordingly decided to declare the unconstitutionality of articles 4º, 6º and 9º of Law 32/2008.

In fact, considering the content of the Metadata Law and bearing in mind the CJEU's ruling in Digital Rights Ireland, this outcome was highly expected. More than that, given the principle of primacy of EU law and the binding force of the Court's rulings (referred to above), all national provisions affected by the deficiencies identified by the Court in similar provisions of the directive should have been immediately disapplied, without the need to wait for a 'confirmatory' ruling of the Constitutional Court.

II. What to expect in the future from the different actors involved?

Since the Metadata Law was enacted in 2008, the Portuguese authorities have used metadata as legitimate evidence in criminal cases, particularly in cases of internet fraud. Despite the CJEU's judgment in Digital Rights Ireland, Portugal maintained its national law transposing the Data Retention Directive until 2022. Therefore, for approximately nine years, Portuguese law required telecommunications companies to retain metadata, including information about the time and duration of communications, the numbers dialled and the location of the device used. As without metadata, it becomes very difficult to identify and monitor suspects or their technological devices, it is crucial for public security reasons that Portugal adopts, as soon as possible, rules complying with both EU law and the CRP and respecting fundamental rights, without losing efficiency in the fight against serious crimes (see Joint Declaration of the European Police Chiefs – Lisbon Declaration, available at https://www.policiajudiciaria.pt/declaracao-de-lisboa-metadata-conference/).

Until this occurs, authorities will not be able to rely on metadata in criminal investigations. However, according to a recent ruling of the Supreme Court of Justice ('SCJ' or 'Supreme Court'), the Constitutional Court's ruling will not affect judgments that became res judicata. Even though this seems to be an acceptable interpretation of paragraph 3 of Article 282 of the CRP, it is regrettable that the SCJ did not consider the interplay with EU law.

Indeed, the compatibility of the Metadata Law with fundamental rights was, to say the least, doubtful since the CJEU's ruling in Digital Rights Ireland in 2014. Apparently, the Supreme Court did not consider itself concerned by the Court's ruling. Additionally, the SCJ did not even consider the obligation to refer a question for preliminary ruling to the CJEU, for the purposes of the third paragraph of Article 267 TFEU. This is a cause for serious concern, as it compromises the uniformity and effectiveness of application of EU law throughout the whole territory of the EU. It is for the national courts to ensure the effective and uniform

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

application of Union law within their jurisdiction, while the CJEU is the final guarantor of that uniformity.

At the EU level, co-legislators have also struggled to adopt new legislation that strikes an appropriate balance between the right to privacy and the legitimate interests of national security and the fight against serious crime. In this context, the proposal for an e-Privacy Regulation, adopted by the European Commission in 2017, recognises the need for European legislation to keep pace with the rapid development of IT-based services in order to strengthen trust and security in the digital world. The proposal highlights the need to adapt e-Privacy legislation to the new rules set out in the General Data Protection Regulation ('GDPR'), including rules for all electronic communications and, more specifically, privacy guarantees for both the content and metadata of communications. In a sense, the proposed e-Privacy Regulation seems to be part of the European Commission's response to the issue as a whole, aiming to address the lack of uniformity and confusion among national legislators.

In fact, since Digital Rights Ireland, and in the absence of an immediate response from the EU legislator, some Member States have introduced provisions to regulate the use of metadata for criminal investigation purposes. However, the approaches taken vary widely, with some Member States allowing the use of metadata with few restrictions, while others have more stringent rules. Some of these rules have been successfully challenged in national courts (v.g., 'Polish government working on controversial surveillance bill'; 'Intelligence law: what metadata can tell about you').

In conclusion, following Digital Rights Ireland, the Portuguese legislature should have amended the law to address the concerns raised by the CJEU. In addition, national courts should have struck down provisions of Portuguese law raising similar issues to those identified by the Court, without waiting for the Constitutional Court to intervene. In cases of doubt, it is imperative to refer the case for a preliminary ruling so that national courts can fulfil their obligations, also to ensure that Portugal complies with EU rules while safeguarding the fundamental rights of EU citizens.

As far as the EU institutions are concerned and given the lack of consistent responses at national level, there is an urgent need to adopt legislation that regulates the retention and use of metadata in a way that respects fundamental rights.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524