Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'

Milaj, Jonida; Kaiser, Carolin

Published in:
International Data Privacy Law

DOI:
10.1093/idpl/ipx002

Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'

Jonida Milaj* and Carolin Kaiser**

Key Points

- The new Anti-money Laundering Directive aims to prevent the crimes of money laundering and terrorist financing in the European Union (EU) and introduces requirements for collecting and retaining personal data from customers of financial systems.
- This article evaluates the proportionality of the data retention requirement in light of the protection of the rights to privacy and personal data of the individuals, taking as a standard for evaluation the reasoning of the Court of Justice of the EU in the *Digital Rights Ireland* case.
- We submit that in light of a human rights guided approach the legislator must follow the logic of 'need to know' instead of the one of 'nice to know' when interfering with the individual's rights to privacy and data protection.

Introduction

The fourth Anti-Money Laundering (AML) Directive[1] was adopted in June 2015, and in July 2016, a little more than one year after the adoption, the procedures for amending it again were initiated.[2] As stated in Article 1(1), the AML Directive aims to prevent the use of the financial system in the Member States for the purposes of two well defined and relatively new crimes, money laundering and terrorist financing. It applies to a range of entities, including credit institutions, financial institutions, auditors, accountants, tax advisors, gambling operators, as well as to other legal and natural persons trading in goods, to the extent that payments are made or received in cash in an amount of EUR 10 000, regardless of whether payments are made in a single, or via a series of transactions that appear to be linked. While at this early stage, it is difficult to assess if the AML Directive will help to reach the set goal of preventing that the financial system in the Member States is used for money laundering and terrorist financing, it may assist the detection, investigation, and prosecution of these crimes. The Directive brings into force new requirements for customer due diligence, supported by increased obligations to report suspicious transactions and the duty to retain certain categories of personal data.

This article assesses the proportionality of the data retention requirement in the AML Directive, as it affects the entire European population independent of any existing connection with the two crimes that the Directive aims to fight. The reasoning of the Court of Justice of the EU (CJEU) in the case *Digital Rights Ireland*,[3] in which the court invalidated the Data Retention Directive (DRD),[4]

* PhD Researcher, STeP - Security, Technology & e-Privacy Research Group, Department of European and Economic Law, Faculty of Law, University of Groningen, P.O.Box 716, 9700 AS Groningen, The Netherlands, Email: j.milaj-weishaar@step-rug.nl

** PhD Researcher, STeP - Security, Technology & e-Privacy Research Group, Department of European and Economic Law, Faculty of Law, University of Groningen, P.O.Box 716, 9700 AS Groningen, The Netherlands, Email: c.kaiser@step-rug.n

1 Dir (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Dir 2005/60/EC of the European Parliament and of the Council and Commission Dir 2006/70/EC (Text with EEA relevance) OJ L 141, 5 June 2015, 73–117.

2 COM (2016) 450: Proposal for a Directive of The European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Dir 2009/101/EC.

3 Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others [2014] nyr.

4 Dir 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 Dir 2002/58/EC. OJ L 105/54, 13.4.2006

will serve as the standard by which the proportionality of the AML Directive is to be measured. The elaboration is inspired by a human rights-based approach, which sets out that measurable goals must be reached by applying human rights standards. According to this approach, while the fight against the crimes of money laundering and terrorist financing is certainly in the public interest, it must not interfere with the fundamental rights to privacy and data protection of individuals beyond what it is strictly necessary and proportionate. We submit that due to the interference with the fundamental rights to privacy and to data protection, any collection and retention of personal data must be justified as 'needed to know' rather than simply 'nice to know'.

After this introduction, Section 'Background information about the crimes of money laundering and terrorist financing in the EU ' contains some background information on the crimes of money laundering and terrorist financing. Section 'The AML Directive and the concerns for the protection of the rights to privacy and data protection' presents the data retention duties in the AML Directive and the concerns connected to the protection of the rights to privacy and data retention of individuals. The following Section 'Data retention in Europe—the invalidation of the DRD' presents the current status of data retention in the EU and the reasons that led to the invalidation of the DRD. In Section 'The proportionality of the data retention requirement in the AML Directive', the proportionality of the data retention requirements in the AML Directive is analysed in light of the reasoning of the CJEU in *Digital Rights Ireland*. The conclusions of the analyses are presented in Section 'Conclusion'. We will argue that the large scale of data collected and retained on the basis of the AML Directive is disproportionate and infringes the rights to privacy and data protection of the European citizens.

Background information about the crimes of money laundering and terrorist financing in the EU

Money laundering and terrorist financing are, compared to the general body of criminal law in Europe, rather new offences. In most European countries, they were not made a criminal charge until the 1990s, and only after considerable international political pressure and against much resistance.[5] Both crimes are discussed further.

Money laundering

To begin with a very elementary definition, money laundering is hiding the illicit origins of funds in such a way as to make them appear legal. The exact definition and scope of what money laundering means varies in the Member States to some degree, but the essential points of AML legislation are brought into uniformity by the AML Directive of the European Union (EU). The European legislator has included a definition of money laundering in Article 1(3)(a–d) of the Directive, according to which there are four different modes of intentional conduct which fall under the term money laundering. First, money laundering is defined as 'the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action'. Secondly, also 'the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity' must also be considered an act of money laundering. Furthermore, the definition of money laundering includes the possession or use of property if the individual is aware of the criminal origin of that property.[6] Finally, any help provided to perpetrators of money laundering is also to be regarded as a criminal offence.[7] According to paragraph 4 of the same provision, a Member State has jurisdiction over the investigation of a money laundering case even if the predicate offence from which the property in question was derived, itself does not fall under the jurisdiction of the same Member State. This definition is clearly very broad. There are still some differences in how money laundering is handled as an offence in national criminal law, as criminal law is hardly harmonized through legislation on the European level. The Directive does, however, set out a detailed minimum standard for this particular crime, to which all Member States must adhere.

5 See for example G Arzt, 'Geldwäscherei – eine neue Masche zwischen Hehlerei, Strafvereitelung und Begünstigung', NStZ 1990, 1, 1ff.

6 Art 1 (3) (c) of Dir 2015/849.

7 Art 1 (3) (d) of Dir 2015/849.

Money laundering essentially consists of three steps: placement, layering, and integration.[8] In the placement stage, the funds are first placed in a certain context, after which, in the layering stage, as much distance is put between the funds and their illicit origin as possible. The goal of the layering stage is that the link between the funds and the predicate offence can no longer be established or proven. Once the money launderer is satisfied that the origin of the funds is sufficiently concealed, the third stage, integration, follows, in which the funds can be legally integrated into the economy and used to the financial advantage of the criminal.

This short outline of the three stages shows that money laundering is not necessarily a very simple thing to do. Often, an international construct of shell companies is established, and the funds are moved between several different countries strategically chosen for their favourable laws, in terms of banking secrecy and police cooperation in criminal matters. Such structures are naturally very difficult to design and expensive to execute and maintain, and equally difficult and expensive for investigators to follow up. The increasing sophistication of the money laundering schemes and the inability of the prosecution to set aside sufficient resources to investigate into such constructions caused legislators to take a radical step with the AML Directive and for the first time to burden financial institutions with investigative duties.

At the beginning of every money laundering offence stands another crime, in which property was procured. Those so-called predicate offences can be of widely different natures, from drug-related offences to corruption and tax fraud. Precisely which offences can be predicate offences to money laundering is to some degree up to the Member States, but the AML Directive contains minimum requirements. According to Article 3(4), at least all crimes related to terrorism as defined in Articles 1–4 of Framework Decision 2002/475/JHA,[9] drug-related crimes as listed in Article 3(1)(a) of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988,[10] and organized crime as set out in Article 1 of Council Joint Action 98/733/JHA[11] must be included as predicate offences. Furthermore, serious 'fraud affecting the Union's financial interest' and corruption are covered. Lastly, and most broadly, all crimes with a punishment of deprivation of liberty over a certain threshold must be included. There are two possible thresholds, depending on the organization of the Member State's criminal law. If minimum thresholds for punishments are defined, all offences punishable with a prison sentence of 'a minimum of more than six months' must be covered, or, where maximum punishments are defined, all offences punishable with a prison sentence 'for a maximum of more than one year' are included. This way, all serious crimes should be covered as possible predicate offences to money laundering.

Predicate offences are so important because naturally, only property of a criminal origin needs to be and can be laundered. There must, therefore, be a causal link between the crime and the funds in question. That such a link is often difficult to establish goes without saying, as does the fact that there can often be considerable difficulties to establish the predicate offence. After the commission of a predicate offence, the criminal finds himself in possession of a large amount of property, the origin of which he cannot reasonably explain to the authorities. The appearance of a sudden and unaccountable fortune is bound to cause suspicion and raise questions, and possibly lead to the discovery of the predicate offence. Therefore, the unlaundered proceeds of a crime are difficult for a criminal to actually use for his own benefit. The funds must thus be laundered before they can be used.

Terrorist financing

Apart from money laundering, the second crime that is to be fought with the help of the AML Directive is the financing of terrorism. According to Article 1(5) of this Directive:

> 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA.[12]

8 For a more detailed description of these stages, please consult FG Madsen, *Transnational Organized Crime* (Routledge 2009) 106 ff.

9 Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22 June 2002, 3–7.

10 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 20 December 1988, United Nations, Treaty Series, vol 1582, 95.

11 98/733/JHA: Joint action of 21 December 1998 adopted by the Council on the basis of art K.3 of the Treaty on EU, on making it a criminal offence to participate in a criminal organisation in the Member States of the EU, OJ L 351, 29 December 1998, 1–3.

12 Council Framework Decision (n 9) 3–7

Articles 1–4 of that Decision list all possible offences connected to terrorism, including any kind of support rendered to a terrorist group, and the different acts of terrorism that can be committed by a group or by an individual. Thus, any intentional attempt to channel funds towards the support of terrorist organizations or individual terrorists and acts of terrorism is covered by this definition.

The crime of terrorist financing is close to the one of money laundering, because very similar constructs as those which are built for the purposes of money laundering can also be designed to channel funds to terrorist organizations. In a money laundering operation, money of an illicit origin is moved through convoluted channels to ultimately arrive back with the criminal. In contrast, a terrorist financing operation moves funds of often perfectly legal origins to an illicit recipient. Therefore, in a money laundering scheme, the origin of the funds must be concealed, while in a terrorist financing scheme, the destination of the funds must be hidden. Apart from this opposite direction of movement, the operations often work in a very similar way as far as the movement of funds is concerned.

The AML Directive and the concerns for the protection of the rights to privacy and data protection

This section presents the way the crimes of money laundering and terrorist financing are addressed in the AML Directive. It is obvious that the investigations into such sophisticated clandestine money transfer operations are very difficult for law enforcement agencies on the international level and particularly, on the national level. An adequate response by the police force would require unprecedented investments in training and funding of investigating units. Instead, the Directive shifts the task of investigating financial movements on to the providers of financial services. In such a framework, the providers of financial services serve as an arm of the law enforcement agencies and collaborate in the field of prevention, detection, investigation, and prosecution of crime.

The entities covered by the Directive are manifold. In principle, all legal and natural persons who, in the course of their professional activities, deal with large amounts of money, are required to apply AML safeguards (Article 2(1)(a)–(f)). In the first place, this concerns banks and companies providing other financial services, but the Directive also covers casinos, lawyers, real estate agents, and any merchant, whenever the merchant accepts a payment of EUR 10,000 or more in cash. The personal scope of the Directive is thus very broad. All those subjects are now charged with a number of duties aimed at minimizing the risk that their services are abused for money laundering purposes.

The first group of duties concerns the assessment of the identity of the customer. Any customer must be identified before the start of the business relationship (Articles 11–13). This also means that any person unwilling or unable to provide a valid identification document is excluded from the services provided by the obliged entities. Secondly, the customer's transactions are subject to uninterrupted scrutiny and monitoring by the obliged entity (Article 13 (1) (d)). That means, for example, that any financial transaction carried out by a bank for a customer must be examined to exclude as far as possible the risk of money laundering for that particular transaction. If any transaction raises a suspicion of money laundering with the obliged party, it must report to the Financial Intelligence Unit (FIU) (Article 33). FIUs are established in each Member State (Article 32) whose task it is to carry out, oversee, and coordinate efforts to prevent, detect, and combat money laundering and terrorist financing operations. There are no official guidelines on how the monitoring must be conducted, and each bank has developed its own programmes which are to identify which patterns or keywords are to be considered 'suspicious'. The customer is not informed if any of his transactions were flagged as suspicious, nor if his personal data is communicated to the FIU (Article 39). Lastly, a copy of the identity documents of the customer and records of the transactions must be stored by the obliged entity for five years after the end of the business relationship with the customer (aArticle 40(1)(a) and (b)). This retention period may be extended by national law to up to 10 years in total (Article 40(1)).

The data retained on the basis of the Directive raise concerns for the protection of the rights to privacy and data protection of the individuals. The large amount of data in a person's transaction history in fact allows an intimate insight into that person's daily life and habits, especially if it is unpurged of unsuspicious transactions. The transaction history will contain information on the customer's wages and where he is employed, or if he receives social benefits. Rent or mortgages are included in the transaction history. The records may show when and where the person does his grocery shopping. He

might have monthly debits from a tennis club or a standing order to pay pocket money to children. Some information that can be deduced from a person's transaction history might concern information that are very private, and touch upon the categories of sensitive information, such as a person's health, political opinion, or religious denomination, information which in principle must not be processed at all.[13] For example, there may be monthly debits from a political party or donations to a religious organization. An individual might pay high medical bills each quarter. He may spend some money each Saturday evening at a local sex club or gay bar. Such information clearly has a connection to a person's health, sex life, and political opinions or religious persuasion. Therefore, although the Directive respects the principle of purpose limitation (Article 41(2)), the indiscriminate retention of all transaction data creates a serious interference with the private life of individuals and with their right to data protection.

Finally, it should be mentioned that the Directive does allow for some gradations in how strictly these surveillance measures must be applied. The Directive demands risk assessments to be carried out on Community, Member State, and individual business level, and where lower risk was identified, a 'Member State may allow obliged entities to apply simplified consumer due diligence measures' (aArticle 15(1)). However, the Directive gives insufficient information about what such simplified measures should look like. The only basic boundary defined by the Directive is spelled out in Article 15(3) which obliges Member States to 'ensure that obliged entities carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions'. The ongoing monitoring of all transactions can therefore not be substantially decreased in scope or extent.

The following section elaborates on the DRD and the reasoning that brought the Court of Justice of the EU (CJEU) to invalidate it. This reasoning is subsequently applied in assessing the proportionality of the data retention requirements in the AML Directive.

Data retention in Europe—the invalidation of the DRD[14]

As a general rule, personal data should be retained in the EU only for the period of time that is necessary for the purpose of processing.[15] In the area of law enforcement, Member States are required to provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for storage of personal data.[16]

Specific rules on data retention are contained in various laws. One of these specific laws was the DRD, adopted by the European legislator in 2006.[17] Its aim was to enable law enforcement authorities to use for the purpose of investigation, detection, and prosecution of serious crimes data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[18] Essentially, providers of fixed and mobile telephony services and Internet service providers were required to retain the records of users of the service to trace and identify the source, destination, date, time, and duration of a communication together with information necessary to identify the type of communication, the equipment used, and the geographical location of the user.[19] All this metadata was to be kept according to the time limit set by national law, with a time margin between 6 and 24 months.[20] The data was in this case, therefore, not retained for a specific and limited known purpose but rather in a general and continuous manner.

Data collection and retention on the basis of the DRD interfered simultaneously with the rights to privacy and data protection.[21] It is clear that a lot of information on the private life of an individual can be gathered by processing personal data. In the case of the DRD, the data could reveal the contacts of an individual, how often he communicates with them, from

13 Art 8(1) of Dir 95/46/EC, included also in art 9(1) of the new General Data Protection Regulation 679/2016/EU.

14 This section has taken its starting point from J Milaj, 'Invalidation of the Data Retention Directive - Extending the Proportionality Test' (2015) 31(5) Computer, Law and Security Review 604.

15 Art 6(1)(e) of Dir 95/46/EC, included also in art 5(1)(e) of the new General Data Protection Regulation 679/2016/EU.

16 Art 5 of Dir 2016/680.

17 Dir 2006/24/EC of the European Parliament and of the Council (n 4) OJ L 105, 13 April 2006, 54–63.

18 For a detailed presentation of the reasons for the introduction of the Data Retention Directive please see: JP Mifsud Bonnici, 'Recent European Union developments on data protection . . . in the name of Islam or "Combating terrorism" ' (2007) 16(2) Information & Communications Technology Law 161; MH Maras, 'While the European Union was Sleeping, the Data Retention Directive was Passed: The Political Consequences of Mandatory Data Retention' (2011) 6(2) Hamburg Review of Social Sciences 1.

19 Art 5 of the Data Retention Directive.

20 Art 6 of the Data Retention Directive.

21 Joint Cases C-465/00, C-138/01 and C-139/01 Rundfunk, para 75.

whom someone seeks advise, how often, etc. The potential use of the data without informing the person concerned made this interference particularly serious as '. . . it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[22] Data retention thus turns surveillance into a normal situation, a rule rather than an exception. At a time when new technologies have the potential to make collection and retention of data easier than ever to perform,[23] it is important to identify the reasons on the basis of which the CJEU invalidated the DRD.

Digital Rights Ireland reached the CJEU as a request for a preliminary ruling. Two cases had reached the High Court of Ireland and the Constitutional Court of Austria, and those courts found that the cases in question concerned the interpretation of European law, to which the CJEU is exclusively entitled.[24] The CJEU alone has the authority to decide on the validity of EU law, such as the DRD. Therefore, national courts can in uncertain cases request a preliminary ruling from the CJEU, and decide on the merits of the case only after receiving the CJEU's interpretation of the relevant European law aspects. In the case concerning the DRD, the High Court of Ireland had to adjudicate a dispute between the Irish company Digital Rights Ireland and the Irish authorities on the legality of national measures implementing the retention of data of electronic communications. The Austrian Constitutional Court similarly had before it several actions filed by a large number of applicants seeking the annulment of the Austrian telecommunications law that transposed the DRD into national law. For deciding each case nationally, a decision of the CJEU on the validity of the DRD was required.

In its ruling, the CJEU invalidated the DRD on the basis of its serious interference with Articles 7 and 8 of the Charter of Fundamental Rights of the EU, and for exceeding the limits imposed by the principle of proportionality.[25] In its elaboration, the CJEU first identified the existence of the interference with the protected rights, and then examined the possible justification for such an interference.[26] The court considered the data retention requirement to genuinely satisfy an objective of general interest, namely the fight against serious crime. It has to be noted, however, that although the court did find an interference with the rights to privacy and data protection, it did not consider the essence of both rights to be adversely affected. In this way, the CJEU allowed for the possibility for other special rules on data retention in the EU, provided that they comply with the proportionality principle.

To assess the proportionality of the interference, the CJEU applied a proportionality test composed of three steps, as established in its earlier case law:[27] (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu*.[28] In the first step, the CJEU established that the measures are appropriate for attaining the objectives of the Directive.[29] The focus of the analyses was on the value that the retained data can have for national authorities, giving them additional opportunities to investigate into serious crime. Data retention methods are, therefore, evaluated as valuable for criminal investigation. The CJEU discussed afterwards jointly the second and the third step of the test. For this the CJEU referred to its previous decision in the *IPI*[30] case and used the formula stating that '. . .derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary'. The test used by the CJEU follows an *ex post* approach focusing on the existence of clear and precise rules to govern the scope and application of the measure and the existing minimum safeguards introduced against the risk of unlawful access and use of personal data.

The detailed reasons on the basis of which the CJEU established the disproportionality of the DRD and invalidated it are discussed below. The CJEU looks first at the scale of the interference, than at substantive concerns for the access to the data from national authorities and finally at technical concerns, on the requirements for the service providers. Each reason is discussed in turn:

Scale of surveillance

The DRD covers all persons, all means of electronic communication, and all communications metadata. It interferes, therefore, with the fundamental rights of the entire European population. The Directive, therefore,

22 Joint Cases C-293/12 and C-594/12 (n 3) para 37.

23 G Marx , 'What is new about "New surveillance"? Classifying for change and continuity' (2002) 1(1) Surveillance and Society 9.

24 E Guild and S Carrera, 'The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive' (2014) CEPS Paper in Liberty and Security in Europe, No 6, 1–18; O Lynskey, 'The Data Retention Directive is Incompatible with the Rights to Privacy and Data Protection and is Invalid in its Entirety: Digital Rights Ireland' (2014) 51 Common Market Law Review 1789.

25 Art 52(1) of the Charter of Fundamental Rights of the EU.

26 MP Granger and K Irion 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39(4) European Law Review 835.

27 *Case 11/70 Internationale Handelsgesellschaft v Einfuhr- und Vorratsstelle Getreide* [1970] ECR1125.

28 A Troncoso Reigada, 'The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The Biometric Data Processing' (2012) 17.2 Lex Electronica 1.

29 Joint Cases C-293/12 and C-594/12(n 3) para 49.

30 *Case C-473/12 Institut professionnel des agents immobiliers (IPI) v Geoffrey Engelbert*, Immo 9 SPRL, Gregory Francotte [2013] nyr.

has the form of mass surveillance, where no exceptions are provided for persons concerning whom there is no evidence suggesting that their conduct might have a link with a serious crime, or for persons whose communications are subject to professional secrecy. In addition, the provisions of the DRD have failed to establish any relationship between the retained data and threat to public security and no restriction was provided with regards to a time period, geographical area, or group of people. There was no limitation of data retention to persons whose data could contribute to the prevention, detection, or prosecution of serious offences.[31]

The scale of surveillance was so disproportionate that it would have sufficed for the CJEU to invalidate the DRD for infringing the right to privacy. The CJEU, however, goes further in its elaboration by assessing the data access from national authorities as well as the requirements for the service providers. This gives the impression that the scale of surveillance in itself does not suffice for establishing the disproportionality of the data retention measure.

Substantive concerns for the access to the data by national authorities[32]

The DRD failed to lay down any objective criteria that could serve to determine the limits of the access of the competent national authorities to the retained data and their subsequent use. The Directive did not contain any substantive and procedural conditions to the access and subsequent use of the data, nor did it provide that these procedures were to be restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto. The data retention period was not established on the basis of objective criteria for categories of data, and it was not ensuring its limitation to what is strictly necessary.[33] In addition, the DRD did not provide for judicial or independent administrative body review whose decision would seek to limit access to the data to what is strictly necessary. This was left to the discretion of the Member States.

Technical concerns on the requirements for service providers[34]

Another reason for establishing the disproportionality of the DRD was that it did not introduce any particular level of data security for the service providers, but instead provided for the possibility to take economic considerations into account when determining the level of data security that they apply. In addition, there were no special requirements for the service providers to retain the data within the territory of the EU. This can be especially problematic when a cloud service provider operates outside the jurisdiction of the EU, as the data protection standards can vary significantly between states, particularly outside the EU, and therefore a high level of data protection cannot always be guaranteed.

As mentioned above, the invalidation of the DRD does not mean that data retention is no longer allowed anywhere in Europe. The decision did not even have as a result the automatic invalidation of national rules on the subject.[35] A new decision from the CJEU was needed to extend the reasoning of the CJEU for invalidating the Directive also to national legislation.[36] At this time, some Member States have still in life their data retention regimes, despite the fact that they were adopted to implement the now invalidated DRD.[37] Other Member States have invalidated their rules[38] and others have introduced or are in the process of introducing new, amended data retention laws.[39] The reasoning of the judgment already showed, however, that the CJEU will not satisfy itself with anything less than a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, independent of the legitimacy of the objectives pursued by the EU legislature and with the existence of adequate safeguards at EU rather than at Member State level.[40] This assessment was confirmed by the CJEU in its *Tele2 Sverige* judgment, in which it evaluated the national data retention laws of Sweden and the UK.[41]

The reasoning of the *Tele2 Sverige* judgment of the CJEU is in large parts identical to its *Digital Rights*

31 Joint Cases C-293/12 and C-594/12 (n 3) paras 56–57.

32 Ibid, paras 58–65.

33 Ibid, para 64.

34 Ibid, paras 67–69.

35 European Commission (2015) Statement/15/5654 on national data retention laws, 16 September 2015.

36 Joined cases C-203/15 and C-698/15 Tele2 Sverige [2016] nyr, para 112.

37 EDRi (2015) Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling <https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702_annex.pdf> (last accessed 11 February 2016).

38 For the Netherlands see: ECLI:NL:RBDHA:2015:2498 Rechtbank Den Haag 11 maart 2015 (Stichting Privacy First and others de Staat der Nederlanden); for France see: Arrêt no 84/2015 du 11 jeun 2015.

39 For the UK see: Data retention and Investigatory powers act 2014; for Germany see: C Reichert, 'Germany Moves Closer to Data Retention', in ZDNet, 19 October 2015 <http://www.zdnet.com/article/germany-moves-closer-to-data-retention/> (last accessed 11 February 2016).

40 Council of the EU 9009/14 LIMITE, Information note from the general Secretariat of the Council to the Permanent Representatives Committee/Council, Brussels, 5 May 2014 <http://www.statewatch.org/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf> (last accessed 21 November 2016).

41 Joined Cases C-203/15 and C-698/15 (n 36).

Ireland judgment. However, as the *Digital Rights Ireland* judgment concerned a directive, it will be used as a blueprint to assess the proportionality of the AML Directive, rather than the *Tele2 Sverige* judgment, which concerned national laws. The proportionality of the data retention requirement in the AML Directive is, therefore, to be assessed in the following section the light of the CJEU's ruling.

The proportionality of the data retention requirement in the AML Directive

As seen in the previous section, although data retention for law enforcement purposes is in principle seen as an appropriate means for the purposes of prevention, detection, investigation and prosecution of criminal activities, it is still subject to a proportionality and necessity evaluation. Even though the application of the principle of proportionality might differ in a case by case situation,[42] and there is no clear definition of what is to be understood under the term 'necessity' in EU law,[43] both principles doubtlessly aim to reduce data collection (and retention) activity to what it is 'needed to know' instead of what it is 'nice to know'. This would mean that personal data must be collected and retained only in very specific cases and on the basis of specific rules.

In contrast to the DRD, the transactions retained on the basis of the AML Directive are collected for a clearly specified purpose—the fight against two criminal offences, namely money laundering and terrorist financing. The fight against both crimes are considered as important public interests.[44] In addition, it is also clear that the retained data in themselves can serve as evidence for the investigation and detection of the said crimes. There is thus no doubt that the retention of the data is an appropriate measure for assisting law enforcement authorities engaged in the fight of these criminal activities. The question raised, however, is whether the AML Directive is limited in such a way as to comply with the proportionality and necessity test, and if there are enough safeguards for the individuals into whose private sphere is intruded. Such a question was anticipated by the drafters of the Directive, who expressly state in recital 64 that the Directive does observe the proportionality standard of Article 5 of the Treaty on the EU and 'does not go beyond what is necessary in order to achieve that objective'. However, we will argue below that the Directive does not deliver what it promises, by focusing on the proportionality of its provisions regarding the data subjects, the collected data, and the period of data retention.

The data subjects

The data subjects, according to the AML Directive, are all individuals who carry out financial transactions through their bank accounts. Everyone's transaction data are indiscriminately retained and there are no exceptions for any particular groups of data subjects.

How far reaching this surveillance is becomes clear, when it is recalled to mind how essential financial services are to the average European. According to the World Bank, only 6 per cent of adults in the high-income OECD countries were unbanked in 2014[45] (22 of the OECD's 35 Member States are EU Member States). It can thus be estimated that 94 per cent or more of all adults in the EU are served by the banking system. In addition, all financial service providers other than banks are covered by the AML Directive, as well as a large number of other professions. Therefore, it can be stated that no member of society in Europe is not covered by the surveillance introduced by the AML Directive.

The provisions of the AML Directive treat each and every customer of financial services providers alike: everyone is treated with some degree of suspicion, as if he or she were a potential money launderer or terrorist financier. As a customer will be unable to prove that he is not a money launderer, and especially as nobody is able to establish that he or she will not commit a crime in the future, there can be no defence in order to free oneself from such suspicion. Therefore, there is no way for a customer to escape the constant monitoring of his financial transactions. There is no mechanism to object to this surveillance of one's bank account, and there is no possibility for any customer to be exempted from scrutiny.

42 T Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16(2) European Law Journal 158.

43 S Greer, 'The Exceptions to Articles 8 to 11 of the European Convention of Human Rights' (1997) 15 Human Rights Files 14–15 (Council of Europe Publishing); A Galetta and P De Hert, 'Complementing the Surveillance Law Principles of the Court of Strasbourg with its Environmental Law Principles. An Integrated Technology Approach to a Human Rights Framework for Surveillance' (2014) 10(1) Utrecht Law Review 55–75.

44 Recital 42 states that 'The fight against money laundering and terrorist financing is recognized as an important public interest ground by all Member States.'

45 See the Global FinDex 2014 <http://www.worldbank.org/content/dam/Worldbank/Research/GlobalFindex/PDF/N1Unbanked.pdf> (last accessed 12 July 2016).

In addition to the unlimited application in terms of data subjects, the Directive also extends the definition of money laundering in one important point. The list of predicate offences in Article 3(4) of the Directive enumerates the classical predicate offences for money laundering, but also a catch-all provision in Article 3(4)(f). According to that provision, Member States with a minimum threshold for punishments must include all crimes which can be punished with a minimum of over six months. Member States which define the maximum sentences in their criminal code must include all crimes punishable by a prison sentence of over one year. This provision thus extends the catalogue of predicate offences by a considerable number of criminal offences, which may be difficult to connect to money laundering. For example, severe cases of defamation, battery, manslaughter, and murder may be punishable by long prison sentences in all Member States and thus be covered by that provision, while in the large majority of cases, no criminal transactions will be connected to those crimes. The reason for this wide extension of the catalogue of predicate offences with all these crimes which lack a financial component is, therefore, not clear.

On the contrary, connecting these crimes to money laundering and to the surveillance exercised over the financial movements of the population creates the danger that the presence of such predicate offences also opens up a possibility for scrutiny of the suspect's financial movements. It is not yet clear which standard of protection will be applied to a person's financial data where there is a reasonable suspicion of a predicate offence, or where such an offence has already been proven. Similarly, the mechanisms established by the AML Directive for access to financial data have not yet been examined by the CJEU in the light of fundamental rights, such as the right to private life, and the right to a fair trial. Connected to the right to a fair trial are, in this case, the presumption of innocence, the protection from illegal search and seizure, and the right to access information to defend oneself.

These rights will be discussed in the following sections in more detail. The indiscriminate collection of data from all data subjects appears to be intended to collect data that are 'nice to know' rather than 'needed to know' for law enforcement.

The data to be retained

The data which is to be retained is, in the first place, customer identification data (Article 40(1)(a)). This concerns a copy of the identification document which the customer has presented at the beginning of the business relationship with the bank, or a newer document if any of the information has changed. Secondly, a bank is also compelled to store 'supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions' (Article 40(1)(b)). This must be understood to mean that a full transaction record must be retained for each customer. The full retention of the transaction record is indeed an interesting point. There are no provisions that allow a bank to purge that record of transactions which are manifestly unsuspicious, such as a person's weekly grocery shopping and rent. However, the inclusion of such a safeguard would be very much in keeping with the principle of data minimization.[46]

Another point to consider is how much a person's transaction record reveals about that person's private life. Such a record will allow deep insights into a person's income and spending behaviour, as well as a web of connections between this person and the children to whom he pays pocket money, the former spouse to whom he pays alimony, the political and religious organizations to which he donates, the shops in which he makes ordinary and extraordinary purchases, and all the other little subscriptions and standing orders which regularly or occasionally deduct money from one's account. All these transactions come with a time stamp and a number of other identifiers, which allow a close look at a person's daily habits and preferences. Undoubtedly, many persons will consider this information very private and object to anyone taking notice of it. Again, this indiscriminate retention of data looks more as if the Directive aims at collecting data that are 'nice to know' rather than 'needed to know'.

The period of retention

Closest to the core of the *Digital Rights Ireland* case is, of course, the retention of customer and transaction data. The term of retention of the customer data (Article 4(1)(a) and (b)) is set at five years after the end of a business relationship between the customer and the obliged entity. However, Member States are free to extend this period to a total of 10 years 'after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection

46 The principle of data minimization is regulated in art 6(1)(c) of the Data Protection Dir 95/46.

or investigation of money laundering or terrorist financing' (Article 40(1)).

The term 'after the end of the business relationship' is an interesting point. The duration of the business relationship is thereby not taken into account. It is not unusual, however, for a business relationship between a bank and a customer to last several years. The retention period is thus the sum of the duration of the business relationship and the five years retention period after the end of the business relationship set by Article 40. This very long retention period is conspicuously at odds with the different statutes of limitation which are observed in Member States for the crime of money laundering. For instance, in Germany, a money laundering offence can only be prosecuted for five years after it has been committed (Article 78 juncto Article 261 (1) StGB). In the Netherlands, the same offence becomes time-barred after 12 years (Article 70 juncto Article 420bis Wetboek van Strafrecht). It does not seem appropriate to ask obliged entities to retain customer data beyond the time frame set by the statute of limitation. Also the very long period of retention of the data, which does not match the timeframe for the prosecution of the crimes shows that the data collected follow a 'nice to know' rather than a 'needed to know' approach.

The proportionality of the data retention requirement

The above discussion leads to several points of critique regarding the proportionality of the data retention requirement in the AML Directive. One of the first questions that one would ask is why such surveillance is directed against the individual, especially if the person asking has never given law enforcement reason to suspect any involvement in criminal financial transactions. It has been emphasized that there are no personal exceptions from scrutiny, which leads to a situation in which every member of the population using financial services is automatically a potential suspect of a money laundering or terrorist financing offence.

Before the introduction of those rules into the national legal systems, the situation was generally reversed. Law enforcement officials would identify a suspect of a financial crime, apply for a warrant and demand the suspect's records from the bank. Ideally, there would be no interference with a person's financial privacy unless the suspicion against that person was of such a nature as to suffice for an official warrant with which the financial service provider would have to comply. Thus, generally, scrutiny of a person's bank data was connected with an existing suspicion against the customer and embedded into an official investigation. Today, with the AML Directive, financial data has lost this protection. Every transaction is scrutinized by the financial service provider, even in the absence of the remotest suspicion against the sender or recipient of funds. If this scrutiny comes across a transaction which raises a flag, the financial intelligence unit must be alerted of the transaction, and the customer's personal records and transaction data are forwarded to this unit. Naturally, the information is shared without the knowledge of the customer.

This situation is clearly comparable to that created by the now invalidated DRD, as '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'.[47] Besides creating an unpleasant feeling in members of the public who are aware of this scrutiny, this mechanism also raises the question whether treating all bank customers with suspicion is compatible with the principle of the presumption of innocence.

Ultimately, the question which needs to be answered in this context is whether, taking all the above into consideration, the data retention requirement in the AML Directive can be considered to be proportionate to the aim which it must achieve. The proportionality standard demands that the measures taken are both effective as well as necessary, ie the objective could not be achieved using any less intrusive measures. While the objective of fighting the crimes of money laundering and terrorist financing is undoubtedly an important one, it must be balanced with the very pronounced intrusion into the private life of every member of society who uses a bank account. The result of the provisions of the directive is the collection and retention for long periods of time of data which are 'nice to know' but not necessarily needed. This result is therefore clearly in conflict with the proportionality principle and thus makes this interference with the rights to privacy and data protection of the individuals unlawful.

Conclusion

The rights to privacy and data protection of individuals are considered to be fundamental rights in the EU, and protected in Articles 7 and 8 of the EU Charter of Fundamental Rights. Any interference with these rights must be proportionate. Retention of personal data is one of the ways the rights to privacy and data protection are interfered with. This method of interference with

47 Joint Cases C-293/12 and C-594/12(n 3) para 37.

the private lives of individuals, especially when done in such an indiscriminate way, covering all individuals and entire categories of data, creates the feeling that the private lives of individuals are under surveillance at all times.

Although the rights to privacy and data protection are not absolute, any interference must respect the principle of proportionality. The invalidation of the DRD showed the importance of this principle, and that a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, independent of the legitimacy of the objectives pursued, must precede any new legislative acts. This article showed that this was not the case with the data retention requirements in the AML Directive.

The Directive introduces in the EU a form of mass surveillance of all individuals using the services of financial institutions for financial transactions. It has been shown that the Directive creates a system in which all financial transactions of all bank customers are scrutinized, with no exceptions for any categories of transactions or customers. Furthermore, the continuous collection of the data and their potential use without informing the person concerned makes the interference with the private sphere of the individuals very serious, as it generates the feeling of being subject of constant surveillance. The Directive does not require a categorisation of individuals on the basis of their potential risk and neither a categorisation of the data collected. In addition, the data retention period is not established on the basis of objective criteria, nor is it linked to the periods for the prosecution of the crimes of money laundering and terrorism financing that are established in the various national laws. Thus, the large scale of data collected and retained on the bases of the AML Directive is disproportionate and infringes the rights to privacy and data protection of European citizens. Since the data retention required by the Directive is linked mostly with data that are 'nice to know' rather than 'needed to know', in the light with a human rights-based approach, we argue that it should be invalidated.

doi:10.1093/idpl/ipx002
Advance Access Publication 5 April 2017