UNIO - *EU Law Journal*. Vol. 3, No. 2, July 2017, pp 45-56.

School of Law – University of Minho

The recent jurisprudence of the CJEU on personal data retention: implications for criminal investigation in Portugal

Alessandra Silveira[1]
Pedro Miguel Freitas[2]

ABSTRACT: It can be concluded from the Tele2 judgment of 2016 that i) the declaration of invalidity of the provisions contained in a directive inevitably affects the legal act of transposition into the legal order of the Member States, and ii) a Member State cannot resort to the Directive 2002/58 to impose a generalised and undifferentiated obligation to conserve traffic and location data following the declaration of invalidity of Directive 2006/24. It is, therefore, urgent to draw conclusions from this recent ruling by the CJEU, which is all the more relevant because, in Member States where the transposed legislation continued to apply following the declaration of invalidity of Directive 2006/24 – as was the case in Portugal – many criminal convictions were based on the access to potentially illegitimate data. The authors seek to demonstrate what is happening in Portugal in this area and call for compliance with the jurisprudence of the CJEU – not only because the effectiveness of the European Union law is at stake, but also (and above all), the legal equality between European citizens.

KEYWORDS: data retention – right to protection of personal data – invalidity of Directive 2006/24 – Digital Rights Ireland's judgment – Tele2's judgment.

[1] Director of the Centre of Studies in EU Law (CEDU) of the University of Minho and Jean Monnet Chair in EU Law.
[2] Professor at the School of Law of the University of Minho. PhD member of the Centre of Studies in EU Law (CEDU) of the University of Minho.

1. The invalidity of Directive 2006/24: implications for the legal order of Member States[3]

Following the terrorist attacks in London and Madrid, and in the context of European competence for the protection of personal data [currently provided for in Article 16 of the Treaty on the Functioning of the European Union (TFEU)], the European Parliament and the Council have adopted the Directive 2006/24 (on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks). This directive regulated the retention of data by service providers in the exercise of economic activities for the purpose of investigating, detecting and prosecuting serious crime, irrespective of any prior request by the Member States' law enforcement officers or judiciary.[4]

The data in question allows one to decipher with whom a user has communicated, by what means, the time of communication, the place from which the communication takes place, and how often a user communicates with certain people during a certain period – information which is known by "*metadata*".[5] The directive was applicable to traffic data and location data, relating to both natural and legal persons, including information consulted using an electronic communications network – albeit it did not apply to the content of the communication. Since then, Member States have been retaining the data for periods of no less than six months and no more than two years from the date of communication, so that they can be transmitted, upon request, to the competent authorities.

However, in the *Digital Rights Ireland* judgment of 2014, the Court of Justice of the European Union (CJEU) declared the Directive 2006/24 invalid. The heart of the matter laid in the fact that the directive covered all those who used electronic communications services in Europe – even those whose data was not criminally relevant. In addition, the directive did not provide for any differentiation, limitation or exception in the light of the objective of combating serious crime and therefore, applied even to persons whose communications were subject to professional secrecy. Besides this general absence of limits, the Directive 2006/24 did not lay down an objective criterion for delimiting the access of the competent national authorities to the data and their subsequent use. Moreover, it did not require that the data in question should be kept within the territory of the Union, and therefore, it could not be considered that supervision by an independent entity was fully guaranteed.

Ultimately, the directive obliged electronic communications service providers to retain data whose analysis makes it possible to "*create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and*

[3] For a detailed account of this topic, see Alessandra Silveira and Pedro Freitas, "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados pessoais ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental", *Revista de Direito, Estado e Telecomunicações*, Universidade de Brasília, vol. 9, nº. 1 (2017), http://www.ndsr.org/SEER/index.php?journal=rdet.

[4] The purpose of the provisions of the Directive 2006/24 was the harmonization of national laws regarding the obligation to retain data (Article 3), categories of data to be retained (Article 5), periods of retention (Article 6), data protection and data security (Article 7), as well as storage requirements for retained data (Article 8).

[5] Elspeth Guild and Sergio Carrera, "The political and judicial life of metadata: Digital Rights Ireland and the trail of the data retention directive", *CEPS Papers in Liberty and Security in Europe* 65 (2014): 1.

accurate picture of his private identity".[6] A general obligation to retain data in these terms allows for serious individual interference by means of targeted surveillance, but also mass interference which might be even more worrying. In other words, those that affect a substantial part or even the entire relevant population of a Member State, such as the identification of all individuals suffering from psychological disorders or of all individuals who are opposed to a certain political regime. For example, individuals who have contacted a psychologist during the data retention period or all individuals on mailing lists who criticise a political regime government policy might be instantly identified.[7]

The CJEU was then called upon to assess the validity of Directive 2006/24 in the light of Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union (CFREU) and was of the opinion that the obligation imposed by the Directive 2006/24 on the providers of electronic communications services constituted an interference with those fundamental rights.[8] To that end, it did not matter whether or not sensitive data was involved, or whether or not such interference caused inconvenience to the parties concerned.[9] While it is true that the fight against serious crime is of prime importance for ensuring public safety and that its effectiveness may depend on the use of modern investigative techniques, such a general interest objective, however fundamental it may be, cannot, in itself, justify that a retention measure such as that introduced by the Directive 2006/24 should be considered necessary for the purposes of that fight.[10]

To this extent, the CJEU concluded that the Directive 2006/24 did not provide sufficient guarantees, as required by Article 8 of the CFREU, to ensure effective protection of the retained data against the risks of abuse and against any unlawful access or use. In fact, the Directive 2006/24 did not lay down rules governing the extent of interference with the fundamental rights of data subjects in order to restrict it to what is strictly necessary. In adopting Directive 2006/24, the European Union's legislator had exceeded the limits imposed by the principle of proportionality in the light of Articles 7, 8 and 52 (1) of the CFREU – which is why the CJEU declared the invalidity of the directive, without reservations as to the temporal effects of its decision (efficacy *ex tunc*).

The decision of the CJEU raised the problem of the effects of that invalidity in relation to the national provisions transposing the directive which have since, been declared invalid. Some scholars suggested that the impact of the CJEU's decision on national law was unclear – since the Court had not given any indications in this particular case – yet the primacy principle and the consequent conformity of national rules with Union law should be complied with.[11] Other scholars adopted a traditional stance according to which the declaration of invalidity of the directive would not

[6] See Opinion of Advocate General Cruz Villalón delivered on 12 December 2013, judgment *Digital Rights Ireland*, C-293/12, recital 74.

[7] See Opinion of Advocate General Henrik Saugmandsgaard Øe delivered on 19 July 2016, judgment *Tele2*, joined cases C-203/15 and C-698/15, recitals 252 to 258.

[8] Judgment *Digital Rights Ireland*, April, 8, 2014, joined cases C-293/12 and C-594/12, recital 34.

[9] Judgment *Digital Rights Ireland*, cit., recital 33.

[10] Judgment *Digital Rights Ireland*, cit., recital 61.

[11] Franziska Boehm and Mark D. Cole, *Data Retention after the Judgement of the Court of Justice of the European Union*, 2014, p. 28 (https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf).

directly imply the invalidity of the national law that transposed it – insofar as the rules in question would come from different sources or separate legal systems –, although it would be necessary to evaluate the compliance of the national rules with Union law following the decision of the CJEU.[12]

In view of the difficulty of the problem, it is not surprising that, following the judgment in *Digital Rights Ireland*, two national courts (one Swedish and one British) have referred questions for a preliminary ruling of the CJEU in order to ultimately test the conformity of national systems that still impose a general obligation of retention of data on providers of publicly available electronic communications services. This judgment was published in December 2016.[13] In other words, by means of the questions referred for a preliminary ruling, the CJEU was asked to specify the consequences of the invalidity declared in *Digital Rights Ireland* for the national authorities and to determine whether a general obligation to retain data would be compatible with Article 15 (1) of Directive 2002/58 (concerning the processing of personal data and the protection of privacy in the electronic communications sector), in the light of Articles 7, 8 and 52 (1) of the CFREU. The cited Article 15 (1) of the Directive 2002/58 authorises Member States to adopt legislative measures for the retention of data for a limited period, subject to compliance with the general principles of the Union law and fundamental rights protected therein.

Thus, by way of preliminary ruling, the CJEU delivered the *Tele2* judgment in 2016, from which it can be concluded that *i*) the declaration of invalidity of the provisions contained in a directive inevitably affects the legal act of transposition of those provisions into the legal system of the Member States and *ii*) a Member State cannot rely on the Directive 2002/58 to enforce a generalised and undifferentiated obligation to retain traffic and location data following the declaration of invalidity of Directive 2006/24. It is therefore, urgent to draw conclusions from this recent ruling by the CJEU, which is all the more relevant because, in Member States where the transposed legislation continued to apply following the declaration of invalidity of Directive 2006/24 – as was the case in Portugal – many criminal convictions relied upon a potentially illegitimate access to data.

2. From the *Digital Rights* judgment to the *Tele2* judgment: implications for understanding the fundamental right to the protection of personal data

Despite being a landmark in the CJEU's case-law on the protection of fundamental rights – comparable, according to Steve Peers, to the classic judgments on civil rights of the US Supreme Court[14] – the *Digital Rights Ireland* judgment did not end the retention of data in the context of the Union,[15] especially since the

[12] Clara Guerra and Filipa Calvão, "Anotação ao Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014", *Forum de proteção de dados*, Comissão Nacional de Proteção de Dados 1 (2015): 79.
[13] Judgment *Tele2*, December, 21, 2016, joined cases C-203/15 and C-698/15.
[14] According to Steve Peers, "The data retention judgment: the CJEU prohibits mass surveillance", *EU law analysis*, 8 April 2014: "*Time will deal whether the Digital Rights judgment is seen as the EU's equivalent of classic civil rights judgments of the US Supreme Court, on the desegregation of schools (Brown) or criminal suspects' rights (Miranda). If the Charter ultimately contributes to the development of a 'constitutional patriotism' in the European Union, this judgment will be one of its foundations*" (http://eulawanalysis.blogspot.pt/2014/04/the-data-retention-judgment-cjeu.html).
[15] Niklas Vainio and Samuli Miettinen, "Telecommunications data retention after Digital Rights

CJEU considered that, while the retention of data imposed by Directive 2006/24 constituted a particularly serious interference with fundamental rights for the protection of privacy and the protection of personal data, it likely, did not affect the essential content of such rights.

In accordance with Article 52 (1) of the CFREU, any restriction on the exercise of the rights and freedoms set out therein must be *i*) provided for by law, *ii*) respect the essential content of those rights, *iii*) respect the principle of proportionality, and *iv*) be necessary for the pursuit of objectives of general interest recognized by the Union or for the protection of the rights and freedoms of third parties. However, in view of the fact that Article 1(2) of Directive 2006/24 did not allow the content of electronic communications to be known, the CJEU held that there was no compromise of the core of the right to privacy.

Furthermore, in the CJEU's view, Article 7 of Directive 2006/24 provided for compliance with the principles of protection and security of personal data, as long as Member States ensured that technical and organizational measures were taken against accidental or unlawful destruction, accidental loss or alteration of data – and therefore the core of the fundamental right to data protection would also be safeguarded.[16] However, even if the essential core was safeguarded, the legislation was disproportionate – this is the understanding of the CJEU that was the basis for the declaration of invalidity of Directive 2006/24.

In our view, it is not clear from the case-law of the European Court of Human Rights (ECtHR) that the general and undifferentiated nature of the retention of personal data by providers of electronic communications services (mass surveillance) is in line with the core of fundamental rights – especially because suspicion is not a necessary element for the justification of data retention. Nor is it in conformity with the constitutional traditions common to the Member States, namely when one takes into account the amount of unconstitutionality rulings of national rules issued by various constitutional courts of the Member States following the declaration of invalidity of Directive 2006/24 by the CJEU.[17]

In the ECtHR's judgment in the *S. and Marper v. The United Kingdom's case*,[18] for example, concerning the preservation of genetic profiles (DNA) or fingerprints of any person acquitted of the commission of a crime or whose proceedings have been closed without conviction, the ECtHR held that the retention of such data was contrary to the European Convention on Human Rights (ECHR), irrespective of the consideration of safeguards.[19] Furthermore, in the case of *Roman Zakharov v. Russia*,[20] which concerned the Russian system of interception of telephone communications, the ECtHR ruled that the automatic retention of irrelevant data for six months was not justified in the light of Article 8 of the ECHR (right to respect for private and

Ireland : legislative and judicial reactions in the Member States", *International Journal of Law and Information Technology*, v. 23, n. 3 (2015): 308.

[16] Judgment *Digital Rights Ireland*, cit., recital 38 to 40.

[17] On this theme, see Matthew White, "The new Opinion on data retention: does it protect the right to privacy?", *EU law analysis*, 27 July 2016 (http://eulawanalysis.blogspot.pt/2016/07/the-new-opinion-on-data-retention-does.html).

[18] Judgment *S. and Marper v. United Kingdom*, 4 December 2008, cases 30562/04 and 30566/04, recital 125.

[19] See Matthew White, "The new Opinion on data retention…", *cit.*

[20] Judgment *Roman Zakharov v. Russia*, 4 December 2015, case 47143/06, recital 255.

family life).[21]

In his Opinion in *Tele2*, the Advocate General took the same approach to the *Digital Rights Ireland's* ruling on the question of the inviolability of the central core of fundamental rights.[22] However, the Advocate-General is manifestly contradicting himself when he points out that "*the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications, as has been pointed out by Open Rights Group, Privacy International and the Law Society of England and Wales, as well as in a recent report by the United Nations High Commissioner for Human Rights*". In particular, the Advocate General adds, "'*metadata' facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not*".[23]

The Advocate General concludes that there is nothing theoretical about the risks of abusive or illegal access to retained data, as the risk must be linked to the extremely large number of requests for access referred to in the observations submitted to the CJEU.[24] Under Swedish law, Tele2 indicated that it received about 10,000 requests for access per month, a number that does not include requests received by other providers active in Sweden. With regard to the United Kingdom, excerpts from an official report mentioned 517,236 authorisations and 55,346 urgent oral authorisations were reproduced in 2014. In addition, the Advocate General acknowledges "*the risk of illegal access, on the part of any person, is as substantial as the existence of computerised databases is extensive*".[25] But if the justification for not affecting the essential core of the right to data protection lies mainly in the measures against accidental or unlawful destruction, accidental loss or alteration of the data, how is that compatible with the remarks above?

It is not hard to discern that the Advocate General avoids admitting that the general and undifferentiated retention of personal data is, *per se*, incompatible with the fundamental rights protected in the CFREU. He, therefore, concentrates on the safeguards which must go with a general obligation of retention of data in order to be compatible with the fundamental rights provided for by Union law – and not in what the Member States would be prohibited from doing in this field.[26] Regrettably, this kind of "headlong rush" is beginning to be usual in the handling of the matter – and it had also guided, in Judge Paulo Pinto Albuquerque's opinion, the decision-making of the ECtHR in *Szabó and Vissy v. Hungary*, on mass surveillance for reasons of intelligence and national security.[27]

---

[21] Commentating the decision of the ECtHR R*oman Zakharov v. Russia, cit.*, the Advocate General underlined, in his Opinion in *Tele 2*, cit., recital 243, that national regimes must lay down an obligation to destroy definitively any retained data once it is no longer strictly necessary in the fight against serious crime. He added that this obligation must be observed not only by service providers that retain data, but also by the authorities that have accessed the retained data.

[22] Opinion on *Tele2*, *cit.*, recital 156-159.

[23] Opinion on *Tele2*, *cit.*, recital 259.

[24] Opinion on *Tele2*, *cit.*, recital 260.

[25] *Idem.*

[26] See Matthew White, "The new Opinion on data retention…", *cit.*

[27] Judgment *Szabó and Vissy v. Hungary*, 12 January 2016, Application No. 37138/14, especially the recital 20 of the concurring opinion, in which Paulo Pinto Albuquerque denounces what he considers "*an illusory conviction that global surveillance is the deus ex machina capable of combating the scourge of global terrorism. Even worse, such delusory language obliterates the fact that the vitrification of society brings with it the Orwellian nightmare of 1984. In practice, the Chamber is condoning, to use the words of the European Parliament, 'the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law*

In any case, among the contradictions of the Advocate General in *Tele2*, perhaps the most perplexing would be the analysis of proportionality, *stricto sensu* of a general data retention obligation. This dimension was not considered by the CJEU in the *Digital Rights Ireland's* case because the Court held that the regime established by Directive 2006/24 exceeded what was necessary for the purpose of combating serious crime. According to the Advocate General, the requirement of proportionality *stricto sensu* arises both, from Article 15 (1) of Directive 2002/58, from Article 52 (1) of the CFREU and from settled case-law of the CJEU – and implies that a restriction of fundamental rights is to be regarded as proportionate only if the disadvantages caused by it are not disproportionate to the objectives pursued.

Thus, the requirement of proportionality *stricto sensu* imposes a balance between the advantages conferred by the measure in the light of the legitimate aim pursued (on the one hand) and the disadvantages which result from that measure to the fundamental rights enshrined in a democratic society (on the other). In other words, it imposes a balance between the advantages and disadvantages of a general data retention obligation applied to all European users without having a requisite of suspicion of serious crime – which would ultimately lead to a debate on the prevailing values and the kind of society in which we want to live.[28]

So, what was the solution proposed by the Advocate General, which was to be to the detriment of the homogeneity of European Union law? That such an evaluative assessment be returned to the national judge in the light of the mandatory safeguards laid down by the CJEU in Recitals 60 to 68 of the judgment in *Digital Rights Ireland*.[29] However, the CJEU did not accept the Opinion of the Advocate General and, in *Tele 2*, took strict proportionality as a basis in order to decide that the CFREU precludes national legislation from laying down, with the purpose of fighting serious crime, the widespread and undifferentiated retention of all traffic and location data of all registered users for all electronic means of communication.[30]

Thus, in answering in in more detail to the questions raised by the national courts in preliminary rulings, the CJEU ruled that Article 15 (1) of Directive 2002/58, in the light of Articles 7, 8, 11 And 52 (1) of the CFREU, must be interpreted as impeding national legislation governing the protection of traffic and location data, in particular the access of national authorities to the data retained *i*) without limiting such access to cases of serious crime and *ii*) without making such access subject to prior review by a court or an independent administrative authority, and; *iii*) without requiring that the data concerned to be kept within the territory of the Union.[31]

3. The *Tele2* judgment and the Portuguese legal system: is there anything new?

To better understand the stance of the CJEU and its implications for Portuguese

in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law-enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence".

[28] Opinion on *Tele2, cit.*, recital 246-248.

[29] Opinion on *Tele2, cit.*, recital 262.

[30] Judgment *Tele2, cit.,* recital 112.

[31] Judgment *Tele2, cit.*, recital 125.

national law, in particular as regards its material compatibility with European Union law, it is necessary to analyze some of the Recitals set out in the judgment.

The CJEU has not, from the outset, altered its position on the absence of a breach of the essential core of the fundamental rights at issue,[32] although it has acknowledged that we are still dealing with a wide and particularly serious interference with Articles 7 and 8 of the CFREU, in the sense that the retention of traffic and location data might convey to people a feeling of constant surveillance.[33] It also acknowledged that the retention of traffic and location data could influence the use of electronic means of communication and, therefore, the exercise of freedom of expression by users of such means, guaranteed by Article 11 of the CFREU.[34] For this reason, it is not surprising that the CJEU sees in this interference, a kind of exceptional instrument vis-à-vis the principles laid down in Directive 2002/58, namely the principle of confidentiality.

The CJEU also states that national rules which retain traffic and location data, affecting all persons using electronic communications, without any limitation or exception, including the existence of prior evidence that links, albeit indirectly, a particular person to a crime cannot be considered justified in a democratic society.[35] There should be limits to data retention and a relationship between the data retained and a threat to public safety should be demanded. Such limits may include, for example, the retention of data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime (or persons who could contribute, through their data being retained, to fighting crime).[36]

Can it be avowed that the Law No. 32/2008 of 17 July, which transposes Directive 2006/24 into the Portuguese national legal order, fulfills these requirements? Perhaps we could put forward the argument of the temporal limitation of the retention of traffic and location data. In fact, Article 6 of the aforementioned law limits to one year the period of retention of traffic and location data, counting from the date of completion of the communication. But this argument can be easily nullified. On the one hand, if we consider Recitals 59 and 64 *et seq*. of the judgment in *Digital Rights Ireland*, the CJEU had sustained the need for the existence of abovementioned limits and, in its view, those were not ensured even though Directive 2006/24, in Article 6, established a period of retention of data between six months and two years from the date of communication. It is, therefore, fairly evident that when the CJEU refers to the lack of temporal periods of data retention in Directive 2006/24, this might not contradict Article 6, as we are dealing with different dimensions of the problem. One thing is to know whether, in the case of data retention, what the period of retention should be. In this regard, the CJEU was clear in stating that the directive did not provide for objective criteria, in particular, depending on the type of data, in order to assess compliance with the principle of proportionality. A completely different thing is to demand that the data retention occurs only in a given time period. To reinforce this idea is the fact that, at the origin of *Tele 2*, *inter alia*, the question of a general obligation of data for only six months. A shorter time period, therefore, than that

[32] Judgment *Tele2, cit.*, recital 101.
[33] Judgment *Tele2, cit.*, recital 100.
[34] Judgment *Tele2, cit.*, recital 101.
[35] Judgment *Tele2*, *cit.*, recital 105.
[36] Judgment *Tele2*, *cit.*, recital 106.

provided for in Law 32/2008, but which did not prevent the CJEU from asserting its incompatibility with Article 15 of Directive 2002/58.

The key expression in this judgment, potentially fatal to Law No. 32/2008 in its current formulation, is "*targeted retention*". Law No. 32/2008 enforces the retention and transmission of traffic, location and related data of all natural and legal persons, without any limit or exception: the data subject has no possibility of opposition to its retention and transmission [Article 3 (4)], and there are no limits on "*categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted*".[37] In this respect, the CJEU is particularly clear about its objection to widespread "surveillance", thus requiring data retention, in particular, for the prevention of serious crime, to comply with what is strictly necessary.

Strictly necessary means for the CJEU that the Member States must lay down the introduction of clear and precise rules which contain *i*) objective criteria establishing a connection between the data to be retained and the objective pursued and *ii*) limit the extent of interference with fundamental rights. This second requirement implies, first, a restriction on the public affected by the retention measure, according to objective criteria, which may, for example, consist of "*geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences*".[38]

In short, "*Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication*".[39] In other words, if it were to be data retention consistent with Article 15 (1) of Directive 2002/58, it should be targeted and limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted.[40]

With this in mind, the legal-material incompatibility of Law No. 32/2008 with European Union law is evident. Following the *Digital Rights Ireland's* case, the reaction of the Member States was not consensual, which led to an unlawful differentiation of treatment between European citizens. According to the Portuguese Public Prosecutor's Office,[41] ten of the Member States of the European Union declared that national laws transposing the data retention directive were invalid, either by parliamentary decision or by their constitutional courts. In the other Member States, including Portugal, this was not the case because it was understood that the requirements of the CJEU's decision were previously met.[42]

According to Practical Note No. 7 of the Portuguese Public Prosecutor's Office, the common understanding, peacefully shared by the judicial community and the Portuguese telecommunications operators, is that Law No. 32/2008 was in force and valid. Allegedly because, in addition to the transposition of Directive 2006/24,

[37] Judgment *Tele2, cit.*, recital 108.
[38] Judgment *Tele2, cit.*, recital 111.
[39] Judgment *Tele2, cit.*, recital 112.
[40] These are cumulative requisites. See Judgment *Tele2, cit.*, recital 108
[41] Gabinete Cibercrime do Ministério Público. Nota Prática n.º 7 sobre retenção de dados de tráfego e Lei n.º 32/2008, 2015 (http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf).
[42] Niklas Vainio and Samuli Miettinen, "Telecommunications data retention after Digital Rights Ireland…", *cit.*, p. 301 ff.

that law introduced a broader regulatory framework for the data retention process (for example, among other things, the rules that should be observed on retention of data, persons empowered to access data or the conditions of storage and access to data). Therefore, in the opinion of the Portuguese Public Prosecutor's Office, the national law had gone far beyond the requirements of the Directive and most of the requirements that came to be made by the CJEU ruling would already have been previously considered in domestic law.[43]

Yet the competence to correct errors and to regulate the matter in accordance with the judgment of the CJEU is not of the Portuguese legislator – it is of the European legislator.[44] That is precisely so, in order to avoid the schizophrenic result whereby, in the context of European competence, citizens of another Member State other than Portugal, who are not suspects of a crime, are no longer subject to the retention of their personal data after the *Digital Rights Ireland's* judgement, and the Portuguese still are. This undermines the effectiveness of European Union law, undermines the uniformity of its application in the different Member States and leads to unjustified differences of treatment between European citizens in the protection of their fundamental rights.

The disparity between the Member States following the declaration of invalidity of Directive 2006/24 suggests that there are serious divergences between the applicable European Union law – which is incompatible with the idea of an Union based on the rule of law. In this context, if the Portuguese courts had doubts as to the continued application of Law No. 32/2008, a dialogue with the CJEU was required by way of preliminary ruling in order to; *i*) disclose the scope or consequences of declared invalidity and; *ii*) to exclude the risk of misinterpretation or breach of European Union law.[45] At the very least, the proceedings should have been suspended on the ground that the CJEU was dealing with two references for a preliminary ruling on the subject[46] – for which the Portuguese authorities could not plead lack of knowledge because, under Article 21(4) of the Rules of Procedure Of the Court of Justice, a notice is published in the Official Journal of the European Union giving an account of the questions referred to the Court and the Portuguese State is notified for the submission of written statements or observations under Article 96 (1) (b) of the Rules.

However, contrary to the CJEU's decision, the Portuguese Public Prosecutor's Office's Practical Note No. 7 states that the Court's decision imposes "*conditions that are not viable or that, if applicable, render the retention useless.*" In this sense, it is defended that data retention, as understood in the framework of Directive 2006/24 and Law No. 32/2008, is only useful if the data refers to all citizens in an indiscriminate

[43] For an analysis of the contradictions between the Law No. 32/2008 and the European Union law, see Clara Guerra and Filipa Calvão, "Anotação acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014", *cit.*, p. 81-82.

[44] See Outcome of the 3528th Council meeting (Justice and Home Affairs), Brussels, 27 and 28 March 2017, Council of the European Union (http://www.consilium.europa.eu/en/meetings/jha/2017/03/st07688_en17_pdf): "*The presidency informed ministers on the ongoing work towards facilitating a common reflection process at EU level in light of recent European court of justice case-law. The presidency intends to work in a specific working group format to hold discussions on the requirements of the relevant judgements, to exchange best practices and to analyse what is needed for the purposes of criminal proceedings related to the availability of certain types of data. The reflection process in the Council will also allow for synergies with the work undertaken by the Commission to provide guidance on bringing national data retention laws into line with the Tele 2 Judgment.*"

[45] Judgment *Ferreira da Silva*, 9 September 2015, C-160/14, recital 44.

[46] Joined cases C-203/15 and C-698/15.

manner, as "*at the time when the data is retained and preserved, it is not possible to know whether such data may be necessary as evidence of a crime. Only after a crime has occurred will the data, however, retained in a generalised and indiscriminate manner assume probative value*".

However, it is clear from the judgment in *Digital Rights Ireland* that the Portuguese Government, in its written observations to the CJEU, considered that the effectiveness of the regime for the collection of traffic and location data imposed by Directive 2006/24 was to some extent limited, in particular, in relation to organized crime and terrorism, due to the existence of several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication and thus, circumvent state surveillance. This limits the ability of the data retention measure to attain the objective pursued.[47] If that is the case, why should we subject Portuguese citizens who are not suspects of committing a crime to a permanent and indiscriminate surveillance? How can we justify creating the feeling that their private life is being constantly monitored?[48]

These doubts were certainly amplified by *Tele2*. Even if we recognize the importance and usefulness of the retention of traffic data for the objective of identifying the alleged perpetrator of a particular crime, which presupposes, in the words of Portuguese Public Prosecutor's Office's, a retention of data that is generalised and indiscriminate, one cannot simply choose to continue to disregard the European Union law, as if it were a strange and foreign *corpus* in face of the Portuguese national law. It is of particular gravity that the Portuguese legal community remains relatively oblivious to this problem, in a matter as sensitive as this, of infringement[49] of what is established not only in the decisions *Digital Rights* and *Tele2*, but especially in view of the fundamental rights enshrined in the CFREU.

We have no doubts that Law No. 32/2008 was, in certain elements, a step forward in the protection of citizens' fundamental rights, for example, the conditions for access to data in Portugal are particularly demanding, since there is a prior judicial control;[50] the obligation to destroy data at the end of the retention period or retention order of the court [Article 7 (1) (e) and (f)];[51] the attention given to the protection of professional secrecy.[52]

However, it cannot be concluded without further ado that the Portuguese law went beyond the requirements of the directive. Among the normative complexity of the Portuguese law, we find solutions, such as those mentioned above, which

---

[47] Judgment *Digital Rights Ireland, cit.*, recital 50.

[48] Judgment *Digital Rights Ireland, cit.*, recital 37.

[49] Upheld in the Practical Note No. 7 of the Portuguese Public Prosecutor's Office.

[50] The CJEU also analysed this question in the *Tele2's* judgment, asserting that "*Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union*".

[51] On this possibility, retaining data beyond the one year period established by Article 6, the Practical Note No. 7 does not address. In fact, according to Article 7 (1) (e) and (f), the destruction of the retained data might not occur as soon as the retention period ends. If the court considers the data relevant for the investigation it can order its preservation, as long as it is strictly necessary, until one of the following happens: an accusation is not filled; acquittal of the accused; prescription of criminal procedure; or amnesty [Article 11 (1) (2)].

[52] See Article 9 (4).

undoubtedly respect the fundamental rights protected by the European legal order. But it is also clear that since the *Digital Rights'* case, other measures, such as widespread and undifferentiated retention, have fallen short of the CJEU's understanding of what is strictly necessary, even if Portuguese law only allows the transmission of data relating to a suspect or accused person, intermediary or to the consenting victim of a crime.[53] Transmission of data only happens if there was a previous retention of data, which is enforced by fines ranging from EUR 1500 to EUR 50 000 or from EUR 5000 to EUR 10 000 000 depending on whether the agent is a natural or legal person.[54]

All that remains for us is, as a legal community that is part of the European Union's *corpus iuris,* to reflect and draw urgent conclusions from the path established by the CJEU.

[53] See Article 9 (3).

[54] Following the Deliberation No. 641/2017 of 9th May 2017, where it recommend an amendment to the Law No. 32/2008 due to the violation of article No. 52 of the CFREU and article No. 18(2) of the Portuguese Constitution, the CNPD (the Portuguese National Commission for the Protection of Data) took a step further with the Deliberation 1008/2007 of 18th July 2017. Taking into account the *Digital Rights Ireland Ltd* and *Tele2* judgements as well as the Deliberation 641/2017, the CNPD stated that it would not appreciate any complaints resulting from the violation of the Law No. 32/2008. In practical terms, considering that the CNPD holds the power of investigation and punishment of administrative offenses arising from the violation of legal norms of this legal instrument, this means that the providers of publicly available electronic communications services or of a public communications network will no longer be liable for not retaining traffic data, location data or related data necessary to identify the subscriber or user.