Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing

Benjamin Vogel *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

In its 2020 Action Plan to comprehensively reform the EU's Anti-Money Laundering and Terrorism Financing (AML/CFT) framework, the European Commission announced, inter alia, that it would issue guidance for Public-Private Partnerships (PPPs). Furthermore, in respect of the envisaged new EU-level Anti-Money Laundering Authority (AMLA), the legislative package published in July 2021 entails a draft provision to allow the AMLA to participate in national or supranational PPPs. If adopted, AML/CFT PPPs will have a legislative foundation in EU law. Though details would still be left to Member States, it is high time to assess the policy ideas behind PPPs as well as their legal ramifications.

AUTHOR

Benjamin Vogel

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law (formerly Max Planck Institute for Foreign and International Criminal Law)

CITATION SUGGESTION

B. Vogel, "Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing", 2022, Vol. 17(1), eucrim, pp52–60. DOI: https://doi.org/10.30709/eucrim-2022-002

Published in
2022, Vol. 17(1) eucrim pp 52 – 60
ISSN: 1862-6947
https://eucrim.eu

I. Public-Private Information Sharing in the Current AML/CFT Framework

The global Anti-Money Laundering and Terrorism Financing (AML/CFT) framework was originally conceived as a system in which the private sector would autonomously screen its customer relationships in order to detect cases where assets are related to criminal activity or where there is at least a suspicion to this effect. Over time, however, there has been increasing awareness on the part of the Financial Action Task Force (FATF) and in the European Union (EU) of the fact that the detection of relevant risks is usually far from being a straightforward task, given that the private sector usually lacks criminalistic expertise and detailed information pertaining to the nature and modi operandi of criminal actors. As a result of these practical limits, the AML/CFT framework has increasingly emphasised the role of the public sector in providing obliged entities with guidance. In the EU, Directive 2015/849 now provides for an obligation on the part of the Commission, the European Supervisory Authorities (ESAs), and Member States to identify and assess money laundering and terrorism financing risks at regular intervals and to make their findings available to obliged entities.[1] Further guidance specifying risk factors is required from the European Banking Authority (EBA),[2] and Member States' authorities must provide obliged entities with information on the practices of money launderers and financers of terrorism.[3] EU law, however, specifies neither the scope of such information nor the functioning of the associated information gateways. Moreover, although Financial Intelligence Units (FIUs) are under a general obligation to provide feedback to obliged entities on Suspicious Activities Reports (SARs) filed by the latter,[4] EU law remains silent on the scope and frequency of this feedback. As a result, obliged entities at the level of the Member States have in most cases not received specific guidance beyond the EBA's risk factors[5] and the typologies provided by various supranational institutions, most importantly the FATF.[6] In short, while EU law in the meantime presupposes that public-private information sharing is a prerequisite for the effective functioning of the AML/CFT system, it does not yet provide meaningful guidance on how to put such information sharing into practice. Against this background, the last few years have seen increasing policy debates on public-private information sharing.[7]

II. Ambiguities of Current Policy Debates

Current policy debates on public-private partnerships (hereinafter: PPPs) usually reflect the need to share strategic and also more targeted information in order to improve the private sector's ability to uncover criminal assets.[8] While this particular conception of the potential utility of PPPs appears to be a common denominator in most stakeholders' understanding of PPPs, the term "PPP", or "public-private partnership", is used in various ways and frequently reflects a mixture of rather unspecified goals. It is particularly interesting to note that PPPs are often presented as what essentially constitutes an attempt to improve the effectiveness of criminal investigations. This is especially the case when PPPs are proposed as a mechanism to share information to provide authorities with additional information in support of an ongoing investigation or to identify as-yet-unknown accomplices.[9] If such practices are labelled as PPPs, this entails some potential for confusion. Using the terminology of AML/CFT to describe and evaluate such ongoing investigation-focused "PPPs" can misrepresent the actual potential of those mechanisms to remedy existing deficits of the AML/CFT framework. In fact, investigation-focused information sharing may ultimately do little more than respond to deficiencies in a particular framework of criminal procedure. If, for example, the sharing of information about suspects in the context of an ongoing investigation is portrayed as an effort to improve the effectiveness of customer due diligence (CDD), and its success therefore measured by the number of SARs attributable to such sharing, the difference between AML/CFT and criminal procedure is blurred in a rather unhelpful way. For what is then called a "SAR" would in other jurisdictions be the mere response of a

private party to a request from an investigative authority. Such terminological nuances matter, because they may create the misleading appearance that the information exchange and the resulting SARs do improve the obliged entities' risk detection capacity. Conversely, other information-sharing practices discussed under the term "PPP" are, in fact, aimed at enhancing the obliged entities' ability to detect hitherto unknown criminals and criminal assets and are therefore genuine ways to improve the quality of CDD and resulting SARs. It is important to keep this ambiguity in mind when discussing a framework for PPPs in AML/CFT, not only because there is otherwise a risk that policy debates will apply the term "PPP" to mechanisms that have rather little to do with improving the quality of CDD, but also because stakeholders might otherwise overlook that some practices at the national level, despite not being called "PPPs", may in essence already provide for the possibility of enhancing public-private information sharing.[10] To identify the need for as well as the practical and legal requirements for such mechanisms, it is therefore necessary to identify the nature and possible functions of PPPs, in more detail, and of public-private information sharing, more generally.

III. The Different Meanings of PPP

The idea of public-private partnerships reflects the idea that the implementation of AML/CFT obligations by private entities and the enforcement of these obligations by supervisory authorities is in practice often – and some will argue most of the time – characterised more by the pursuit of formal compliance with rules than the pursuit of effective prevention and repression of crime.[11] This is because, in order to avoid being sanctioned by supervisory authorities for possible compliance violations,[12] obliged entities will first and foremost strive to show that they undertook reasonable steps to conform with the law. This will all too often push them, in an effort to refute possible supervisory criticism, towards applying CDD in a way that is primarily concerned with creating evidence that they followed the law.[13] Effectiveness, in contrast, is a much more relative criterion, making it ill-suited as a standard against which supervisors can assess the compliance of private obliged entities and likewise ill-suited as a standard that obliged entities themselves can look to in protecting themselves against sanctions. As a result, obliged entities regularly do as much as is necessary, but not much more than that, to show that they did not act carelessly vis-à-vis a particular customer.[14] It will often be much less in the interest of the obliged entity to invest additional efforts to inquire into a problematic customer relationship where such efforts – especially if they do not ultimately lead to the detection of criminal assets – will likely not be valued by regulators. In other words, it is often safer for obliged entities to ensure a mediocre compliance performance – that is, just ticking boxes – than to focus on better outcomes. This is not to say that formal compliance does not also produce useful results in many cases. The idea behind the concept of partnerships, however, is that current frameworks could be improved if it were possible to shape them in a more effectiveness-oriented way.

A partnership approach, as is often hoped, can achieve exactly this by ensuring that AML/CFT compliance is able to prioritise cases that merit greater scrutiny. By introducing mechanisms that allow for more dialogue among obliged entities, supervisors, and other competent authorities, a partnership approach can facilitate the discussion of compliance efforts and the pursuit of ways to refine them – all in the spirit of an effective detection of criminal assets. As the term "partnership" implies, such a dialogue requires that both sides be prepared to contribute to the common cause. On the private side, a partnership approach principally presupposes that an obliged entity is willing to go beyond the regulatory minimum and thus demonstrate a commitment not only to its formal compliance with the applicable obligations but also to greater effectiveness. On the public side, partnership entails a willingness on the part of the relevant authorities to listen and respond in an appropriate way to the concerns and difficulties expressed by obliged entities regarding their implementation of compliance obligations and – crucially – regarding the provision of information that may help them overcome or mitigate such difficulties. While AML/CTF PPPs are thus firmly grounded on a legal reality – namely, on the private sector's compliance obligations – the idea of PPPs also constitutes an acknowledg-

ment of the practical limits of top-down command-and-control approaches to regulation. This acknowledgement is evident from one of the primary aims of PPPs: the stimulation and encouragement of a sense of common purpose, based on shared interests of the public and private partners.

AML/CFT consists of a plurality of different key elements ranging from CDD and SARs to FIU analyses and, ultimately, where applicable, criminal investigations.[15] It follows that there are various stages at which closer public-private collaborations may come into play. Although public-private information sharing is the common denominator of PPPs, it is necessary to distinguish precisely how such information sharing is meant to contribute to greater effectiveness – that is, to define the intended purposes of PPPs. Without such differentiation, any policy debate risks losing orientation and ultimately suffering the fate of all disoriented policy initiatives: a situation in which the resulting measures offer no added value or even worsen the status quo by adding confusion and wasting valuable resources.

Public-private information sharing in the context of AML/CFT may essentially be divided into two primary purposes: the furtherance of ongoing investigations and the improvement of the effectiveness of CDD.[16] Both objectives do, of course, frequently overlap, because more effective CDD is ultimately likely to add value to criminal investigations. However, bearing this distinction in mind is nevertheless vital, because it makes a difference whether the immediate purpose of public-private information sharing is to support the compliance efforts of the private sector or the investigations of competent authorities. To overlook this difference would be to overlook the double purpose of AML/CFT: supporting law enforcement authorities in their investigations into relevant offences and supporting obliged entities in the prevention of ML/TF.

More specifically, each of the two primary purposes of public-private information sharing may again be subdivided into two particular functions that help explain not only the type of information to be shared but also the applicable legal framework and potentially the need for legal reform. As regards the furtherance of ongoing investigations,[17] competent authorities may share information with the private sector to trigger monitoring of the financial conduct of suspects and other persons and entities of interest. This would typically include in particular the sharing of names of targets, and could possibly include the sharing of additional information that may be helpful in rendering the monitoring more effective (for example, information on contact persons or the business activities of the targeted person). Alternatively, competent authorities may provide a private entity with information about persons of interest or profiles of potential suspects, with the aim of allowing the private entity to search its data records in a targeted way.[18] From an operational viewpoint, enabling such targeted searches may be attractive for two reasons. One reason is that it can allow private entities to respond to an information request from an investigative authority without drowning this authority in unstructured and often largely useless bulk data. The other reason is that it may allow investigative authorities to have private data records screened, using offender profiles, for hitherto unidentified suspects.

As regards public-private information sharing with the primary aim of improving obliged entities' CDD,[19] it is helpful to again distinguish between two more specific functions. On the one hand, competent authorities may provide obliged entities with information pertaining to specific SARs, in particular through the provision of feedback once an SAR has been filed.[20] This may entail the provision of information on whether the risk parameters applied in certain cases were appropriate in the eyes of the relevant authority (in particular the supervisory authority or the FIU). The information that competent authorities share with regard to specific SARs may, however, also encompass more personalised data. For example, a competent authority may communicate to an obliged entity that a transaction or customer mentioned in a particular SAR is, according to the assessment of the authority, indeed linked to crime, or that there is reasonable suspicion to this effect. On the other hand, compliance-focused public-private data sharing may entail the provision of information independently of any particular SAR, with the aim of enabling the obliged entity to improve its risk detection

capacity. This may, for example, include strategic information about criminal phenomena in a certain region or business sector but also more specific information such as profiles of relevant offenders or even information about particular suspects and their activities.[21]

Lastly, concepts for PPPs cannot and should not be disconnected from broader reflections about legal reform. As already mentioned, the concept of partnership seeks effectiveness by building on the shared interests of the parties in order to encourage both sides to go beyond legal obligations. Voluntariness is therefore a defining feature of PPPs. Insofar as PPPs are a response to deficiencies in the current state of the law or its implementation, however, they ultimately invite reform that goes well beyond the mere establishment of rules for new informal and voluntary mechanisms that would operate as an addition to formalised legal frameworks. Obviously, when policymakers acknowledge that informal and voluntary practices are being used or could be used to remedy insufficiencies in the existing legal framework, this usually indicates a need for the legal framework to be improved sooner or later. Such a need is more pressing when the legal order provides only very limited leeway for informal and voluntary mechanisms that operate outside of judicial oversight or comparable independent oversight. The use of the term "partnership" in current policy debates must therefore not distract from the fact that the calls for PPPs ultimately imply, at least in some respect, a call to reform some rights and obligations of obliged entities. Awareness of this fact is all the more important on the eve of a fundamental reform of the EU AML/CFT architecture[22] that will provide the opportunity to address some of the deficits that underlie calls for PPPs. From this vantage point, developing a framework for PPPs is not only about creating mechanisms that operate as an addition to other elements of the current architecture. Rather, it is ultimately also about adapting current laws towards a more effectiveness-driven implementation of CDD obligations. Similar considerations apply to the other primary role of public-private information sharing – namely, that of supporting ongoing investigations. The role of public-private information sharing in ongoing investigations highlights in particular a number of unresolved questions concerning the relationship between the laws of criminal procedure and AML/CFT laws. Where informal practices of public-private information sharing aimed at supporting ongoing criminal investigations are established, this may constitute an example of PPPs operating in parallel and in addition to measures of criminal procedure (i.e. measures such as judicial information requests and production orders addressed to obliged entities). Where PPPs allow FIUs to share information with obliged entities in support of a particular criminal investigation, this underscores with particular clarity the continuing uncertainty – observable in not a few jurisdictions – of the relationship between criminal justice authorities and FIUs[23] as well as the relationship between the formal gathering of evidence and the informal gathering of criminal intelligence.[24] Here again, it is unlikely that informal and voluntary mechanisms will be able to provide a legally sustainable framework for the exchange of information between competent authorities and the private sector.

IV. Policy Considerations

When designing public-private information sharing mechanisms in view of improving obliged entities' ability to detect criminal assets, policymakers should avoid and prevent practices that would ultimately weaken the thoroughness of CDD and the ability of FIUs and supervisory authorities to detect risky business practices and compliance violations. To this end, it should notably be clear that the production of valuable intelligence must never be recognised as a justification or compensation for a deficient compliance framework. Furthermore, insofar as public and private parties engage in dialogue about operational priorities for CDD or a joint determination of red flags, participating agencies must ensure that the priorities and risks thereby determined are in every case based on impartial, public-interest-focused policy considerations and reflect these agencies' mission and an up-to-date state of knowledge as regards relevant criminal threats. Participating agencies should always seek and value the experiences of the private sector and strive to improve the effectiveness of CDD by including this expertise in their own work and assisting the private side with tailored

guidance. At the same time, however, these agencies must ensure that collaboration on a joint development of priorities and risk parameters is not allowed to deflect compliance attention from business areas which, while being commercially attractive and therefore sensitive for private participants, may entail significant ML/TF risks.

As already indicated, the EU AML/CFT framework is characterised by two central objectives: the fight against crime and the protection of the integrity of the financial sector.[25] This widely recognised differentiation has profound implications for the design and functioning of AML/CFT. For while the two objectives overlap and mutually reinforce each other, they are still defined by fundamentally distinct concerns. The "fighting crime" objective is founded on the idea that financial intelligence offers rich opportunities to better detect and prosecute profit-generating criminality. Often summarised by the phrase "follow-the-money", the crime-fighting objective of AML/CFT is manifested most clearly in the mission of FIUs to analyse SARs in order to decide whether a particular suspicious activity should be further investigated. Naturally, insofar as policymakers emphasise this component of AML/CFT,[26] the quality of SAR filing is taken to be of particular importance.

In turn, insofar as policymakers emphasise the other central objective of the AML/CFT framework – namely, the protection of the integrity of the financial sector[27] – somewhat different considerations become important. The "integrity" objective reflects the conviction that it is, for multiple reasons, pivotal to prevent an inflow of criminal assets into the financial sector. This approach, in comparison to the "crime-fighting" approach, is based less on the idea that financial entities and their customer data may be useful for the detection and investigation of crime; it is based more on the concern that lawful businesses, government institutions, and wider society would be greatly endangered if criminal actors, and in particular organised criminal networks, were allowed to freely spend and invest their ill-gotten gains.[28] By assigning to financial institutions (and increasingly other types of obliged entities as well) a gatekeeper function that aims to shield the market from criminal assets and from the criminals who may exercise economic and social power through these assets, this objective focuses less on the gathering of financial intelligence. Instead, the goal of protecting the integrity of financial institutions leads AML/CFT policy to focus on the private sector's ability to prevent the inflow of criminal assets and, to this end, to focus in particular on obliged entities' compliance with their preventive duties.

The "fighting crime" and "protecting integrity" objectives of AML/CFT are of course by no means mutually exclusive but rather may ideally strengthen each other. Policymakers must appreciate, however, that solutions that are good for one objective are not necessarily desirable for the other. It is important to remember this in the present context because policy visions for the design of PPPs are frequently characterised by a one-sided focus on financial intelligence that may not be in the interest of the objective of ensuring effective compliance with preventive duties. Three areas are especially relevant in this regard: First, an intelligence-gathering focus of AML/CFT will usually prioritise the question whether SARs are adding value to criminal investigations and therefore advocate policies that reduce false positives. However, insofar as policymakers emphasise the protection of the integrity of financial institutions as being an objective equal to the goal of gathering valuable intelligence, it is far from obvious that the value of SARs should be measured exclusively based on their utility for criminal proceedings. An approach that elicits a large number of SAR filings may, for example, offer value also insofar as it can provide FIUs with a more detailed picture of potentially risky situations and thereby enhance FIUs' ability to understand individual obliged entities' risk appetite and, as a result, FIUs' ability to identify particularly risky business practices. Second, the two central objectives of AML/CFT will collide if the gathering of valuable intelligence is prioritised over the gatekeeping function of obliged entities. This would obviously be problematic from the viewpoint of an integrity-focused approach because such rewarding or *ex post* acceptance of high-risk practices would invite more frequent onboarding of such risks. Third, the more that obliged entities' customer due diligence is treated as a system

whose primary function is to respond to leads from competent authorities in order to help these authorities gather intelligence, the more this could effectively relieve these entities from their responsibility to search for relevant risks on their own initiative.

The preceding observations are not inconsistent with a more proactive AML/CFT policy in which competent authorities provide the private sector with up-to-date guidance on criminal phenomena and, in some cases, possibly also more targeted information. They do however explain that designing mechanisms of enhanced public-private cooperation requires heightened awareness of any conflicting interests at stake.[29] To this end, it is pivotal to understand that the two above-described objectives of AML/CFT essentially reflect two different and only partially overlapping visions of the role of the private sector in the fight against crime. The first vision – focusing on the production of financial intelligence – conceives AML/CFT as a surveillance instrument of the state. The second – focusing on the gatekeeping role of obliged entities – puts the emphasis on the goal of preventing the inflow of criminal assets into the legal economy. Both visions are of course intimately interlinked, given that the better the intelligence is, the greater the chances will be of detecting criminal assets. Yet, a one-sided emphasis on intelligence-gathering can also jeopardise the effectiveness of private sector prevention. It is therefore important, when examining AML/CFT in general and enhanced public-private cooperation more particularly, not to look at these issues exclusively through the eyes of investigative authorities, who will often be more interested in the gathering of intelligence than in the effectiveness of the regulatory framework. Insofar as public-private sharing is meant to contribute to ongoing investigations, it is, as already mentioned, usually not appropriate to discuss such sharing as a contribution to the effectiveness of AML/CFT compliance.

Finally, policymakers should seek to fully comprehend the actual reasons for ineffectiveness of current AML/CFT practices before deciding about the shape and scope of enhanced public-private cooperation. There can of course be little doubt that the current performance of the framework to detect criminal assets is far from satisfactory.[30] However, while it is clear that obliged entities often lack proper guidance to detect criminal assets, one should not hastily dismiss the quality of current private compliance efforts, especially at a time when new technological solutions for the analysis of bulk data signal the potential that this performance may increasingly improve. In addressing the question how to improve the current state of affairs through new forms of public-private cooperation, policymakers should consider, in particular, that failures in the detection of criminal assets are frequently not the result of insufficient compliance efforts on the part of the private sector but rather the result of insufficient performance by, and underlying inadequate resourcing of, public authorities when it comes to the assessment of the information reported by obliged entities.[31] As long as such obstacles on the public side are not remedied, increasing public-private information sharing remains unlikely to improve the detection and prevention of criminals and criminal assets that are hitherto unknown to the authorities.

V. Legal Challenges

In addition to those policy considerations, public-private information sharing in the context of AML/CFT raises a number of legal challenges for which legislators will have to provide appropriate solutions in order to ensure the sustainability of such mechanisms. Three areas deserve particular attention in this regard: data protection law, the impact of information sharing on the de-risking of obliged entities' customers, and the rights of suspects in criminal proceedings.

With regard to data protection law, there is a growing awareness among public and private stakeholders that the processing of personal data within AML/CFT has to date not been sufficiently addressed by legislators at the EU and national levels.[32] With the decline of cash as a means of payment and the ever-growing digitalisation of financial services, financial data provides increasingly detailed information about the personal life and

other activities of citizens. At the same time, one must recall that communication between FIUs and obliged entities is shielded by far-reaching tip-off obligations[33] that usually prevent customers from learning about the processing of their data by obliged entities and FIUs, thereby effectively preventing affected persons from seeking judicial or other remedies to have the reasons, methods, and outcomes of the processing as well as the accuracy of the underlying data reviewed by an independent body. Given that its main purpose is the identification of criminal suspicion and thus the initiation of criminal proceedings, and that it may therefore have a grave impact on targeted persons, the processing of personal data in AML/CFT must be taken to be of considerable gravity. This is all the more so when obliged entities are entitled or even expected to share information with other obliged entities about suspicious transactions, as a suspicion may thereby effectively give rise to the blacklisting of individuals on the basis of a suspicion, even when the suspicion has never been properly verified by the FIU or investigative authorities.[34] Without proper safeguards, public-private information sharing can significantly increase these existing tensions between data protection law and AML/CFT in that it effectively involves state authorities in obliged entities' processing of data.[35] Depending on the scope and purpose of information sharing, authorities may then effectively control the processing of obliged entities' data records, thereby escalating proportionality concerns.[36] Particular concerns in this regard arise insofar as public-private information sharing is aimed at or results in profiling, thereby categorising individuals in ways that expose them to a heightened risk of being subjected to repressive measures or stigmatised in commercial activities. Such concerns should not be a reason not to develop gateways for information sharing. In fact, greater commitment of competent authorities to obliged entities' AML/CFT compliance may in some respects also offer opportunities to reduce current data protection deficits. Post-SAR feedback may, for example, help to ensure that customers do not permanently suffer the consequences of an erroneous risk assessment. However, there can be little doubt that the expansion of AML/CFT through public-private information sharing poses additional challenges to an AML/CFT framework that, already in its current form, frequently struggles to find the right balance between criminal policy needs and data protection law. Defining appropriate rules for public-private information sharing therefore requires prudence to ensure that AML/CFT becomes both more effective and legally sustainable.

Similar to the above-described issues under data protection law, public-private information sharing also highlights questions around existing de-risking practices – that is, the termination of business relationships by obliged entities for the purpose of managing ML/TF risk. To appreciate this point, one must remember that AML/CFT constitutes, among other things, a preventive framework whose enforcement is largely assigned to the private sector. This enforcement takes the form of the requirement that obliged entities abstain from business relationships when they determine that assets are related to criminal activity[37] or when they are unable or unwilling to perform adequate CDD.[38] While the resulting private de-risking practices can sometimes be problematic insofar as they could constitute unlawful discrimination,[39] the current framework benefits from the fact that private entities are, by virtue of their freedom of contract, in principle free not to continue a business relationship with particular customers.[40] By relying on the private sector for ML/TF prevention, legislators thus effectively take advantage of the greater scope of action available to private entities, who are most of the time much less constrained than competent authorities by fundamental rights considerations.[41] This flexibility may however be lost if obliged entities' risk management and de-risking is decisively determined or even just influenced by public-private information sharing. That is, the more that business relationships are terminated or otherwise negatively impacted as a result of information that the obliged entity received from the authorities, the more these consequences will be attributed to the state.[42] In such cases, the lack of meaningful remedies against de-risking that prevails under current AML/CFT laws would become particularly difficult to justify. Rules on public-private information sharing could of course anticipate this by prohibiting de-risking on the basis of particular information shared by the authorities. However, such limitations might be much easier to define than to enforce in practice, given that the reasons for the termination of a business relationship will often remain ambiguous. Insofar as public-private information

sharing is further developed, legislators may therefore have to give thought to how to improve customers' rights against private preventive measures.

Finally, public-private information sharing can have a profound impact on the relationship between criminal investigations, FIUs, and obliged entities' compliance. Historically, information flows in the AML/CFT framework have in essence been designed as a one-way street through which obliged entities generate financial intelligence that, in suspicious cases, is forwarded to the FIU and then possibly on to criminal justice authorities. This setup, however, is fundamentally changed if information is flowing in both directions, including possibly from criminal investigations to FIUs and to obliged entities. If information is allowed to flow in both directions, FIUs' operational analysis and obliged entities' CDD could effectively be transformed into a surveillance and intelligence gathering framework that may be triggered by information generated in criminal proceedings[43] and may ultimately serve those proceedings but will at the same time, in principle, not operate under the rules of criminal procedure law. Insofar as this leads to the gathering outside of criminal proceedings of information for the furtherance of criminal proceedings that are already ongoing at the time of the public-private sharing, legislators will need to define the relationship between both legal frameworks and regulate how information obtained with the help of obliged entities can be used. In particular, insofar as the information generated by obliged entities' CDD can, under the rules of the applicable criminal justice system, be used as evidence, public-private information sharing may result in the circumvention of rights provided to suspects under criminal procedure law. Under such a scenario, affected rights could include, for example, those guaranteeing judicial authorisation or at least judicial oversight of the requisition of documents. One of the attractions of the use of FIUs and CDD as a de facto investigative tool may, in fact, lie in the flexibility of data gathering under AML/CFT laws. Given that AML/CFT is subject to extensive confidentiality obligations, suspects may then, however, be prevented from understanding how particular incriminating evidence was produced. Moreover, insofar as public-private information sharing leads an obliged entity to inquire into a customer's activities, possibly by requesting information directly from the customer, the entity may effectively act as an informant of investigative authorities without its action being subject to judicial or other impartial oversight.[44] Though different national jurisdictions may allow for different degrees of flexibility in this regard, especially the public-private sharing of information regarding particular suspects suggests a need to clarify the respective roles of investigative authorities and FIUs. This would ultimately invite a stronger emphasis on the distinction between evidence-gathering and the gathering of mere criminal intelligence. Not least for the sake of safeguarding defence rights, any sharing of information aimed at supporting ongoing investigations would then naturally fall to investigative authorities. The role of FIUs would then, in turn, be limited to the sharing of information aimed at improving obliged entities' risk management – a division of competences that would also prevent FIUs from getting too intimately involved in criminal investigations and thereby putting the confidentiality of their communication – not least with obliged entities and foreign partners – at risk of being compromised.[45]

VI. Outlook

To summarise, one should recall that the introduction of public-private information sharing mechanisms raises complex questions both as regards the determination of AML/CFT policy and as regards the drafting of an adequate legal framework. It is, to this end, particularly important to clearly differentiate between the function of the AML/CFT framework to protect the financial system from criminal assets and the function of this same framework to support criminal investigations. These two functions must not be confused, because the distinction between them is key for deciding about the design of public-private sharing. In the latter case, such sharing is ultimately about the design of criminal procedure law, while in the former case it is about improving the performance of the regulatory framework. While a public-private information sharing policy must certainly deal with important limitations, especially from data protection law, policymakers will

also need to recognise that, in a globalised world, reliance on closer cooperation with the private sector can offer promising opportunities to address today's challenges resulting from transnational organised crime, terrorism, and malign state actors. However, as explained, enhancing the role of public-private sharing will require legislators to address legal deficits of existing AML/CFT laws. Otherwise, public-private sharing could lead to an exacerbation of existing problems that would then sooner or later damage the AML/CFT system instead of improving it.

---

1. Art. 6 paras. 1–3 and 5, Art. 7 paras. 1 and 4(a)(e) of Directive (EU) 2015/849 of 20 May 2015, *O.J.* L 141, 5.6.2015, 73 as amended by Directive (EU) 2018/843 of 30 May 2018, *O.J.* L 156, 19.6.2018, 43.↩
2. Arts. 17 and 18(4) of Directive (EU) 2015/849, as amended by Directive (EU) 2019/2177, *O.J.* L 334, 27.12.2019, 155.↩
3. Art. 46 para. 2 of Directive (EU) 2015/849.↩
4. Art. 46 para. 3 of Directive (EU) 2015/849.↩
5. European Banking Authority, "Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The ML/TF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849, 1 March 2021, <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf>. All hyperlinks in the endnotes of this article were accessed on 24 March 2022.↩
6. See for example FATF, Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing of September 2020.↩
7. For comprehensive accounts, see N. Maxwell and D. Artingstall, "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime", *RUSI Occasional Paper*, 2017, <https://rusi.org/explore-our-research/publications/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime>; N. Maxwell, "Expanding the Capability of Financial Information-Sharing Partnerships", *RUSI, Occasional Paper*, 2019, <https://rusi.org/explore-our-research/publications/occasional-papers/expanding-capability-financial-information-sharing-partnerships>.↩
8. See already P. Reuter and E. Truman, *Chasing Dirty Money: The Fight against Money Laundering*, 2004, pp. 176–177.↩
9. For an analysis of tactical information sharing mechanisms, see the categorization in N. Maxwell, "Five years of growth in public–private financial information-sharing partnerships to tackle crime", *Future of Financial Intelligence Sharing (FFIS)*, 2020, p. 13 < https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2020.pdf>.↩
10. For an example of the sharing by investigative authorities of tactical information for the purpose of identifying offenders, see Bundesverfassungsgericht (BVerfG) [German Federal Constitutional Court], (2009) *Neue Juristische Wochenzeitschrift (NJW)*, 1405, 1407.↩
11. See A. Verhage, "Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry", (2009) 52 *Crime, Law and Social Change,* 29–30; A. Amicelle and V. Iafolla, "Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing", (2018) 58(4*) The British Journal of Criminology*, 855–857.↩
12. W. Laufer, "Corporate Liability, Risk Shifting, and the Paradox of Compliance", (1999) 52 *Vanderbilt Law Review*, 1402–1404.↩
13. See N. Ryder, "Is It Time to Reform the Counter-terrorist Financing Reporting Obligations? On the EU and the UK System", (2018) 19 *German Law Journal,* 1185–1186.↩
14. For a critique of this tick-the-box approach, see European Banking Federation, "Lifting the Spell of Dirty Money: EBF blueprint for an effective EU framework to fight money laundering", *EBF*, 2020, < https://www.ebf.eu/wp-content/uploads/2020/03/EBF-Blueprint-for-an-effective-EU-framework-to-fight-money-laundering-Lifting-the-Spell-of-Dirty-Money-.pdf> , 4.↩
15. B. Vogel and J. Maillart, "National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection", 2020, <https://pure.mpg.de/rest/items/item_3262446_6/component/file_3286393/content> accessed 24 March 2022, pp. 911-1024.↩
16. Ibid., pp. 924-925; see also European Data Protection Supervisor (EDPS), "Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing", 23 July 2020 <https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf> para. 38-41.↩
17. Art. 13 para. 1 s. 1 (d) and Art. 18 para. 2 s. 2 of Directive (EU) 2015/849 of 20 May 2015, as amended by Directive (EU) 2018/843 of 30 May 2018.↩
18. B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 930-934.↩
19. Ibid., pp. 1021-1024.↩
20. See Art. 46 para. 3 of Directive (EU) 2015/849; for the lack of feedback in current practice, see European Commission, "Commission Staff Working Document Impact Assessment accompanying the Anti-money laundering package", SWD(2021) 190 final, p. 12.↩
21. For a detailed account of the various types of information shared within PPPs for the purpose of improving obliged entities' risk detection, see N. Maxwell*, op. cit.* (n. 9), 26-84.↩
22. European Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010", COM(2021) 421 final.↩
23. For a clarification of FIUs' access to law enforcement data, see now European Commission, "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", COM(2021/) 423 final, recital 47 and Art. 18 para. 1(c).↩
24. See B. Vogel (ed.), *Secret Evidence in Criminal Proceedings: Balancing Procedural Fairness and Covert Surveillance*, 2021.↩

25. See recital 1 of Directive (EU) 2015/849 and recital 1 of Directive (EU) 2018/1673. On the somewhat inconclusive historic origin of the AML framework, see P. van Duyne, H. Harvey and L. Gelemerova, *The Critical Handbook of Money Laundering: Policy, Analysis and Myths*, 2018, pp. 41–90.↩
26. See Europol, "From Suspicion to Action, Converting financial intelligence into greater operational impact", *Financial Intelligence Group*, 2017, <https://www.europol.europa.eu/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf accessed 24 March 2022>, 29–30.↩
27. To this effect European Commission, "Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions", COM(2019) 373 final.↩
28. See the preamble of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988, United Nations Treaty Series, vol. 1582, p. 95; see also P. van Duyne, "Money laundering policy: fears and facts", in P. van Duyne, K. von Lampe and J. Newell (eds.), *Criminal Finances and Organised Crime in Europe*, 2003, p. 76.↩
29. For an illustration, see Deloitte/Institute of International Finance, "The global framework for fighting financial crime: Enhancing effectiveness & improving outcomes", *The Institute of International Finance and Deloitte LLP White Paper*, Issue 06/2020, <https://www2.deloitte.com/content/dam/Deloitte/tw/Documents/financial-services/tw-the-global-framework-for-fighting-financial-crime-en.pdf> where the added value of PPPs is explained by the conceptual starting point that "a government's 'victim of crime' is usually a bank's 'customer'. […] both parties, public and private, have an interest and an obligation to work in support of each other in protecting that person and the public more widely". Such a claim can be misleading. For it overlooks that, for the purpose of preventing and detecting money laundering, a bank's customer is first and foremost relevant insofar as s/he is a perpetrator.↩
30. To this effect already KPMG, "Money Laundering: Review of the Reporting System", *Cja/NCIS web site and report wording*, 2003, <https://www.dematerialisedid.com/PDFs/kpmgreport.pdf>↩
31. See FATF, "AML/CFT and public-private sector partnership", *FATF*, 2016, <https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-private-sector-partnership.html>, adding that "[i]t has not helped that the governments have lost large numbers of their experts to the banks."↩
32. See European Commission, "Commission Staff Working Document Impact Assessment accompanying the Anti-money laundering package" SWD(2021) 190 final, pp. 52-55.↩
33. Art. 39 para. 1 of Directive (EU) 2015/849.↩
34. See notably EBA, "The ML/TF Risk Factors Guidelines of 1 March 2021", *op. cit.* (n. 5), para. 2.5, which explicitly mentions allegations of criminality against the customer as a potentially relevant risk factor, and further specifies that "[f]irms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing."↩
35. See also EDPS, "Opinion 5/2020", *op. cit.* (n. 16), para. 41-47.↩
36. B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 927-928.↩
37. Art. 35 para. 1 of Directive (EU) 2015/849; Art. 3 para. 1 of Directive (EU) 2018/1673.↩
38. See Art. 14 para. 4(1) of Directive (EU) 2015/849.↩
39. See European Data Protection Supervisor (EDPS), "Opinion on a proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds", 4 July 2013, <https://edps.europa.eu/data-protection/our-work/publications/opinions/prevention-money-laundering-and-terrorist-financing_en > para. 78; T. Durner and L. Shetret, "Understanding bank de-risking and its effect on financial inclusion", *Oxfam*, 2015, <https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf> pp. 9–12.↩
40. See D. Artingstall, N. Dove, J. Howell and M. Levi, *Drivers & Impacts of Derisking*, 2016, pp. 17–27.↩
41. But see B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 964-965 on the horizontal effect of the right to non-discrimination.↩
42. See ECtHR (Grand Chamber), 3 April 2012, *Kotov v. Russia*, Appl. no 54522/00, paras. 102–103.↩
43. For more on possible covert surveillance of customers as a result of the interplay between FIUs and obliged entities: B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 904-911 and 923-925.↩
44. To this effect also EDPS, "Opinion 5/2020", *op. cit.* (n. 16), para. 41-45.↩
45. B. Vogel and J. Maillart, *op. cit.* (n. 15), p. 943.↩

* Author statement

Research for this article has been funded by the European Union's Internal Security Fund – Police. The content of this study represents the views of the author only and is his sole responsibility. The article is an amended version of the author's response to the Commission, which was submitted as part of its public consultation on 27 July 2021 to receive guidance on the rules applicable to PPPs within the framework of preventing and fighting money laundering and terrorist financing.

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