The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention

A Flawed Comparison?

Lukas Martin Landerer

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

Early in its development, the EU's anti-money laundering (AML) scheme was already criticized for its interference with the fundamental rights to privacy. Quite recently, some scholars have highlighted that customer due diligence obligations constitute a massive retention of financial data. Consequently, they have tried to apply the ECJ's findings on data retention of telecommunication traffic data to the AML framework. Financial data is quite legitimately seen as a honeypot for law enforcement authorities, which makes a comparison between retention of financial data and retention of telecommunication traffic data readily apparent. Surprisingly, not much attention is paid to the AML framework in this context, compared to the pile of comments telecommunication data. Not even the EDPS mentioned data retention as a problem in his opinion of the EU's action plan on money laundering in 2020. It is thus also not surprising that no alterations to the retention obligations can be found in the recently proposed AML Regulation. The question arises: does the AML scheme really compare as easily to the prominent data retention of telecommunication meta data after all? As yet another AML package lies ahead of us, it is time to have a look at why the EU legislator does not seem to be intimated by the ECJ's case law regarding its AML framework. The author argues that the definition of data retention, which the scholars who wish to apply the ECJ's case law to the AML framework have in mind, is too broad. It does not capture why the ECJ has so strictly ruled on the retention of telecommunication traffic data. The AML scheme deviates from the retention of telecommunication traffic data in several ways. These differences make it difficult to test the lawfulness of the Union's AML law in its new guise by applying the ECJ's jurisprudence on data retention. In light of the ECJ's case law, it is the access permissions whose legitimacy seems questionable, not the obligation clauses.

AUTHOR

Lukas Martin Landerer

Doctoral Researcher
Max Planck Institute for the Study of Crime, Security and Law

CITATION SUGGESTION

L. Landerer, "The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention", 2022, Vol. 17(1), eucrim, pp67–72. DOI: https://doi.org/10.30709/eucrim-2022-005

Published in
2022, Vol. 17(1) eucrim pp 67 – 72
ISSN: 1862-6947
https://eucrim.eu

I. Introduction

The term *data retention* can generally be defined as "the collection and storage of personal data for an undetermined purpose in the event that it should ever be needed for not yet specified future use."[1] Its notoriety stems from a – more than decade-long – legal dispute between EU Member States and the European Court of Justice (ECJ). The story really began in 2006, when the EU obligated its Member States to set up or align laws on retention of telecommunication traffic data via a directive.[2] Providers of electronic communication, including internet access and internet telephony, were thereby forced to retain traffic data (who called who, when, and from where?) of their customers for six months and to make them accessible to state security authorities.

As is known, the ECJ was not happy with this directive. In the *Digital Rights Ireland* judgment of 2014, the Court found that the massive retention of data without specific cause would constitute a disproportionate interference with the rights of private life and data privacy, Arts. 7 and 8 of the Charter of Fundamental Rights of the EU, and thus revoked the directive.[3] Subsequently, some Member States argued that the judgment would not affect respective norms in domestic law and kept their retention obligations.[4] Inevitably, the ECJ had to decide on these national data retention laws as well. It took the opportunity to affirm its case law, in principle, but specified it in two consecutive judgements, *Tele2 Sverige*[5] and *La Quadrature du Net*.[6]

The findings of the Court regarding the conditions for data retention can be briefly summarized as follows:[7] Principally, data retention must be viewed as a two-stage process. First, there is a legal obligation, mainly for private actors, to store a bulk of data for a specific period of time. The second stage comprises the legal provisions that enable state authorities to access these data. Both elements independently interfere with fundamental rights to privacy.[8] Therefore, there must be safeguards for each stage.[9] As of now, a general retention of data is only permissible if a Member State is threatened by a real and present danger to national security.[10] If this is not the case, only data from specific persons may be retained, based on objective, non-discriminating, or geographical criteria.[11] In any case, state access to these data may only be permissible if it is necessary to combat serious crime, if it is subject to prior review by a court or an independent administrative authority, and if the retained data is based within the EU.[12]

In the following section, I will briefly describe, where data retention rules are included in the European AML framework (II). It shall then be shown that retention of transaction data is nothing new as it has been included in various legal provisions already (III). Hence, I will argue that maybe instead one should shift away from focussing on retention clauses and rather critically review the clauses, which grant the FIUs access to retained transaction data (IV).

II. Data Retention in the New AML Regulation

The European Union's anti-money laundering (AML) framework obliges entities to retain personal financial data. As of now, the central norm can be found in Art. 40 of the anti-money laundering Directive,[13] which was amended for the fifth time in 2018 (AMLD5).[14] Art. 40(1)(a) AMLD5 obliges entities to retain a copy of *the documents and information which are necessary to comply with the customer due diligence requirements (…) for a period of five years after the end of their business relationship (…) or after the date of an occasional transaction.* Furthermore, Art. 40(1)(b) AMLD5 obliges entities to keep 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, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.*

The recent proposal for an AML regulation (hereinafter: AMLR-p)[15] does not make substantial changes to these obligations. Art. 56(1) AMLR-p reads almost identically with Art. 40(1) AMLD5. Just like its predecessor, it differentiates between information that was necessary for the execution of customer due diligence (CDD) measures in para 1(a) and transaction records in para 1(b). The declaration of para. 1(b) is unambiguous. It provides an obligation to retain records of any transaction, independently from the scope of the applied CDD measures.

This issue has been acknowledged not only by legal scholars[16] but also by Article 29 (Data Protection) Working Party as early as 2011.[17] Although the Working Party did not directly compare the AML framework to the data retention rules regarding telecommunication meta data, it was deeply concerned by the long and rigid retention periods.[18] The Union legislator has yet to react to this criticism. The retention periods have not been altered since 2011 and still amount to five years according to Art. 56(3) AMLR-p.

The fact that the retention rules have not changed substantially might be explained by the low public awareness of the topic, both in academic and in political discussions. Although data retention, especially that of telecommunication data and of passenger flight records, is heavily discussed in Germany,[19] the AML framework is noted merely as a side issue.[20] The European literature looks somewhat better, with about a handful of authors commenting on the issue.[21] Yet, the amount of literature regarding the topic falls significantly short to the prominence of data retention concerning telecommunication data.

III. Retention of Transaction Data in other Legal Provisions

The reason for this lack of attention is surely not to be found in the characteristics of the retained data. As all the scholars involved in researching this topic[22] have noticed, financial data are as sensitive as it can get according to the standards of the ECJ. The judges in Luxembourg rightfully considers the quality of personal data and therefore the intensity of its retention according to the way the data can be used to develop personality profiles.[23] There are few documents imaginable that are as suitable for creating such personality profiles as transaction records. They contain information on personal preferences, income, location, personal relations, and much more. Especially in a consumer age of cashless payments, bank account statements can be read as a summary of one's personal life.[24] Thus, unsurprisingly, security and intelligence agencies are quite keen on obtaining financial records.[25] The general German acceptance of the disclosure of financial data relates to this trend coherently. In an empirical study, however, 66% of the respondents answered that the duty of banks to hand out information to state authorities is "not a good thing".[26]

A better explanation for the absence of the topic in legal discussions might be the universality of retention obligations regarding financial data in various legal provisions. Other than telecommunication traffic data, transaction records are not stored for security purposes only. This will be exemplified in the following by taking a look at German and European Union law.

1. Germany

According to German law, banks and other financial services that provide accounts for their customers have a civil law accountability to report the balances to their customers in detail. This duty stems directly from the banking contract itself, e.g. giro accounts, in accordance with §§ 666, 675 of the German Civil Code (*Bürgerliches Gesetzbuch– BGB*).[27] Financial companies usually fulfil this duty by providing account statements.[28]

Furthermore, banks and payment services are merchants according to § 1 paras. 1, 2 of the German Commercial Code (*Handelsgesetzbuch – HGB*). As such, they are required to adhere to commercial account-

ing rules (§ 238 para. 1 HGB). These include an obligation to retain *accounting receipts* for ten years (§ 257 para. 1 (4) HGB). Such receipts include all documents referencing business events and transactions.[29] Now, every transaction and deposit that is carried out via a banking or payment account is considered a business event from the bank's point of view, since they directly affect the contractual relationship with their customer. Thus, the account statement, where all accounting events are listed, fall under the scope of application of § 257 para. 1 (4) HGB.[30] To handle this vast amount of data, banks have made a transition to storing their customers' statements digitally.[31]

Overlapping with the trade law's obligation is the accounting obligation in German tax law. § 147 para. 1 (4) of the Fiscal Code (*Abgabenordnung –AO*). It reads similar to § 257 HGB regarding accounting receipts and contains the same retention period. The rules are coordinated.[32] The German banking law also contains an accountability clause in § 25a para. 1 sentence 6 (2) of the Banking Act (*Gesetz über das Kreditwesen – KWG*).

2. European Union

At the EU level, various provisions regulate which specific information must be contained in account statements. Arts. 57, 58 of the second Payment Services Directive (PSD2)[33] regulate information that must be provided by the payment service providers to both payer and payee. This involves transactions conducted via giro accounts.[34] The banks of both payer and payee which act as payment service providers,in turn fulfil their respective duties by providing account statements.[35] Art. 21 PSD2 includes a five-year record-keeping clause, affecting *all appropriate records for the purpose* of title 3 of the PSD2, but it does not affect domestic retention clauses, since it only sets a minimum retention period. It also explicitly does not affect the retention rules of the AML framework.

Another source of information provisions on payments can be found in the Regulation Regarding Direct Debit and other Transfers in Euro (SEPA-Regulation).[36] Art. 5 (1) and (3) SEPA-Regulation in conjunction with No. 1, 2 of its Annex provide some obligatory information that the acting payment providers must submit to payer and payee. The information mostly overlaps with what is already mandatory according to PSD2. The same can be said for the Transfer of Funds Regulation,[37] which also includes a five-year retention clause in Art. 16.

In sum, German law in conjunction with EU law poses a whole package of retention rules regarding account statements.

IV. A New Focus: The FIU's Access to Retained Financial Data

The fact, that banks and other payment service providers store transaction record and thus retain sensitive financial data is thus, nothing new. The AML-framework does not constitute an obligation, which wouldn't otherwise exist. Its effect is of mere declarative or repetitive nature.

Yet, the focus of attention has primarily been on monitoring and retention clauses which cannot come as a surprise. From the very beginning, the ECJ has highlighted that not only state access, but also retention (by private actors) itself affects fundamental rights.[38] It is questionable whether this approach is persuasive in its generality , if one takes into account that companies' accounting and compliance rules as well as social and public administration law, in many cases, inevitably lead to the processing and storage of large amounts of personal data. Also, accessing this data is usually not a problem for security authorities – at least not in Germany. Although the correct legal rules for information requests may be debated in criminal procedure[39] and police law,[40] their general permissibility is not disputed. For intelligence services, there are even explicit

norms that allow for secret information requests from banks, e.g., § 8a para 1 (2) of the Federal Office for the Protection of the Constitution Act (*BVerfSchG*).

1. The root of the issue with data retention structures

One can thus conclude that the general idea of data retention for private entities or public administration authorities cannot be the reason for the ECJ's disfavour. It is in the nature of today's society that information is documented for various reasons. And it belongs to the very nature of criminal investigation that pre-existing information is gathered. Hence, the broad definition that was presented in the introduction must be narrowed down, if one wishes to get to the core of what makes the famous data retention cases so significant.

One factor that must be highlighted is the purpose of the retention clause.[41] Only if strictly for security issues should the narrow conditions of the ECJ be applied. This is obviously the case for the AML data retention clauses, as they are aimed at fighting money laundering and the financing of terrorism. Yet, they constitute a special case, since the obligation to retain transaction records overlaps with legal rules that have different purposes, for example economical ones. Thus, the question is whether the mere addition of a security purpose to an already existing retention obligation should be viewed as strictly as retention clauses that exist only for security reasons, as was the case with the 2006 Data Retention Directive.

To answer this question, one must shift the focus away from the retention level and look towards access structure. In Germany, the purpose of access rules on telecommunication meta data can be twofold.

First and in any case, they allow for secret access. Traffic data could previously be accessed directly from telecommunication providers according to § 113 of the 2015 Telecommunications Act (*Telekommunikationsgesetz – TKG 2015* [not in force anymore]). The providers were legally forced to treat the request confidentially according to §§ 15, 33 Telecommunications Interception Ordinance. Such an obligation to secrecy does not exist if the request were to be based on the general provisions of the criminal procedure code.[42]

The second purpose, which can be found in the access provisions for contractual data, is simplification. The access privilege for telecommunication contract data (name, number, identification code, device number, etc.) lies with a central authority, the Bundesnetzagentur (*Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway*), which has direct access to the providers' databases, § 173 TKG. The same holds true for contractual data of bank account holders, § 24c KWG, §§ 93b, 93 paras. 7, 8 AO.[43] In these "automated processes", security authorities do not themselves address the (private) providers but must rather ask the respective central authorities to do so. The investigating officer can instead stay in his/her office without having to disclose the investigation to anyone. This ability to investigate via communication alone makes the citizen easily transparent. Especially if the investigation solely takes place between authorities. Perhaps it was this image that led the ECJ to conduct its strict review on retention of telecommunication data, as it deviates from the conventional image of investigation under the rule of law. Traditionally, the state must face the concerned person to ensure equality of arms.[44] This includes the principle of an openly investigating police.[45]

2. The FIU's access provisions

Here lies the problem with data retention structures. The more they deviate from our traditional picture of legal investigation, the more they infringe the right to privacy. It has already been recognized that the retention obligation in the AML framework only adds a purpose and does not lead to more factual records. In this context, it is less infringing than the retention of telecommunication traffic data. If one wishes to apply the ECJ's jurisdiction in *La quadrature du net* to the AML framework, one must then check whether the ac-

cess rules of the AML framework deviate from traditional principles of investigation in such a way that it lends itself to a comparison with the retention of telecommunication traffic data.

In principle, the AML framework is a compliance system. The private entities – not security authorities – are at the forefront of the fight. Unlike telecommunication providers, banks must actively monitor transactions and report suspicious activities. These "suspicious activity reports" (SARs) can even be seen as the core of the system.[46] Meanwhile, the ECJ[47] and the ECtHR[48] have found that the obligation to submit SARs would, at least, not even infringe the rights of obliged lawyers. The privacy rights of the affected customers were not substantially checked; thus, it seems that the case law does not recognize them as a problem with regard to SARs.

However, the AML framework does allow for the reverse direction as well. According to Art. 32(9) AMLD5, the Financial Intelligence Units (FIUs) *are "able to request, obtain and use information from any obliged entity for the purpose set in paragraph 1 of this Article, even if no prior report is filed"*. This authorisation of FIU's to request information is included Art. 18 (4) of the proposal for a sixth AML-directive – AMLD6-p[49] and reads identically to its predecessor. A similar provision can be found in Art. 33 (1) (b) AMLD4 respectively Art. 50(1)(b) AMLR-p, which reads: "*Obliged entities, and, where applicable, their directors and employees, shall cooperate fully by promptly providing the FIU directly, at its request, with all necessary information.*" Although the wording suggests that Art. 33 (1) (b) AMLD4 respectively Art. 50(1)(b) AMLR-p are no authorisation rules. In any case, the FIUs are authorised by 32(9) AMLD5 respectively Art. 18 (4) AMLD6-p. These provisions state that a prior report is not needed for the FIUs' requests which is also clarified by recital 79 AMLR-p.

The FIUs' competence to request information must be read in conjunction with the other competent security authorities' permission to request information from the FIU. This authorisation is stated in Art. 32(4) AMLD4/5 and can be found, almost unchanged, in Art. 19(1) AMLD6-p.

In theory, without a SAR having been filed, security authorities can access the financial information of a target indivudal by requesting this information from the FIU. The FIU could then send a request to the respective private entities. Via this route, security authorities could access the retained account statements without themselves having disclosed the investigation towards the obliged entities.

The private entities are not allowed to disclose the FIU's request to third parties, especially not to their customers (Art. 39 (1) AMLD5/Art. 54(1) AMLR-p). Therefore, the access remains secret. This access route should be focused on in any proportionality test of potential fundamental rights infringements.[50] As long as the access is not subject to the conditions that were demanded in the ECJ's case law on data retention, the argument can well be made that the current and proposed AML framework violates privacy rights.

V. Conclusion

It has been shown that applying the ECJ's pattern regarding retention of (teleocommunication) data to the AML framework is intrusive, but not as easy as some scholars[51] have suggested. The obligation to retain financial data does not factually increase the amount of stored data, since overlapping obligations are already in place. The purpose has merely been expanded to now include security-related issues.

One should thus shift from focusing on the retention obligation as such and instead review the FIUs' access to the records more strictly. Via information requests, other competent state authorities could indirectly access financial data, without a suspicious activity reports being filed (by a private entity). This leads to secret access to privately stored data through an intermediary authority. Since this structure deviates from the traditional approach to law enforcement, a case can be made for applying the ECJ's data retention conditions, at least as regards the accessibility of data pursuant to the AML legal framework. The fact that

corresponding considerations are missing in the recently proposed AML package raises doubts as to whether or not the Union legislator is really willing to implement the ECJ's findings.

---

1. M. Albers, "Data Retention in Germany", in: M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws,* 2021, p. 117.↩
2. Directive 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 Directive 2002/58/EC, *O.J.* L 105, 13.4.2006, 54.↩
3. ECJ, 8 April 2014, cases C-293/12 and C-594/12, *Digital Rights Ireland*, paras. 45-69.↩
4. For an overview, see J. Kühling and S. Heitzer, "Returning Through the National Back Door? the Future of Data Retention After the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere", (2015) 40(2) *European Law Review,* 263; X Tracol, "Legislative Genesis and Judicial Death of a Directive", (2014) 30(6) *Computer Law & Security Review,* 736, 743–744.↩
5. ECJ, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige, Tom Watson and Others*.↩
6. ECJ, 8 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*.↩
7. For an overview, see T. Wahl, "Spotlight: CJEU: Data Retention Allowed in Exceptional Cases", (2020) *eucrim*, 184.↩
8. ECJ, *Digital Rights Ireland*, *op. cit.* (n. 3) paras. 58-60; 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(6) *European Law Review*, 834.↩
9. See AM. Pedersen, H. Udsen and SS. Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", (2018) 8(2) *International Data Privacy Law,* 160.↩
10. ECJ, *La Quadrature du Net and Others, op. cit.* (n. 6), paras. 137, 168.↩
11. ECJ, *La Quadrature du Net and Others, op. cit.* (n. 6), para. 168.↩
12. ECJ, *Tele2 Sverige, op. cit.* (n. 5), para. 125.↩
13. Directive (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 Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *O.J.* L 141, 5.6.2015, 73.↩
14. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 Directives 2009/138/EC and 2013/36/EU, *O.J.* L 156, 19.6.2018, 43.↩
15. Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 20.7.2021, COM(2021) 420 final. For a summary, see T. Wahl, "Spotlight: AML Package II: Commission Proposes AML Regulation", (2021) *eucrim*, 154-155.↩
16. C. Kaiser, *Privacy and identity issues in financial transactions,* 2018, pp. 101-104, 492-495; J. Milaj and C. Kaiser, "Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'", (2017) 7(2) *International Data Privacy Law,* 115, 123.↩
17. Article 29 Data Protection Working Party, "Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing", (01008/2011/EN WP 186 13 June 2011), Annex No 28, 29, pp. 22-24.↩
18. Article 29 Data Protection Working Party, *op. cit.* (n. 17), No. 28, 29, pp. 22-24.↩
19. See *inter alia* A. Moser-Knierim, *Vorratsdatenspeicherung,* 2014.↩
20. See, for example, Albers, *op. cit.* (n. 1), p. 117.↩
21. A. Bertrand, W. Maxwell and X. Vamparys, "Do AI-based anti-money laundering (AML) systems violate European fundamental rights?", (2021) 11(3) *International Data Privacy Law,* 276; B. Vogel, "Conclusions and Recommendations", in: B. Vogel and J.-B. Maillart (eds.), *National and international anti-money laundering law. Rethinking the architecture of criminal justice, regulation and data protection,* 2020, pp. 881, 897-904; Kaiser *op. cit.* (n. 16); J. Milaj and C. Kaiser, (2017) 7(2) *Int. Data Privacy Law*, *op. cit.* (n. 16).↩
22. Ibid.↩
23. ECJ, *La Quadrature du Net and Others, op. cit.* (n. 6), para. 117; ECJ, *Digital Rights Ireland, op. cit.* (n. 3) para. 27; see MW. Müller and T. Schwabenbauer, "Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden", (2021) *Neue Juristische Wochenschrift* (*NJW*), 2079, 2084.↩
24. V. Pfisterer, "»Finanzprivatsphäre« in Deutschland", (2017) 65(1) *Jahrbuch des öffentlichen Rechts der Gegenwart. Neue Folge* (*JöR*), 393, 400; C. Westermeier, "Money Is Data – the Platformization of Financial Transactions", (2020) 23(14) *Information, Communication & Society*, 2047; Wissenschaftliche Dienste des Bundestags, "Zu möglichen erweiterten Befugnissen der Nachrichtendienste bei der Überwachung von „Finanzströmen", (WD 3 - 3000 - 040/19 2019), 7.3.2019, p. 11.↩
25. See T. Reichling, "Strafprozessuale Ermittlungen bei Kreditinstituten – ein Überblick", (2011) *Juristische Rundschau* (*JR*), 12; M. Parker and M. Taylor, "Financial Intelligence: A Price Worth Paying?", (2010) 33(11) *Studies in Conflict & Terrorism,* 949, 952–954; B. Scott and M. McGoldrick, "Financial intelligence and financial investigation: opportunities and challenges", (2018) 13(3) *Journal of Policing, Intelligence and Counter Terrorism*, 301.↩
26. M. Heiden, *Banken als Erfüllungsgehilfen staatlicher Politik,* 2013, p. 100.↩
27. Bundesgerichtshof (BGH) [German Federal Court of Justice], (2003) *Neue Juristische Wochenschrift – Rechtsreport (NJW-RR)*, 1555, 1556; G. Bitter, Kontenpfändung in: H. Schimansky, H.-J. Bunte and H.-J. Lwowski (eds.), *Bankrechts-Handbuch,* 5th ed. 2017, § 33, mn. 56.↩
28. Bundesgerichtshof (BGH) [German Federal Court of Justice], (2001) *Neue Juristische Wochenschrift –(NJW)*, 1486; M .Löhnig, "BGH v. 8. 11. 2005 – ZR 90/05, Anspruch auf Erteilung von Kontoauszügen wird nicht mit Hauptforderung mitgepfändet", (2007) *Juristische Rundschau* (*JR*), 73, 75.↩
29. B. Rätke, in: E.-M. Gersch and others (eds.), *Abgabenordnung: Einschließlich Steuerstrafrecht,* 15th ed. 2020, § 147, mn. 24.↩
30. See T. Knierim, in: B. Bannenberg and others (eds.),Straftaten im Bankbereich, *Handbuch des Wirtschafts- und Steuerstrafrechts,* 5th ed., 2020, Chapter 10, mn. 25.↩

31. Ibid.↩
32. S. Shin, *Bank- und kapitalmarktrechtliche Organisationspflichten,* 2013, p. 169; Rätke, *op. cit.* (n. 29), § 147, mn. 147.↩
33. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *O.J.* L 337, 23.12.2015, 35.↩
34. K. Wahlers, *Die rechtliche und ökonomische Struktur von Zahlungssystemen inner- und außerhalb des Bankensystems,* 2013, p. 30.↩
35. Bundesgerichtshof (BGH) [German Federal Court of Justice], (2014) *Neue Juristische Wochenschrift (NJW)*, 922.↩
36. Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009, *O.J.* L 94, 30.03.2012, 22.↩
37. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, *O.J.* L 141, 05.06.2015, 1.↩
38. ECJ, *Digital Rights Ireland*, *op. cit.* (n. 3), paras. 58-60.↩
39. T. Reichling (2011) *JR*, *op. cit.* (n. 25); T. Kahler, *Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten,* 2017, pp. 31–55.↩
40. J. Wonka, "Die Rechtmäßigkeit staatlicher Auskunftsersuchen gegenüber Banken", (2017) *Neue Juristische Wochenschrift* (*NJW*), 3334, 3337-3338.↩
41. See *Bundesverfassungsgericht* (BVerfG) [Federal Constitutional Court], (2010) *Neue Juristische Wochenschrift (NJW),* 833, mn. 227; W. Bär in: J. Graf (ed.), *BeckOK StPO mit RiStBV und MiStra,* Ed. 1.10.2020, § 100g StPO, mn. 1.↩
42. See T. Reichling, (2011) *JR*, *op. cit.* (n 25), 16.↩
43. See *Bundesverfassungsgericht* (BVerfG) [Federal Constitutional Court], (2007) *Neue Juristische Wochenschrift (NJW),* 2464; A. Kokemoor, "Der Automatisierte Abruf von Kontoinformationen nach § 24c KWG", (2004) *Zeitschrift für Bank- und Kapitalmarktrecht* (*BKR*), 135; V. Pfisterer, (2017) 65(1) *JöR*, *op. cit.* (n. 24), 407–412.↩
44. *Bundesgerichtshof* (BGH) [Federal Court of Justice], (2010) *Neue Juristische Wochenschrift (NJW),* 1297, 1298; K. Gaede, *Fairness als Teilhabe,* 2010, pp. 305-310.↩
45. S. Stavros, *The Guarantees for Accused Persons Under Article 6 of the European Convention on Human Rights,* 1993, p. 75; M. Fincke, "Zum Begriff des Beschuldigten und den Verdachtsgraden", (1983) 95(4) *Zeitschrift für die gesamte Strafrechtswissenschaft* (ZStW), 918, 955–972; Gaede, *op. cit.* (n. 44), pp. 233–238.↩
46. S. Barreto da Rosa, in: F. Herzog and O. C Achtelik (eds.), *Geldwäschegesetz (GwG),* 4th ed., 2020, § 43, mn.1.↩
47. ECJ, 26 June 2007, Case C-305/05, *Ordre des barreaux francophones et Germanophone v Conseil des ministers*.↩
48. ECtHR, 6 December 2012, *Michaud v France*, Appl. No. 12323/11.↩
49. Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, 20.07.2021, COM(2021) 423 final.↩
50. See also B. Vogel, "The Anti-Money Laundering Architecture of Germany", in: B. Vogel and J.-B. Maillart (eds.), *op. cit.* (n. 21) , pp. 157, 242–246; Barreto da Rosa, *op. cit.* (n. 46), § 30, mn. 21.↩
51. Kaiser, *op. cit.* (n. 16); Milaj and Kaiser, (2017) 7(2) *Int. Data Privacy Law*, *op. cit.* (n. 16); A. Bertrand, W. Maxwell and X. Vamparys, (2021) 11(3) *Int. Data Privacy Law*, *op. cit.* (n. 21).↩

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.

Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union