JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–28
doi: 10.1093/cybsec/tyab004
Research Paper

Research Paper

Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces

Iwona Karasek-Wojciechowicz *

Faculty of Law, Jagiellonian University in Krakow, 24 Golebia Street, 31-007 Kraków, Poland

*Correspondence address. Faculty of Law, Jagiellonian University in Krakow, 24 Golebia Street, 31-007 Kraków, Poland. Tel: +48-6-01-44-04-44; E-mail: iwona.karasek@uj.edu.pl

Received 19 March 2020; revised 17 August 2020; accepted 25 January 2021

Abstract

This article is an attempt to reconcile the requirements of the EU General Data Protection Regulation (GDPR) and anti-money laundering and combat terrorist financing (AML/CFT) instruments used in permissionless ecosystems based on distributed ledger technology (DLT). Usually, analysis is focused only on one of these regulations. Covering by this research the interplay between both regulations reveals their incoherencies in relation to permissionless DLT. The GDPR requirements force permissionless blockchain communities to use anonymization or, at the very least, strong pseudonymization technologies to ensure compliance of data processing with the GDPR. At the same time, instruments of global AML/CFT policy that are presently being implemented in many countries following the recommendations of the Financial Action Task Force, counteract the anonymity-enhanced technologies built into blockchain protocols. Solutions suggested in this article aim to induce the shaping of permissionless DLT-based networks in ways that at the same time would secure the protection of personal data according to the GDPR rules, while also addressing the money laundering and terrorist financing risks created by transactions in anonymous blockchain spaces or those with strong pseudonyms. Searching for new policy instruments is necessary to ensure that governments do not combat the development of all privacy-blockchains so as to enable a high level of privacy protection and GDPR-compliant data processing. This article indicates two AML/CFT tools which may be helpful for shaping privacy-blockchains that can enable the feasibility of such tools. The first tool is exceptional government access to transactional data written on non-transparent ledgers, obfuscated by advanced anonymization cryptography. The tool should be optional for networks as long as another effective AML/CFT measures are accessible for the intermediaries or for the government in relation to a given network. If these other measures are not available and the network does not grant exceptional access, the regulations should allow governments to combat the development of those networks. Effective tools in that scope should target the value of privacy-cryptocurrency, not its users. Such tools could include, as a tool of last resort, state attacks which would undermine the trust of the community in a specific network.

Key words: permissionless blockchain; permissionless DLT; anti-money laundering; AML; personal data protection; privacy; right to be forgotten

Introduction

The last two decades have seen the intensive global development of measures to fight money laundering, terrorist financing and counter financing of the proliferation of weapons of mass destruction [anti-money laundering and combat terrorist financing (AML/CFT)], which are in constant tension with the protection of privacy. The primary sources of global AML/CFT policies are standards and recommendations of Financial Action Task Force (FATF). The FATF members, which are governments and supra-national regional organizations, currently represent major financial centres in all parts of the world. The FATF standards and recommendations form the most influential global AML/CFT policies in effect today. They do not bind directly the individuals and organizations but the FATF members are obliged to implement these standards and recommendations in their national legislation [1]. In that way there become binding for individuals and organizations. In the EU, the FATF policies and standards are implemented in the AML Directives [2]. I do not refer in this article to the provisions of national regulations because the source of the problem analysed here lies at a higher (global) level, namely, in the policies set up by FATF.

The last few years have also seen intensive developments concerning data/privacy protection regulations. The EU General Data Protection Regulation (GDPR) [3] is one of the most stringent standards [4, 5] in this area. It has inspired more and more new regulations globally, also including certain US state laws [6, 7] and Chinese regulations [8]. Therefore, this model of regulation has a massive impact on shaping global technology. In contrast to the AML/CFT area, there is no comparable global inter-governmental organization which sets the global standards for regulations in the realm of data/privacy protection. Thus, to analyse the interplay between the global AML/CFT policy and data/privacy protection law, I could not refer to any global data protection standard. The global models of data/privacy protection are developed in a non-centralized way: more and more countries, adopting their data protection regulations, shape these regulations in a way more or less similar to the GDPR, as one of few models of regulation. Therefore, the GDPR, being a binding law in the EU, becomes at the same time one of the few influential global standards for data protection regulations [5]. Its broad territorial scope of application also determines its global significance.[1] Thus, an analysis of the interplay between global AML/CFT policy and the GDPR as one of the global standards for data protection regulation—the scope of this research—is both justified and practically significant.

There is a constant tension between personal data protection and crime-prevention policies. The 1990s were a battleground for Internet openness, one in which law-enforcement bodies lobbied for providers of data and communication services to engineer their products so that they were guaranteed access to all data ('exceptional access') [9]. A compromise has been achieved, which shares similar characteristics in many countries around the world. Generally speaking, the Internet was left as a space free from direct instruments enabling law enforcement, such as exceptional access [9], while within the financial services sector, the protection of public interest has prevailed over ensuring privacy. Financial institutions and providers of asset management services have become "obliged entities" under the AML/CFT regulations, being obliged to apply measures to minimize the risks of money laundering and terrorist financing (ML/FT). These duties include an obligation to identify and, to some extent, to verify the identity of their clients, commonly referred to as 'Know Your Customer' (KYC). There is also an obligation to continually monitor clients' activities to identify ML/FT risks and report the outcomes of these analyses to national financial intelligence units (FIU).

Obliged entities are required to have a permanent 'exceptional access' to customer data, including details of their customers' transactions. The FIU do not have direct access to the operating systems of financial service providers, but they do receive suspicious activity reports, which are provided by obliged entities. The scope of obliged entities has been constantly expanding over the years. Functionally, this tool ensures 'exceptional access' of state authorities to the personal data gathered by obliged entities. Moreover, this access is connected with customers' KYC obligations imposed on service providers. The costs of complying with these auditing and reporting requirements for obliged entities are so huge that for several years, obliged entities proposed that governments should take over direct 'exceptional access' to their operating systems, thereby potentially removing a significant part of their costly reporting obligations [10]. The EU policymakers are already exploring opportunities to automate such supervisory processes and to create direct automated reporting utilities (so-called regulatory technology) [11, 12] based on permissioned distributed ledger technology (DLT). Embedded supervision may result in governments taking over 'exceptional access' to the operating systems of financial services providers. Presently, however, governments have already ensured 'exceptional access' based on the reporting obligations of obliged entities.

At the same time, entities which are obliged to implement AML/CFT measures are also obliged to ensure data protection as required by data protection regulations; for example, by the GDPR, if applicable. In case of conflict between those two protected values, the GDPR recognizes the primacy of AML regulatory tools.[2] The reconciliation of those duties placed on obliged entities by both groups of regulations results in a necessity of ensuring very high standards of protection against unauthorized data access and, at the same time, a necessity of providing safe 'exceptional access' that allows such entities to monitor their clients and to report to the supervisory bodies. For example, banks are not allowed to implement end-to-end encryption of transactional data generated by their clients. Some briefly mentioned characteristics of AML/CFT policy show that the policy is currently based on obligations imposed on service providers (intermediaries), which enable the FIU to access these surveillance data.

The above-mentioned mechanism has ensured the protection of data gathered by intermediaries, as well as achieving the goals of AML. It worked well until permissionless blockchains[3] emerged and cryptocurrencies[4] began to be used for payment or investment purposes. Unlike the Internet, the space of permissionless blockchains is designed for the transfer of value. According to some views, the permissionless blockchain spaces can be a world without intermediaries [14–16], but in fact new categories of intermediaries (such as decentralized exchanges, wallet providers, and decentralized applications

1 Article 3 GDPR.

2 Recital 19 GDPR.

3 This article covers the whole of distributed-ledger technologies (DLT), though the term is used interchangeably with the term 'blockchain' in this paper, which is the most well-known type of DLT.

4 In this article, I use the term 'cryptocurrency' to refer to schemes characterised by the following features: decentralised organization governed by a network protocol, cryptography as means to secure transactions, and a public ledger that documents the system's state and history [13]. The category of 'cryptocurrency' includes also 'virtual assets', which are defined below.

operators) have appeared in and around DLT ecosystems [16, 17]. Because permissionless DLT-based systems must include intermediaries to maintain the wide acceptance of their cryptocurrencies, the AML/CFT duties imposed on intermediaries are still necessary.

When parties transact peer-to-peer using non-custodian wallets, key financial transactional data have been written on a blockchain ledger. The content of these publicly viewable ledgers has become the essential source of information for intermediaries which are obliged to verify the ML/FT risks. Intelligence agencies monitor blockchain ledgers which store details of all transactions (their proofs). These entities try (sometimes successfully) to detect the ML/FT risks by analysing the content of blockchain ledgers and enormous amounts of external data (as far as available), based on the use of advanced analytical mechanisms and technologies [18–22]. Access to resources needed to conduct such analysis differs between states and intelligence companies. As a result, intelligence does not often succeed with re-identification of suspected users or ML/FT risks.

We now come to a source of one of the challenges concerning permissionless blockchains. To ensure data confidentiality in a publicly viewable database (blockchain ledgers), the GDPR requires, in general terms, very strong capacity for 'masquing' personal data on ledgers to prevent unauthorized access and identification of data subjects. In contrast, AML/CFT policy combats anonymity-enhanced technologies and mechanisms that hinder or prevent law enforcement agencies from identifying users and connecting and tracking transactions on blockchain ledgers. Thus, in my opinion, the GDPR thereby pushes permissionless blockchains to ensure strong pseudonymization or anonymity, while the AML combats the strong pseudonymization or anonymity with the aim of being able to analyse the ledgers' content. These very general observations are a starting point for further analysis regarding transparency versus anonymity requirements as regards the permissionless DLT-based networks.

Policy makers have not addressed this concern thus far. Sometimes it is mentioned but not further analysed. For example, Finck, in her Study for the EU Parliament, indicates that if any 'anonymization' technology is able to reach the GDPR's anonymization threshold, in turn, 'the resulting anonymity can be problematic when examined through the lens of other policy requirements, such as that of tax evasion or antiterrorism legislation' [23]. However, Barsan dives deeper into that problem and proposes a solution [24] which is analysed in this article in section 'Searching for solutions—analysis of existing proposals'.

The following sections begin with a short description of users' identification possibilities in permissionless networks. Then I present the basics of GDPR, showing with more detail how the GDPR is related to actors in the blockchain space. The possible ways for the GDPR-compliant processing of data on publicly viewable blockchains ledger are analysed. The focus is mostly concentrated on the determination of the GDPR' threshold of data anonymity. These sections, mostly descriptive, also includes my own analysis. Next, the FATF's AML/CFT global policy towards permissionless blockchains is presented as well as its impact on shaping permissionless network development. Then, the tensions between the regulations are analysed, as well as the impact on data/privacy protection. Already existing approaches aimed at reconciling the GDPR with AML/CFT policy concerning permissionless DLT-based platforms are briefly presented and analysed. Finally, my proposal towards such solutions is presented along with a discussion on arising concerns.

Transparency versus anonymity: The identification of parties to transactions on permissionless blockchains

The FATF, in accordance with the G20 (point 17 in [25]), stresses that anonymity risks have emerged in decentralized systems [26]. Consequently, measures for combating anonymity-enhanced cryptocurrencies and their underlying technologies must be developed and implemented into national systems (point 98 in [27]. At the same time, the EU Blockchain Observatory states that '[t]here is often a misconception that users of blockchain-based platforms are anonymous and therefore can act with impunity. Quite the contrary, platforms like Bitcoin offer pseudonymity at the most' [17].

Such contradictory statements concerning the anonymity in blockchain spaces result from a differing understanding of the concept of 'anonymity' adopted by the GDPR when compared with AML/CFT policies. The GDPR sets the anonymity threshold very high [28]. Therefore, from the perspective of the GDPR, the vast majority of DLT permissionless implementations—if not all of them [29, 30]—only ensure the pseudonymization of data written on blockchain ledgers. The FATF recommendations are not coherent nor precise in distinguishing anonymization techniques from those that guarantee strong pseudonymization. Sometimes such a distinction is made (point 98 in [27]), but usually AML/CFT recommendations use the term 'anonymity' to cover both strong pseudonymization and anonymization technologies and their data-masquing outcomes. Thus, anonymity under AML/CFT policies means, both (i) the impossibility or near impossibility of linking data on a ledger with an identified person(s), and also (ii) a situation when such a linking is 'only' significantly hampered (point 4 in [27]). In a situation when data on public ledgers are qualified only as pseudonymous under the GDPR, law enforcement agencies may not be able to quickly identify the person hidden behind these specific pseudonymous data, for example, under a Bitcoin or Monero address, to effectively mitigate the AML/CFT risks. The AML/CFT policies tend to understand anonymous data or anonymization technologies very broadly. Therefore, the same data could be qualified as pseudonymous under the GDPR and as anonymous under AML policies. We should bear that difference in mind, because it can lead to misunderstandings in the debate between policy makers and researchers in the scope of data protection and AML.

Moving now to the transparency issues in blockchains, it should be emphasized that, because of the technological diversity of DLT, the chances of users' identification by law enforcement agencies differ significantly between networks and also inside the individual systems. The traceability and linkability of the transactions are impacted by many factors—which, ultimately, and along with accessible data external to the public ledgers—can (but do not necessarily) lead to user identification. State intelligence agencies and private companies alike build tools to identify users of permissionless networks based on the linkage data on ledgers with external data available in public space and also by using machine learning and statistical modelling [30]. Research projects have been launched to develop novel data-driven techniques and solutions designed to support law enforcement agencies charged with investigating criminal or terrorist activities that involve virtual currencies [31]. As the most 'transparent' blockchains (regarding the chances for transactions traceability and users' identification), are generally considered these public ledgers that reveal the public addresses of the parties and the value of the transaction concerned [32]. One example is the Bitcoin blockchain, which keeps publicly viewable data that, when

combined with external data, provide a relatively high chance of identifying users (in comparison to other blockchain networks).

Conversely, in terms of the probability of identifying peer-to-peer transaction parties, networks can deploy anonymity-enhanced or strong pseudonymization technologies on the protocol level. These are all commonly referred to as 'anonymous', 'privacy-preserving' [33] networks or 'privacy-blockchains'. Examples of the most advanced anonymity-enhanced technologies and solutions available today include homomorphic encryptions, multi-party computation [34], ring signatures [35], bulletproofs [36], and a range of zero-knowledge proofs [37–40]. Some of these technologies already address future risks that are likely to arise due to the rapid development of quantum computing [41].

Many privacy-preserving networks constantly improve their anonymity-enhanced features. After assessing the Monero networks as enabling a quite high level of traceability of transactions [42, 43], the community implemented several protocol changes in the protocols and network architecture. Their effectiveness was reassessed in 2019, and the researchers who carried out the assessment found that Monero was currently resistant to tracking and tracing methods that applied to other cryptocurrencies [30]. However, no precise delimitation is possible between transparent and privacy-focused blockchains. Rather, these two types of blockchains are at the beginning and end of a scale; between these two points, other networks can be located in different places. The likelihood of law enforcement agencies identifying users varies from high to extremely low, both within and among systems. Initially, the most popular blockchains were highly transparent, and some recently created networks, such as Ethereum 2.0, deploy anonymity-enhanced technologies at the protocol level [44].

Solutions implemented at the protocol level are not the only essential factors regarding user traceability. Users also obfuscate the origin of coins individually using other mechanisms, which can hinder or entirely prevent the user from being identified. Examples of these mechanisms include 'good practice' concerning the one-time use of addresses [45], as well as using other tools such as mixers, tumblers, or similar. Such mechanisms can be developed and used independently by users or group of users. Users alternatively have at their disposal services provided by third parties or by autonomous smart contracts, like lightning networks, shapeshifting, or cross-chain transaction tools that can also be used on transparent blockchains. Researchers continuously develop methods of tracing transactions when such services are used [46], also developing risk scoring models related to following the coins derived from illicit activity [47].

GDPR basics

In this section, simplified and basic information regarding the GDPR is provided for the readers not familiar with that regulation.

It is often said that the GDPR gives control of personal data back to the owners (data subjects) by established, comprehensive, and general obligations of data controllers and processors [48]. Controllers and processors are obliged to process the personal data in compliance with some core principles of the GDPR. A data subject has a set of rights against the (joint) controllers and processors. The rights and obligations are not limited to the use of any particular technology or method of data processing. The GDPR adopts a technology-neutral approach, setting out the required general effects (principles of data processing and data subjects' rights) without prescriptions for how they may, and how they should, be achieved. If a controller or a processor breaches their obligations or violates any data subject's rights, compensation can be awarded and supervisory bodies may punish the violations by means of a severe fine.

'Personal data' is 'any information relating to an identified or identifiable natural person', where an 'identifiable person' is a natural person who 'can be identified, directly or indirectly'. The notion of personal data includes pseudonymized personal data as well, that is, data which 'can no longer be attributed to a specific data subject without the use of additional information'. Anonymous data stay outside of the GDPR's scope of application. The 'processing' of data means any operation or set of operations performed upon data, such as collection, recording, storage, use, disclosure by transmission or dissemination, erasure, or destruction.

The general rules of data processing by controllers and processors include, among others:

i. Lawfulness of data processing: processing needs a legal base; the legal basis are limited by the GDPR[5] including, for example, (a) consent of data subject, (b) complaining by a controller with legal obligations, or (c) the necessity of data processing' for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data'.
ii. Purpose limitation: data should be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'.
iii. Data minimization: processed data should be 'adequate, relevant and limited to what is necessary for the purposes for which they are processed'; the controller 'shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'.
iv. Transparency of data processing: data subjects should be informed about, among other things, how and by whom the data will be processed, for which purpose, to what extent the personal data are or will be processed; data breach notifications should be sent to data subjects and supervisory bodies within short periods;
v. Data confidentiality: personal data must be processed in a manner that ensures their security, 'including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures'.
vi. Accountability: the data controller is responsible for, and should be able to demonstrate compliance with, the duties of controllers.

The rights of data subjects against (joint) controllers and processors include, among others:

i. To be informed regarding the controller's identity and contact details, purposes of the processing, data recipients, transferring the data to third countries, and so on.
ii. To object to data processing; that right is important when data are processed solely on the legal basis of satisfying the controller's 'legitimate interests': when a data subject objects to data processing in such a situation, 'the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override

5 Article 6(1) GDPR.

the interests, rights, and freedoms of the data subject or for the establishment, exercise or defense of legal claims'.

iii. Right to be forgotten;[6] when a data subject invokes that right, the data controller and data processor are obliged 'to erase' the personal data if a valid legal basis for further processing does not exist.

When the GDPR meets DLT, the extremely controversial arises of whether it is possible at all to comply with the data subject's right to be forgotten [49]. I will come back to that issue with further details in the context of immutable distributed ledgers. Here I indicate in general terms, that a data subject should have the right 'to be forgotten' where the retention of his or her personal data infringes the GDPR. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with the GDPR.[7]

The GDPR also introduced the rules regarding the relations between (joint) controllers and processors, as well as regulation of data transfers to third countries or international organizations. Some of those issues are presented in the subsection below. (For more on the GDPR in general, see, for example, Kuner *et al.* [50], and in the context of the DLT, see Finck[23]. For a presentation highlighting the different approaches between the GDPR and US privacy law, see Hoofnagle *et al.* [51].

How does the GDPR relate to the blockchain actors?

This section presents a summary of the current state of discussion that asks: how can it be determined which persons in and around decentralized blockchain networks are to be subsumed under the respective terms of the GDPR? I also consider the implications of the recent development in the case law of the Court of Justice of the European Union (CJEU) when drawing conclusions.

Data written on immutable and publicly viewable blockchain ledgers include legal and illegal content, including child abuse images [52]. Many of these data are also personal data. Personal data may be information written on a ledger in plain text, as well as in the form of hashes. Many hashes on ledgers can be attributed to an identifiable person using ledger analysis or additional external resources [53]. As a rule, hashes are considered to be pseudonymized personal data [53–55]). According to the single opposing view [54], hashes on DLT-based ledgers cannot be qualified as personal data because these data are not used for concealing identities but for solving a technical problem: the double-spending problem. It must, however, be underlined that according to the GDPR, data attributed to an identifiable person are to be qualified as personal data, regardless of the purposes for which they are used. As a rule, no purposes of personal data use exempt such data from the GDPR's scope, unless an exemption is established by law. Thus, in a typical situation, every node in the DLT-based system processes a massive amount of personal data. Users of permissionless networks, validators, and miners usually serve as node operators when they install blockchain clients and full or partial data ledgers. By 'users of permissionless networks' I mean here the end users as well as the business users (intermediaries) like decentralised applications (dApp) operators, for example, decentralised exchanges (dExchanges) or wallet providers. There is already a scientific debate whether and, if so, which of mentioned persons in and around decentralized blockchain systems should be qualified as a controller, joint controller, or processor. When one starts using a permissionless DLT-based network, it is essential to assess the risk of one's own liability for GDPR non-compliance, unless one believes that one will stay unidentifiable or unreachable for the law enforcement bodies and will avoid any liability.

The GDPR defines a data controller as a person 'which, alone or jointly with others, determines the purposes and means of the processing of personal data'; joint controllers are two or more controllers who jointly determine the purposes and means of processing. 'Processor' means a person who 'processes personal data on behalf of the controller'. The CJEU has emphasized many times the need to adopt a broad definition of controllership (para. 28 in [56]) and joint controllership [57] to ensure the effective and complete protection of data subjects.

The CJEU emphasizes the necessity to qualify a person as a (joint) controller or processor taking into account all circumstances of a given case. In this regard, the following comments are only very general indications. The qualification of network communities' group of members (end users, business users, miners and validators, developers) may be different in a specific case and may be different even between members of each group. It depends primarily on the level of decentralization of network governance, which differs significantly from network to network and inside the same networks may vary over time.

According to an almost unanimous view among academics, a user who sends personal data (related to others) to the DLT-based network is a controller of these data (para. 23 in [23, 58, 59]. That statement is in line with CJEU case law. A person, only by 'creating opportunity' for another person to process specific data, determines the purposes and means of the processing. As a result, they are both joint controllers (para. 35 in [56]). In the 'Jehovan todistajat' case, the CJEU stated that a person who exerts influence over the processing of personal data by others for their own purposes and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller (para. 69 in [57]).

That rule was recalled in the recent 'Fashion ID' case. By embedding the Facebook 'Like' button on its website, the company Fashion ID has exerted 'a decisive influence' over the collection and transmission of website visitors' personal data to the provider of that plugin, which would not have occurred without that plugin (paras 74–78 in [60]). It may be claimed that a DLT-based network user who sends, or orders an intermediary to send, the personal data to that network, exerts a decisive influence on processing these data by all network nodes, miners, or validators, even if any of them, acting alone, has no critical control over further data processing.

Some experts suggest that node operators, miners, and validators should be qualified only as processors [23, 61]. Others argue that the nodes' operators are joint controllers, similar to the SWIFT operator which many experts have seen as a processor but which was finally qualified as a joint controller ([23, 59, 62]. Differences in the

6 Article 17 GDPR.

7 Recital 65 GDPR.

qualification of blockchain communities' members may have objective and factual grounds: that is, differences inside the individual networks' communities. As the Article 29 Working Party (A29WP)[8] has pointed out, the concept of controllership 'is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis' [63].

Thus, if in a given case the community members jointly determine the goals of data processing, or, at least, if they jointly exert a 'decisive influence' over the means, I would say that in such a case all members of a network's community who take part in off-chain network governance may be qualified as joint controllers of personal data written on a DLT ledger. 'Means' in the context of permissionless blockchains refers to a software, its protocol, the network architecture, and the ledger.

The CJEU stated that the 'Fashion ID' case that a person cannot be considered a controller in the context of operations that precede or are subsequent in the overall chain of data processing operations, for which that person does not determine either the purposes or the means (para. 74 in [60]). That rule was formulated by the CJEU, as suggested by the Advocate General, to avoid excessive legal consequences of an expansive interpretation of joint control. However, it must be noted that as regards communities of DLT-based permissionless networks, which are operated under decentralized governance, the scope of responsibility of a community's members (core developers, miners or validators, nodes operators, users) will likely only slightly be limited by applying such a rule. In the 'Fashion ID' case, the Fashion ID, as website operator, did not exert any influence on processing the data by Facebook (neither purposes nor means of processing) when the data had been already transferred to Facebook. However, when the user sends the data to the DLT-based network that is under highly decentralized governance, this networks' user still co-exert decisive influence (with all other members of the community) on how these data are further processed. It can be claimed that usually all members of a permissionless blockchain community exert such influence 'jointly' by using a commonly operated network. They all support network operation to use and maintain such a network and they all perform off-chain governance [23]. In a typical situation, the network operation is in the interest of all such members of a network community, although the interests of each group of members are different. Thus, in my opinion, highly decentralized governance, where any narrower group of decisive persons could not be identified, could result in joint responsibility of everybody who has co-influenced how the data are processed on a permissionless DLT ledger. The lack of a most influenced point(s) in the network's governance (i.e. a central operator) thus leads to the conclusion that everybody who participated in off-chain governance jointly exerted decisive influence over the means of processing. The view that nobody controls the network cannot be accepted, because each network is controlled by somebody: by a more or less wide group of community members, coordinated by software (code) and the developed rules of off-chain governance. Qualification of a network's members should always be decided, however, on a case-by-case basis and may not be pre-determined in abstract. Sometimes a narrow group of most influenced persons may be indicated within a community; networks bear significantly different levels and ways of governance's decentralization [64]. No two networks are the same in terms of their governance and control, and as a result, networks generate different level of risk for their members in terms of GDPR compliance.

According to the so-called 'household exemption'[9] the GDPR is exempted when data are processed by 'a natural person in the course of a purely personal or household activity' (GDPR, however, applies to controllers or processors which provide the means for processing personal data for personal or household activities). It was right to point out that it is unlikely to apply that exemption where a permissionless blockchain is used, as in that case personal data are shared with an indefinite number of people [23].

Until recently, academics have questioned the qualification of core developers as (joint) controllers because they were considered to be merely the creators of the tool (software) used to process data by other entities [23]. However, in my opinion, the recent development of CJEU case law paves the way for core developers to be subsumed under the role of (joint) controllers. As the CJEU claims in the 'Jehovan todistajat' case, a person who exerts influence over the processing of personal data by others—for personal purposes, even if not for profit—may be regarded as a controller. To qualify a person as a controller, it is enough that the person organizes, coordinates, and encourages the processing of personal data by others. This person does not need to have access to the data; sufficient is the person's knowledge, on a general level, that the processing of data by others is being carried out [57]. In light of the above, core developers of permissionless networks could usually be qualified as joint controllers because often they co-organize, coordinate, and encourage people to use DLT-based permissionless networks designed by them. They do it for their own financial or non-financial interest. The final assessment, however, needs to be determined on a case-by-case basis.

The discussion above illustrates that where personal data are processed on DLT-based permissionless ledgers under highly decentralized governance, usually all the members within the DLT-based networks' community (users, nodes, miners or validators, developers) face a high legal risk of GDPR non-compliance. It is almost a common view that most members of permissionless DLT-based network communities could be subsumed under the respective GDPR provisions as data (joint) controllers or, at least, as processors. The more a network's governance is centralized, the more probable it is that only the most influenced group(s) of community members can be qualified as (joint) controllers. However, even if the other community members are qualified as 'only' processors, they still suffer the legal risk of being responsible under the GDPR's provisions directly concerning data subjects or supervisory bodies. A presentation of controllers' and processors' liability rules is beyond the scope of this article; interested readers may find that information in many sources [23, 50].

In search of a permissionless blockchain that enables GDPR-compliant data processing

It is emphasized that there is no such thing as a 'GDPR-compliant blockchain'—there are only GDPR-compliant use cases [61]. However, the crucial question is whether any permissionless blockchain exists, or may exist at all, which functionally (by design) enables GDPR-compliant data processing. I will refer to such a blockchain, which would by design enable GDPR-compliant processing of data stored on its ledger, as a 'GDPR-compliant permissionless blockchain'.

8 The Article 29 Working Party was an independent European working party that dealt with issues relating to the protection of privacy and personal. It has been replaced by the European Data Protection Board (EDPB).

9 Article 2.2(c) GDPR.

Below, I will briefly present some of the GDPR requirements which members of blockchain ecosystems face if they are qualified—under the GDPR—as controllers or processors.

Obligation to conclude agreements among joint controllers of data

According to the GDPR,[10] joint controllers should 'in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information … by means of an arrangement between them …. The arrangement … shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects.'

Permissionless DLT networks are—at the protocol-layer level—under the decentralized off-chain governance of their respective communities. Concerning highly decentralized communities, the networks can comprise millions of network participants. For example, in the near future, this may be the case of the permissionless OpenLibra project [65]. Interactions between members of such community take place both on-chain, through procedures determined by the network protocol, and off-chain. Concerning off-chain reactions, each blockchain community creates its own ways and customs of conducting off-chain communications [16, 17] that are either slightly formalized or not formalized at all. Members of the community are usually unable to identify each other unless they voluntarily disclose their identities (as core developers often do). In the architecture of permissionless networks any procedures or mechanisms have not been introduced which could incentivize or force community actors to disclose their identities within the community. Even if identification among network members is achievable, it would be undesirable as this might jeopardise security and trust within the network. Core developers suggest the introduction of mechanisms to discourage mutual identification, as this protects against potentially dangerous collusions within the community [66].

The above implies that it is practically nearly impossible to conclude agreements, per GDPR requirements, among all highly decentralized network actors qualified as joint controllers. Even if one could argue that the 'arrangements' are already coded in the blockchain protocol [24], it is unclear whether they can be qualified as defining their responsibilities in a transparent manner (per GDPR requirements). The software of permissionless DLT-based networks is transparent in the sense that it is open source and can be audited by anyone. However, use of the software does not create *per se* legal obligations, nor does it determine those legal responsibilities with which data controllers have to comply. Ultimately, networks' protocols and blockchain ledgers, as they currently stand, do not contain all the elements required by GDPR for the arrangements.

Obligation to maintain a record of processing activities

Each data controller under the GDPR is obliged to maintain a record of processing activities regarding processed data[11] which must contain, among other items, 'the name and contact details of the … joint controller'. One of the obligations of a processor is maintaining a record of all categories of processing activities, containing, among other items, the name and the contact details of the processor or processors, as well as those details for each controller on whose behalf the processor is acting. However, even if a blockchain ledger was qualified under the GDPR as a transaction register, it would not contain all the information required by the regulations, as indicated above [24].

Transfer of data to third countries

According to the GDPR,[12] any transfer of personal data to a third country can take place only if, subject to the other special provisions, the conditions laid down in the GDPR are complied with by the controller and processor. The legal grounds for data transfer to third countries are limited. The broadest basis for data transfer which does not require any specific authorization is an adequacy decision issued by the European Commission.[13] This decision claims that third country must ensure an 'adequate' level of protection, that is, a level that is 'essentially equivalent to that ensured within the EU'.[14] At the time of writing, there are only a few adequacy decisions issued by the European Commission [67]. Recently, the CJEU in the 'Facebook and Schrems II' case [68] ruled that an adequacy decision related to the EU–US Privacy Shield is invalid because the USA does not ensure an adequate level of personal data protection, as required by the GDPR. In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.[15]

If a transfer may not be performed on the basis indicated above, and none of the GDPR's derogations for a specific situation are applicable, a transfer may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and if the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with respect to the protection of personal data.

In the context of a permissionless network, a controller's or processor's transfer of personal data to the network, where data may be processed by nodes and servers worldwide, may constitute the data transfer to third countries. It is hardly (if at all) possible that controllers and processors of data written on permissionless blockchain ledgers are able to provide appropriate safeguards for data subjects where data are transferred to any country in the world to the non-identified nodes' operators, miners, or validators. Moreover, sending data to permissionless networks seems to concern an unlimited number of data subjects. It is doubtful whether in such situations legitimate interests pursued by the controller are not overridden by the interests or rights and freedoms of the data subject(s)—which should be assessed on a case-by-case basis.

The right to be forgotten and the requirement to minimize stored data

One of the most difficult GDPR obligations to fulfil concerning data processing on public DLT-based ledgers is ensuring data removability. This functionality is necessary for performing the right to be forgotten and for complying with data storage limitation requirements.[16] One of the obligations of a controller is the 'erasure'

10 Article 26 GDPR.
11 Article 30 GDPR.
12 Article 44 GDPR.
13 Article 45 GDPR.
14 Recital 104 GDPR.
15 Article 46 GDPR.
16 Article 5.1(e) GDPR.

of personal data on data subjects, without undue delay, if one of the legal grounds applies.[17] The controller should—both at the time of determining a means for processing and at the time of processing—implement appropriate technical and organizational measures designed to implement data protection principles effectively, as well as to integrate the necessary safeguards into the processing to meet GDPR requirements and protect the rights of data subjects.[18] It is unclear whether the term 'erasure', as used by the GDPR, always means 'destruction' [23], which as a principle would not be possible on the blockchain-based ledgers. Essential and basic DLT features include the integrity and immutability of data. These properties are necessary to ensure the uniqueness of a given datum and to exclude double spending. Removing these features to achieve data erasure would be contrary to the essence of this technology.

DLT legers may be changed via forks. However, these forks do not ensure a data removal mechanism as required by the GDPR. Introducing forks in highly decentralized networks is often too much of a time-consuming process. This process also often fails to achieve its desired result: the removal of data from the ledger. In the case of a hard fork, data may not be removed from one of forked chains which is supported by less computing power and by the members who do not accept the data removal (as was the case of The Dao hack and the Ethereum fork).

According to the Austrian Data Protection Authority, data controllers enjoy flexibility regarding the technical means of realizing erasure, and anonymization itself can be considered as a means of realizing data erasure [69]. An often-proposed solution to this data erasure issue is private key destruction [23]. The French Data Protection Authority suggests [70] that the deletion of the keyed hash function's secret key would have ensured a similar effect to 'data erasure' under the GDPR. In case of deletion of the keyed hash function's secret key, proving or verifying which information has been hashed would no longer be possible. In practice, the hashed information would no longer pose a confidentiality risk [70].

In my opinion, this interpretation of the concept of 'deletion' of digital data corresponds to the objectives of the GDPR. The physical destruction of data is not required when technologies are available to ensure that there is no linkage between the particular data and the individual, while taking into account 'all the means reasonably likely to be used'.[19] The mechanisms suggested by national data protection supervisors for ensuring the deletion of data compliant with the GDPR—anonymization and the destruction of private keys enabling access to the identifiers—are not two alternative ways of ensuring the feasibility of the right to be forgotten, but they are complementary solutions. The destruction of the controller's private key that provides access to personal data can only be considered as an effective means of deleting data by this controller if those data which are still stored on the public ledger are processed anonymously (in relation to the given controller). This case will arise if, after destroying the keys, the given controller is unable to determine the same information and connect it to the identifiable person merely by using data that are publicly viewable on ledgers or through additional data that they, or a third party, possess, taking into account 'all the means reasonably likely to be used'.[20] If, after destroying the access keys, the controller is still able to link the data stored on the ledger with the natural person (e.g. by analysing the content of public ledgers and external data that the controller could access, taking into account all those means that have a reasonable likelihood of being used), then, despite the destruction of keys, the erasure of data has not taken place under the GDPR. The destruction of keys which give access to data stored on a 'transparent' blockchain cannot usually be considered to be a removal of personal data. To reach the threshold of 'anonymity' under the GDPR, the destruction of access keys by a data controller should have to be similar to the physical deletion of data. This effect may be achieved only if the data processed by the controller (and all joint controllers) on the public ledger are deeply masqued to reach the GDPR threshold of anonymity. If the data still stored and processed on the blockchain (after deleting the key) are only pseudonymous, then the private-key deletion would not ensure the erasure of these data.

The above position seems to be in line also with the recent view of The European Union Agency for Cybersecurity. The Agency states that 'in cases that the data controllers process the personal data in a way that they cannot identify the individuals (e.g. in processes where the additional information allowing for re-identification has been deleted by the controller...) [I]n such cases and depending on the technique used, this way of processing might actually lead effectively to data anonymization' [71]. Therefore, as I emphasize above, to ensure this result, those data that are still processed by the controller on the public ledger (following the key deletion) should be the anonymized data.

In conclusion, ensuring data-removal mechanisms from the blockchain requires the anonymization of data recorded on its public ledger.

Anonymization of data on blockchains

It is doubtful whether the data recorded on public ledgers can be qualified, under the GDPR, as anonymized data in situations in which the user (data subject) still retains access to its identifiers, such as public and private keys/addresses and the transaction value.[21] On privacy-blockchains, some data (depending on the blockchain protocol) are masqued by zero-knowledge cryptography, but they are still visible to the user. Can anonymous data under the GDPR be considered anonymous in relation to controllers and processors if they are not anonymous in relation to the data subject? Access to the identifiers by the data subject could allow them to link data stored on the public ledger with their person, even if no other person can do this. Concerning cloud computing, it was stated that, where the user is the only person who is able to access reunified shards of their stored data, then, at least pursuant to a relative approach to the concept of personal data (see the next section), 'the data may be personal data to the user, but not to anyone else' [23, 75].

Although interpreting the concept of personal data, there is a need to refer to the dispute about the 'relative' versus 'absolute' approach concerning such data. According to the relative approach to personal data, when assessing a person's traceability based on specific data, the individual capabilities and perspectives of a particular controller should be considered. If additional data which are needed for identification are in the possession of a third party, then an examination should be carried out to determine whether a particular controller has the ability to access and use these data, within their own means, to identify the person. According to the opposing

17 Article 17 GDPR.
18 Article 25 GDPR.
19 Recital 26 GDPR.
20 Recital 26 GDPR.
21 The A29WP defines an identifier as piece of information that holds a particularly privileged and close relationship with an individual, allowing for his or her identification [72, 73, 74].

absolute approach, when assessing the possibility of connecting information (data) with a specific person, all available information—regardless of who possesses that information and whether the controller is able to obtain it from a third party—should be taken into account (paras 52–53 in [76, 77]).

The leading CJEU case in that scope is the 'Breyer' case, C-582/14 [78]. The court stated that 'there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person' (para. 31 in [78]). However, Finck stresses that since the CJEU assessed the nature of the data by analysing the controller's ability to obtain additional data from the third party for the purpose of identification, this indicates that the CJEU has adopted a relative approach [23, 53]. However, the CJEU has also significantly reduced the effects of narrowing the data protections resulting from a relative approach by ruling that the possibility of a controller obtaining additional data from a third party should be interpreted broadly. Namely, the additional information needed for identification (and that is also in possession of a third party) may be omitted when assessing whether the controller can use it for identification purposes, but only if the controllers' access to the data in the third party's possession 'was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant' (para. 46 in [78]). Although these criteria are related to DLT, I would claim that, if the level of data masquing on the ledgers has reached the anonymization threshold, and if only the user has access to the identifiers, then linkage of data on the public ledger with a data subject would be impossible for any controller without the use of information possessed by that data subject. In a typical situation, it can be considered practically impossible for the data controller to obtain the additional data from the data subject (taking into account that it requires a disproportionate effort in terms of time, cost, and workforce). It is so because if the anonymization techniques are used, usually it would be practically impossible for the data controllers to identify and find the user in possession of this additional information needed to identify this data subject. Of course, any assessment should always be made on a case-by-case basis.

Consequently, maintaining by the user (data subject) its exclusive access to the identifiers (such as public and private keys and transaction value) does not preclude the qualification of data stored on a public ledger as 'anonymous' in the GDPR's meaning.

Reaching the GDPR data anonymization threshold

The analysis of the presented GDPR requirements in the context of the DLT and decentralized governance of permissionless networks shows that some GDPR requirements are practically impossible to implement in highly decentralized DLT-based networks. These would become feasible (or almost feasible) for networks after their transformation into permissioned systems, or after strengthening the network centralization, which, in turn, would undermine the trust in permissionless DLT and thereby result in the loss of permissionless DLT's practical importance. Therefore, in my opinion, the GDPR leaves only one option available for permissionless networks to create a protocol enabling GDPR-compliant processing of data written on the ledger: implementing the technology which will ensure the anonymization of data stored on the ledger. The GDPR does not apply to anonymized data.

Nevertheless, it is doubtful whether the data anonymization GDPR' threshold is currently reachable on permissionless blockchains or whether it may be reachable in the future (in a broader technological context, see Purtova [28]). Any information regarding an identified or identifiable natural person is personal data.[22] Data that do not relate to an identifiable natural person are considered to carry anonymous information. According the GDPR, to determine whether a natural person is identifiable, 'account should be taken of all the means reasonably likely to be used, either by the controller or by another person to identify the natural person directly or indirectly… To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors … taking into consideration the available technology at the time of the processing and technological developments'.[23] As Finck points out, the criterion for determining whether data are anonymous is the likelihood of identification; identification should not be likely through reliance on all the means reasonably likely to be used [23, 53].

According to the opinion of A29WP, 'anonymization results from processing personal data in order to irreversibly prevent identification' [79], and 'the outcome of anonymization as a technique applied to personal data should be, in the current state of technology, as permanent as erasure, that is, making it impossible to process personal data' [79]. To the A29WP, a risk-based approach seems to be insufficient: 'it deems that the risk of identification must be zero' [23, 80]. However, in the same opinion, the A29WP indicates that 'a residual risk of identification is not a problem if no one is reasonably likely to exploit it' [79]. Consequently, the opinion of A29WP within this scope may be regarded as unclear, leaving space for opposite interpretations concerning the required threshold of anonymization.

The European Union Agency for Cybersecurity has recently expressed its view regarding the GDPR' threshold of anonymization. This opinion is important because it takes into account the further development of technology following the previous opinion of the A29WP. Moreover, it is highly possible that the European Data Protection Board will henceforth follow the position of the European Union Agency for Cybersecurity in his future opinion, long-awaited by the business community, regarding the data protection in the context of permissionless networks. In a recent recommendation (2019) of the Agency on shaping technology according to data protection and privacy provisions [74], the Agency defined anonymization as a 'process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party' [74]. Although the Agency expressly referred to the GDPR, the above-cited definition is not taken from the GDPR but from the ISO Standards for 'Health informatics—Pseudonymization' (point 3.2. in [81]). In the ISO comment to this Standard, it is indicated that the concept of anonymity 'is absolute, and in practice, it may be difficult to obtain' (point 3.2. in [81]). One might think that the European Union Agency for Cybersecurity only mistakenly omitted the definition of GDPR, basing its understanding of 'anonymity' on the ISO definition instead—but this is not the case. In its previous report, the Agency clearly quoted the GDPR (and not the ISO) definition of personal data, stated that before characterizing data as anonymous, cautiously should be answered the question: 'as to whether it is really impossible for any

22 Article 4(1) GDPR.

23 Recital 26 GDPR.

party—including the data controller—to identify from these data any individuals' [82]. The requirement of data to be 'really impossible to identify' may be interpreted as adoption by the Agency of an absolute (zero-risk) approach. As noted above, however, this position is not justified either in the text of GDPR or in CJEU case law. Therefore, it is worth noticing that current difficulties in finding effective anonymization techniques may not lie with the technology itself, which seems to be developed enough, but with faulty interpretations of the EU regulations by some EU supervisory bodies.

However, the European Union Agency for Cybersecurity, adopting the absolute approach for data anonymization (hardly, if at all, achievable in practice [53]), at the same time indicates that zero-knowledge proofs and the broader area of attribute-based credentials fall within the group of 'techniques that can effectively be used to increase anonymization' [74]. This statement, in turn, could be interpreted as a deviation of the Agency from an absolutist approach. We should also bear in mind that the determination of a given technology or mechanism as guaranteeing data anonymization might not be possible in general. As has been emphasized, the risk of identification must be assessed on a case-by-case basis [23]; each set of data has in its own unique set of circumstances, and no one method of identifying an individual is considered 'reasonably likely' to identify individuals in all cases [83].

If not data anonymization, then what?

The architecture of permissionless networks, their governance, and deployed technologies vary substantially. It is not unlikely that, in the future, DLT-based permissionless networks would be able to cope with the GDPR requirements. One example of such technological progress is exemplified by the recently announced proof of concept of a redactable blockchain, a prospective solution to the right to be forgotten [84]. Researchers proposed to accommodate editing operations in the blockchain by extending the block structure to include another copy of the transaction's Merkle root. The edit operation is performed by replacing the original block with the other (candidate) block based on miners' voting on the user's edit request [84]. This newly proposed solution has not yet been widely assessed. If successfully tested, it could become a prospective useful means for the sporadic deletion of data concerning the data subject's demand to be forgotten, or else it might be used for the erasure of illegal or harmful data stored on public ledgers in plain text [85, 86]. However, adapting this tool to meet the GDPR requirement of data minimization would remain a huge challenge. The fulfilment of this obligation may lead to mass and frequent data erasure after the expiration of the retention period,[24] raising questions regarding the security and trustfulness of such redactable permissionless blockchains. There is a need for further research into whether this proposed solution, based on miners' voting, could also be adapted to fulfil the GDPR principle of data minimization.

Thus, it cannot be excluded from the realm of possibility that future permissionless DLT developments could bring effective means of data erasure and other means that enable to meet other GDPR requirements. However, even if data anonymization is no longer necessary to exclude the applicability of the GDPR, in that situation, implemented pseudonymization techniques of the data written on blockchain ledgers would have to be very strong because blockchains ledgers are publicly viewable. According to the GDPR confidentiality principle, data ought to be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing. . . using appropriate technical or organizational measures'.[25] Therefore, in order to meet the confidentiality requirement related to the processing of personal data, it would be necessary to use advanced pseudonymization techniques which would effectively protect the data subject against reverting the pseudonymous nature of these data by unauthorized third persons. Such techniques should be almost near the anonymization threshold because if the pseudonymized data allowed any third persons to identify users easily after reading the data on ledgers, the confidentiality principle of data processing would not be met by the data controller and the data processor.

Anti-money laundering and combating the financing of terrorism policy instruments in permissionless blockchain spaces

The above analysis shows that GDPR requirements for personal data protection push permissionless blockchain-based networks towards ensuring the anonymization of data processed on a public ledger. Ensuring data anonymization is currently needed if public ledgers are to enable GDPR-compliant data processing on ledgers by data controllers and data processors. However, at the same time, the privacy-blockchains which use anonymity-enhanced technologies, as well as their native privacy-coins, are combated by AML/CFT policies. Generally speaking, intermediaries are not allowed to trade or manage such virtual assets as far as they are unable to mitigate AML/CFT the risks posed by privacy-coins. Advanced anonymization technologies, needed to protect personal data, are not acceptable by AML/CFT policies. This section presents some tools of global AML/CFT policy and describes their impact on shaping the architecture and protocols of permissionless blockchain-based networks.

Financial action task force recommendations for anti-money laundering and combating the financing of terrorism policy in relation to virtual assets

In 2018, the FATF updated its Standards [87] to clarify their application to virtual assets[26] and the virtual asset service provider (VASP).[27] In 2019, FATF issued the Guidance [27] further clarifying

24 Article 5.1(e) GDPR, Recital 39 GDPR.

25 Article 5.1(f) GDPR.

26 According to the FATF Standards (2019) [87], a 'virtual asset' is a 'digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'. In its earlier documents, the FATF mainly used the concept of 'virtual currency'. However, following the most recent amendments to FATF Standards, a new term of 'virtual assets' appears, even though the concept of 'cryptocurrency' is still used by the FATF in the term 'anonymity-enhanced cryptocurrency'. Consequently, I use FATF terminology in this article.

27 According to the FATF Standards (2019) [87], '"Virtual asset service provider" means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies, (ii) exchange between one or more forms of virtual assets, (iii) transfer of virtual assets, (iv) safekeeping and/or

the FATF's previous amendment to the Standards relating to virtual assets [83, 84]. FATF's Standards (2019) recommend establishing AML/CFT measures that are related to both governmental bodies and the VASP. These obligations require governments to assess and mitigate risks associated with virtual asset activities and VASP. The VASPs are to be licenced or registered or subject to supervision or monitoring by national authorities. The governments are to implement sanctions and other enforcement measures when a VASP fails to comply with their AML/CFT obligations [88]. In order to identify those VASPs operating without a licence or registration, governments should consider non-publicly available information, as well as web-scraping and open-source information, to identify online advertising or possible solicitations for business by unregistered or unlicensed entities (point 84 in [27]). FATF recommendations require governments to impose on VASPs the obligations of assessment and mitigation of ML/FT risks and the implementation of AML/CFT preventive measures, including KYC, record-keeping, suspicious transaction reporting, and screening all transactions for compliance with targeted financial sanctions, among other measures applied to any other entities in the financial industry [88].

Many of the VASP-related FATF recommendations directly address virtual assets, including anonymity-enhancing currencies. Several risk factors are highlighted in the FATF Guidelines, which increase the risk of non-compliance with AML/CFT rules: anonymity-enhanced features of technology and network architecture; decentralized, unregistered, and unlicensed VASPs; disintermediation of transactions; and peer-to-peer transactions (point 51 in [27]). In order to meet the FATF requirements (as they are implemented in systems of national law), the VASP must be able to prove that they can manage and mitigate the risks of engaging in virtual assets-related activities which involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to anonymous-enhanced cryptocurrencies, mixers, tumblers, and other technologies that obfuscate the identity of the sender, recipient, holder, or beneficial owner of virtual assets (point 110 in [27]). If a VASP cannot manage or mitigate the risks posed by engaging in such activities, it should not be permitted to engage in such activities (point 110 in [27]).

Finally, according to the 2019 FATF recommendations, 'V[irtual] A[ssets] products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF risks' (point 98 in [27]). Countries should 'consider the risk factors associated with the V[irtual] A[ssets] product, service, transaction, or delivery channel, including whether the activity involves pseudonymous or anonymous transactions. . .. The fact that nearly all V[irtual] A[ssets] include one or more of these features or characteristics may result in countries determining that activities in this space are inherently higher risk' (point 28 in [27]). This statement shows that, from an AML policy perspective, strong pseudonymization techniques present nearly the same high risk as the anonymity-enhanced techniques. Even if advanced cryptographic methods, such as zero-knowledge proofs, are to be qualified according to the GDPR as only pseudonymization techniques, for law enforcement agencies to identify the users (data subjects) masqued by these techniques remains extremely difficult. It does not depend on the qualification of such masqued data under the GDPR as pseudonymous or anonymous data. Advanced anonymization technologies exclude effective counteracting of ML/FT risks—regardless of the technology and data qualification—slightly below or slightly above the GDPR's anonymization threshold. Pseudonymization techniques can also exclude a quick identification of network users and financial beneficiaries of transactions, which is crucial for preventing ML/FT risks. Accordingly, strong pseudonymization technologies used within networks under decentralized governance should be combated today by AML/CFT national regulation and by obliged entities with the same intensity as technologies ensuring data anonymization according to the meaning provided by the GDPR.

The impact of anti-money laundering and combating the financing of terrorism measures on anonymous permissionless blockchains

One characteristic of the present AML/CFT policy is its focus on combating anonymization or strong pseudonymization techniques, which seem to be perceived by the authors of regulatory instruments as the primary sources of threat. In practice, AML requirements force intermediaries (VASPs) to stop handling transactions when instruments are used that impede the traceability of transactions on the public ledger. In situations where these advanced privacy-focused technologies are embedded in the protocol as non-optional and the owner of virtual assets cannot remove these features, in that situation, a VASP is not allowed to handle transactions involving these virtual assets as it would not be able to mitigate AML/CFT risks. Therefore, AML policy measures combat technologies which are able to protect data on public ledgers at the level required by the GDPR. Moreover, that policy pushes owners of such privacy-coins towards peer-to-peer (or even off-chain) transacting on privacy-focused blockchains or directs them to use inter-chain autonomous tools.

Joint impact of the GDPR and AML/CFT policy instruments on permissionless blockchain spaces—The conclusion

The GDPR and AML/CFT policy instruments in permissionless blockchain spaces are on a collision course: AML policy fights anonymity-enhanced and strong pseudonymization technologies deployed in permissionless DLT protocols. In practice, the obligation imposed on VASPs to refrain from involvement in transactions in which they cannot mitigate ML/FT risks associated with virtual assets results in VASPs refraining from engaging in transactions which involve anonymity-enhanced (privacy-focused) cryptocurrencies [89]. At the same time, the only way for networks to ensure the GDPR-compliance of data processing on public ledgers seems to be data anonymization. As presented above, the whole community of permissionless blockchains, especially the part which may be reached by fines issued by the European data protection supervisory bodies, has an interest in the exemption of the GDPR applicability to their activities. As I pointed out above, one possibility (it seems the only one) for removing the GDPR applicability is to design the protocol and the whole network's architecture in such a way that all data sent and written on the ledger would be anonymized in the meaning of the GDPR. However, when such privacy-blockchains are (or will be) operated, their users, and at the same time the users

administration of virtual assets or instruments enabling control over virtual assets, and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.'

of privacy-coins, have no possibility to refer to supervized intermediaries (VASP). This hinders the development of such networks. Moreover, it also induces designing of more and more tools to bypass regulated intermediaries by holders of privacy-coins. Thus, there is a need to find and implement AML/CFT tools which would be feasible and enforceable in anonymous cyberspaces, instead of lowering the level of data/privacy protection at publicly viewable ledgers.

As we can observe, the development of new permissionless DLT networks seems going in the direction of enhanced protection of privacy. The use of advancing anonymization techniques is needed for blockchain communities to be GDPR-compliant and to avoid severe fines. The increasing use of more and more advanced anonymization techniques may eventually enable the processing of anonymous data on permissionless networks' ledgers, per the GDPR. Advanced anonymization techniques, reaching the GDPR level of data anonymization, should be accepted by global or national policies towards the permissionless DLT. However, to ensure that the AML/CFT needs are met, the government(s) should search for effective tools feasible and available in anonymous or strong pseudonymous cyberspace.

Searching for solutions: Analysis of existing proposals

The tension between privacy and the needs of law enforcement agencies is widely debated concerning different communication technologies. For example, to facilitate acceptance by the governments of the end-to-end encryption used in messenger applications, as well as to improve privacy in data surveillance instead of granting states exceptional access into messenger applications, Segal *et al.* [90] have proposed a lawful search of third parties' records of data. Concerning permissionless DLT-based networks, some interesting approaches have been already proposed, such as, for example, blacklisting [47] or collaborative deanonymization [91]. However, only a few proposals address the protection of data according to the rules required by the GDPR. They are discussed below.

Registration of the virtual currency addresses in FIU

The Vth EU AML Directive[28] recommends that the FIU should be able to associate virtual currency addresses with the identity of the owner of virtual currencies and further that the possibility for users to self-declare to designated authorities on a voluntary basis should be further assessed.

There is no doubt that for the FIU to become able to associate virtual currency addresses to the identity of the owners of virtual assets would be a desirable solution. However, neither the FATF recommendation nor the EU AML Directives provide technically and legally feasible instruments for achieving this result. It is impossible to build an effective AML/CFT policy based on the voluntary registration of all address owners. Each person can generate, within a short time, any number of addresses they do not have to use. It is unclear why anyone would register an address without being legally obligated. However, even if address registration were obligatory, the anonymity or strong pseudonymity of blockchain users would practically prevent verification by the FIU, whether or not all addresses generated for transactions on privacy-blockchains have been reported to them. Finally, registering virtual currency addresses in FIU would not be useful for crime prevention in situations of anonymity-enhanced blockchains when the addresses of the transactions' parties are masqued. Linking the person to a specific address would not allow for the traceability of their transactions. This problem is being partially addressed by the 'travel rule' imposed on the VASPs according to the FATF recommendations, but that tool only applies to transactions mediated by VASPs and leaves peer-to-peer transactions outside its scope of application.

Lowering the GDPR personal data protection on permissionless blockchains

Lowering the level of the GDPR data protection requirements for public permissionless blockchains is proposed to solve this privacy–transparency conundrum [24]. According to this approach, any lowering of the GDPR protection should reach a level that ensures the right balance between the protection of personal data on permissionless blockchains and the transparency necessary to deter criminal behaviour. 'Regulators need to talk with each other in order to set the cursor at the right place' [24]. Consequently, there should be a corresponding change in regulations, particularly regarding the GDPR and the AML [24]. According to this proposition, these amendments to the law should require that permissionless networks deploy only those technologies that ensure a certain, and not too low, level of personal data protection. However, at the same time, the networks should also provide a level of data protection that is not too high to enable identifying users by the law enforcement agencies, based on an analysis of data recorded on (transparent) public ledgers. It has been debated how to set this appropriate balance between data protection and the requirement of ensuring transparency. According to this proposal, only low-tech solutions—such as the creation of several public keys, registering only hashed information on ledgers, and using mixers—should be required by regulation to protect the privacy and should be sufficient to protect personal data on public blockchain-based ledgers. At the same time, AML regulations should prohibit the use of 'high-tech solutions', that is, advanced cryptographic methods such as zero-knowledge proofs [24]. Thus, the analysed proposal strictly determines the technologies which should be used; overly strong pseudonymization technologies should be banned to ensure the right level of ledger transparency, while technologies that are too weak (too transparent) should be banned to ensure personal data protection.

The above solution does not seem to be appropriate, even without considering the difficulties in qualifying different new technologies as too strong ('high-tech') or too weak ('low-tech') solutions. Implementing this proposal would provide law enforcement agencies with the necessary minimum degree of user traceability in permissionless space. On the other hand, this solution would allow any third person other than governmental agencies to have ensured the same level of user traceability and identifiability. Accordingly, the proposal fails to ensure a sufficiently high level of user privacy protection against third persons other than governmental agencies. As public ledgers are viewable for everyone, this failure is significant. Lowering the requirements of data privacy protection on public ledgers by banning the use of anonymity-enhanced technologies does not protect users against the possibility of being identified by the state or by any other actors. If the above solution were selected, practically everyone would gain access to anyone else's personal

28 Recital 9 Vth EU AML Directive.

data on public ledgers. Therefore, as permissionless DLT ledgers are publicly viewable and searchable by everyone, the GDPR requirements to ensure the confidentiality of data should not be lowered. Lowering the required level of masquing personal data would expose data subjects to identification by anyone who has enough knowledge and resources. Lowering the required level of masquing data on DLT ledgers would also violate the GDPR principle of technological neutrality. Moreover, the proposition suggests restricting instruments of personal data protection on public ledgers only to the use of 'low-tech' solutions. However, these instruments are not embedded by design in the blockchain protocol. The effective and successful use of such instruments would not be an easy task for average users. This approach would also violate the GDPR because it is required that privacy protection instruments be built by design into systems and their implementations should not burden data subjects. Finally, mixers, tumblers, and similar 'low-tech' solutions may effectively protect data subjects if such mechanisms are used simultaneously with anonymity-enhanced technologies that do not allow for tracking and linking transactions. The suggested ban on advanced anonymity-enhanced technologies would significantly reduce the effectiveness of accepted 'low-tech' solutions.

Certification mechanisms and codes of conducts

According to Finck, the certification mechanisms and codes of conduct may overcome difficulties in applying the GDPR obligations to specific cases of personal data processing [23]. However, at the same time, she underlines that codes of conduct and certification mechanisms will not resolve the lack of compliance where there are technical or governance limitations to compliance. In such cases, these limitations could be addressed by interdisciplinary research on these matters [99].

Indeed, certification mechanisms may be helpful for standardization of solutions used by permissioned networks, but it is not the case with permissionless systems which are under decentralized governance. Certification mechanisms and codes of conduct are not able, nor are they are allowed, to change the GDPR rules, for example by removing all these problematic GDPR' requirements which seem not to be feasible to meet under decentralized governance of DLT-based networks (some of them have been indicated above in the section 'In search of a permissionless blockchain that enables GDPR-compliant data processing'). The research work should be done to identify solutions which can square permissionless blockchains with the GDPR, but simultaneously not forgetting about the needs of AML/CFT policies. Certification mechanism and codes of contact cannot help until any feasible solution(s) to reconcile these two regulations become accepted by policy makers and regulators.

Blacklisting

Another approach that should be discussed here, aimed at reconciliation between the privacy and AML/CFT needs, is a blacklisting approach developed by Möser et al. [47]. By blacklisting suspected transactions, the tool helps prevent the acceptance of coins derived from illicit activity, and it requires intermediaries (and incentivizes other users) to check coins against public blacklists of illicit funds before accepting them. Blacklisting is enabled by the ability to follow coins from one transaction to the next [92]. That system requires traceability of transactions as a minimum. Thus, it could work well on transparent blockchains, that is, on blockchains which, as indicated above, create a high legal risk for almost all community members of being responsible for the processing of personal data written on the blockchain ledger in contravention of the GDPR.

To reconcile the GDPR and AML/CFT aims, however, an AML/CFT policy tool is needed that would work in an anonymous blockchain space (and which, in turn, may be acceptable, or at least less risky, from the GDPR point of view).

The traceability of transactions needed for blacklisting systems is something less than the possibility of user identification. The users' identification is not needed to trace the transactions. Thus, in terms of personal data/privacy protection, it is definitely a step in the right direction which supports and strengthens the level of privacy protection.

However, it would be a useful tool to resolve the problem analysed in the article if it were feasible on blockchains where anonymous data were processed, that is, when the controllers and processor had no possibility to link data written on the ledger (in hash form or plain text) with data subjects, apart from a residual risk of identification (as explained above). As pointed out above, because traceability of some transactions on publicly viewable ledgers is today possible (even if often it requires an extreme amount of resources) and it also increases the chances for the users' identification, it indicates that the likelihood of data subjects identification is not only residual (identification at least of some data subjects is likely through reliance on all the means reasonably likely to be used). However, as presented above, it varies from network to network, as well inside the networks. Moreover, transactions' traceability increases the chance of associating a whole chain of transactions with some external data, which, in turn, increases the chances of identification of some data subjects. Where zero-knowledge proof cryptography is used, almost excluding the traceability of transaction, the blacklisting system fails, taking into account its current development [92]. The designers of blacklisting noted that the concept might not be feasible in all cryptocurrencies, especially those built on zero-knowledge proof cryptography [92].

Thus, blacklisting can be feasible AML/CFT tools in relation to, generally speaking, transparent blockchains, such as the Bitcoin blockchain, even when different anonymity technologies or techniques are used by their users [47, 92]. These blockchains, however, do not enable, by design, the GDPR-compliant processing of data, for example, (i) where all nodes process personal data written on the ledger without the possibility to erase these data from all copies of the ledger, including even data treated worldwide as illegal, such as child abuse content [52, 93] and (ii) where personal data are transferred to the third countries without legal basis and protection for data subjects. Contrary to exceptional access, the blacklisting system, in its current stage of development, does not simultaneously address the needs of both the GDPR and the AML/CFT with respect to the privacy-blockchains. As presented above, the zero-knowledge proof cryptography is today seen as one of the most promising methods that may enable, with appropriate systems architecture, the achievement of the data anonymity threshold defined by the GDPR on permissionless blockchains' ledgers.

Towards reconciliation between the GDPR and AML/CFT: proposed solutions

In the scope where the GDPR applies to data processed on permissionless blockchains' ledgers, the level of data protection required by this regulation should be met. National and global policy

towards permissionless blockchains should not combat the operation of networks that use advanced anonymization technologies on the protocol level as a non-optional feature, provided that any effective AML/CFT tools or approaches are accessible for VASP or for FIU on such privacy-blockchains. The governments should actively search for such solutions and should use or create any possible tools, even if they are more expensive or less convenient to use than a simple ban on VASPSs accepting any privacy-coins from another VASP. The presented solution is aimed at expanding policy makers' toolkits of instruments used to govern permissionless DLT financial platforms by adding to it a set of tools feasible in relation to privacy-blockchains. Promoting of use of privacy-focused blockchains, where the AML/CFT tools are available, is important from the privacy protection point of view.

The proposed solution should complement rather than replace existing AML policy instruments in relation to privacy-blockchains, while at the same time ensuring the achievement of GDPR goals. Thus, I do not suggest removing the VASPs' KYC and the 'travel rule' obligations. However, in relation to cryptocurrency underlying privacy-blockchains, the VASP ability to trace the coins is limited. That fact should not oblige them to refrain from transacting in such virtual assets if the privacy-focused networks granted the FIU the exceptional access (as proposed below) or if any other possibility existed in the future to gather transactional surveillance data by FIU. As indicated above, the effective measures that would enable the FIU or the VASPs to trace transactions made on privacy-focused blockchains are not available today—and that absence is the main reason why they are combated by the AML/CFT policies and why the VASP refrain from transacting privacy-coins. It is always possible that such tools will be developed by blockchains developers or by researchers in the future. However, as for today, the only AML/CFT tool which seems to be feasible in relation to privacy-blockchains is exceptional access, as proposed below.

Key elements of the proposed solution

The first proposed measure is the introduction of an optional regulatory instrument available for permissionless DLT-based privacy-networks granting the FIU exceptional access to some transactional data as a reporting feature embedded in the network's protocol. Without such a regulation, the FIU is not allowed to verify, accept, or use such access, even if offered by a network. That proposal relates only to those networks which, by design, use anonymization or strong pseudonymization technology to masque transactional data. That scope includes the networks which would ensure, by design, the processing of data written on the ledger in a GDPR-compliant way. That scope can also cover privacy-focused networks which underlie the privacy-coins commonly delisted or rejected by dExchanges (when the VASPs are not able to verify the source of coins), even if such networks do not reach the level that would enable data anonymization in the sense reflected in the GDPR. Depending on the anonymization technologies and the architecture of the network, offering a reporting feature for the FIU seems to be today the only feasible tool to protect data on the level required by the GDPR (or at least, near this level) and at the same time to enable effective AML/CFT screening. When access is granted by a network and accepted by FIU, they would have to analyse data obtained through 'exceptional access using available analytical technologies (today, VASPs are obliged to analyse and report these data to the FIU).

The second proposal is to add to policy makers' toolkits a set of effective tools aimed at combating cryptocurrency of those privacy-blockchains where virtual assets are transacted if (i) a network fails to deploy the reporting feature and, at the same time, if (ii) no other means or sources of surveillance data is available for the FIU to minimize AML/CFT risks.

A set of tools to combat privacy-coins may include means of a different technological, regulatory, economic (fiscal) nature, also including state attacks on underlying privacy-blockchains. The letter tool, as possible regulatory access points of the blockchain space, was already mentioned by Finck [16], however, without further analysis in that domain. The AML/CFT measures should concentrate on the cryptocurrency of indicated networks, instead of targeting the people who are members of their communities. The tools can and should aim towards reducing the particular currencies' value, consequently inducing a voluntary outflow of their users.

This article is not intended to present all tools which may be used to combat those cryptocurrencies. I rather suggest the general direction towards shaping effective sanctions for non-compliance with AML/CFT requirements in anonymous blockchain space. In subsequent subsections I analyse some aspects connected with that issue. Some of the indicated tools (e.g. different kinds of attacks on permissionless blockchains) have for a long time been a vital field of interest among computer and cybersecurity scientists. However, today these kinds of tools are not included in the AML/CFT policies, and there is a lack of legal basis in AML/CFT regulations for their use (at least, in European regulations). The indicated tools are discussed below from various perspectives.

Automatic reporting

The optional instrument of automated reporting as a feature embedded directly into the blockchain protocols requires specifying the scope and method of such reporting, as well as detailed rules for processing data received by the government (FIU) as a result of this reporting. Elements that must be defined when designing such exceptional access have been listed by a group of security experts and computer scientists [9]. Although this list was concerned with providing exceptional access in Internet spaces and on mobile devices, it is also helpful for the blockchain cyberspaces. Many issues identified therein are addressed in this article.

Scope of data covered

The proposal for embedded reporting is addressed only to privacy-blockchains. There is no need for exceptional access to transparent blockchain ledgers because data on their ledgers are publicly viewable and transactions are, more or less, traceable. Reporting from privacy-blockchains should relate to certain available data, such as public addresses engaged in a transaction, transaction ID, value of the transactions, and any additional content added by the user to the transaction. These data are accessible on privacy-blockchains for a user depending on the features implemented in protocols. Users may lift the cryptography veil of anonymization techniques.

Through proposed exceptional access to transactional data related to the transactions on such financial platforms, the FIU could gather and analyse the pseudonymized data which are currently hidden by zero-knowledge proof cryptography from the eyes of everyone except the user. For example, with Bitcoin blockchain, Zcash shielded transaction data are posted to a public blockchain; but unlike Bitcoin, zero-knowledge proofs allow transactions to be verified

without revealing the sender, receiver, or transaction amount. Selective disclosure features within Zcash allow a user to share some transaction details for the purposes of compliance or audit [94]. If such disclosure features would be accessible, by design, for the FIU, the FIU could analyse this data to identify the AML/CFT risks and flag suspected transactions. However, analysing pseudonymized data does not guarantee the FIU success in all cases. I address this concern in the last section 'Discussion of common concerns'.

Technology-neutral approach

Technical solutions for providing the automatic reporting feature on permissionless blockchains can be based, for example, on developing the 'viewing key' functionalities deployed on some privacy-blockchains such as Zcash [94]. This feature could ensure FIU access to the details of transactions in the same form in which such details are accessible to the user (the party to a given transaction). The other example can be the technical solution for the modification and optimization of the Monero system to create a regulatable privacy-preserving blockchain which has already been proposed [33].

However, the law should not strictly define technological requirements for such reporting functionalities. This could impede the rapid development of technology. I would suggest adopting a similar solution as accepted in the GDPR: legal regulations should only indicate the expected result (functionality) at a very general level, without pre-empting any technological details that must be implemented by networks. Ensuring effective trustful FIU access to specified transactional data, as well as possibilities of auditing such access, should constitute such a result. The functionality embedded in the blockchain protocol should ensure that transactions cannot be approved without automated reporting to FIU or without ensuring FIU access to the transactional details. It is the network community that should both choose and deploy the right technological solutions to achieve the required result. The auditing of solutions offered to FIU should be practicably easier when taking into account that the permissionless network's software is open source.

KYC features

Another tool that may be considered—either instead of, or in parallel with, the above-mentioned embedded reporting—is protocol-level deployment of a KYC functionality. This is currently the direction of development of, for example, the Concordium blockchain [95]. In such a case, the software should not allow transactions to be added to the ledger without confirmation that the parties to the transaction related to virtual assets have performed KYC trusted procedure. The proofs of KYC performance by the external trustful entity could be based on, for example, zero-knowledge proof cryptography. The services of external decentralized identity (dID) [96] providers could be used, assuming the relevant country has certified them. This solution would significantly complicate the network architecture in the global context. Each government could require that the dID and KYC providers would be licenced within the given state. It is most probable that not all providers would be able to obtain a licence in all countries, especially if that licence meant that dID and KYC providers had to accept their own readiness to reveal the user's identity as a result of a court or administrative order or any of the FIU's requirements. Some users, and even some governments, would be unwilling to accept that the identification of users could be revealed at the request of any FIU from any country globally. Moreover, making the network dependent on external trusted dID providers would create the risk of blocking the entire network, assuming an attack on a dID provider would involve the given network's central point of failure. The security of a network will be put at risk. It seems that the feasibility of such a concept in highly decentralized global networks is quite poor, if this approach is at all possible. Further research in that scope will be an interesting subject to explore.

Functionalities of exceptional access

Legal requirements for providing certain functionalities in relation to exceptional access should be limited to the absolute minimum necessary for mitigating AML/CFT risks. Creating overly extensive requirements concerning such an instrument would jeopardize network security and/or would make the permissionless technology practically useless. For example, the requirement of providing to the government the functionality of 'seizure' regarding virtual assets (useful in, for example, enforcement proceedings) would not be an appropriate policy tool, as this would open back doors that could be used by hackers to steal currency. Even providing to the government(s) the ability to freeze acceptance of transactions within the network (e.g. in the case of identifying a virtual asset transfer to entities, which are subject to international AML/CFT sanctions), would significantly complicate the system and expose it to hacking. The feasibility of such a measure and its impact on the security of an entire network would require in-depth cybersecurity analysis.

Automated reporting addressee: government(s)

In maintaining the simplicity of a networks' architecture, it would be optimal to include only a single FIU as an addressee of exceptional access. However, achieving this on a global scale seems unlikely [9]. This proposal is submitted assuming an absence of such international cooperation between all countries in the world.

Designing the architecture of exceptional access requires the community to determine to which government (FIU) transactional data are to be automatically reported. As indicated above, the reported data may include only those data which are today visible on privacy-focused blockchains and which are masqued on privacy-blockchains by, for example, zero-knowledge proof cryptography. This additional content can also include any data, either in plain text or encrypted by the user. Most of these data (except those written in plain text by user) would be pseudonymized. In such a situation, I see no reasonable general criterion for determining (on the protocol level) one government (country) which should be the reporting addressee if a network were to grant access to the FIUs of a few countries or a few international organizations. However, this does not constitute an obstacle for proposed tools where a network grants access to many governments.

The data mentioned above, which should be reported to FIU, are today publicly visible on transparent blockchains for everybody, including every government. Therefore, it seems appropriate that pseudonymized data from all transactions on non-transparent blockchains are to be reported, in the same scope, to all those government bodies to which a given network has granted exceptional access. The ability of each government regarding the identification of transaction parties, basing on reported data, would differ. It would depend on the analytical methods and technologies used by a given government, as well as on the additional external data available to that government. The data received by the government would only be pseudonymous. Consequently, the chances to identify users and

suspicious transactions based on data gathered through embedded reporting would vary between countries.

Implementation of the proposed solution would ensure access to transactional data only to governments chosen by a network community and not to everyone, as is the case with transparent blockchains. Data reported to the governments are to be processed on the basis of their national personal data protection regulations. Rules and procedures for governments' processing of personal data vary significantly among countries. Within the EU, this processing is regulated by the GDPR and the Directive 2016/680 on the processing of data for the purpose of preventing and combating crime [97]. In particular, a country is obliged to erase all those personal data where no legal basis for their processing exists. This obligation would also include deleting the secret keys which would grant access to such personal data on a ledger. The rules for governments' processing of such data should be the same as those that apply when FIUs process personal data received from the VASPs or any other intermediaries in AML/CFT proceedings. That regulation should allow for FIU gathering and analysing of the data gathered through the embedded reporting only, as a rule, for AML/CFT purposes.

Transparency of embedded reporting

As permissionless software is open source, the reporting mechanisms (architecture) would and should be transparent to all ecosystem members. Each user would decide whether to use a given financial platform, knowing which countries have been granted access to the transactional data on that network. Today, every Bitcoin or Ethereum 1.0 blockchain user must accept that all people and all governments have access to all data recorded on network ledgers.

The optional character of embedded reporting

The implementation of reporting features into a blockchain protocol is proposed as a free-to-choose option which may allow governments to accept the operation and mass use of privacy-blockchains. The exceptional access should stay optional for privacy-focused networks as long as there are accessible for FIU any other effective AML/CFT tools.

It is highly likely that some networks will not decide to implement them. However, some networks actively search for possibilities for compliance with the GDPR and AML/CFT requirements. Compliance with regulations may attract the mass of users to a given network and place it into the mainstream. The proposed tool, if accepted by regulators, may create an opportunity for permissionless networks to design protocols and network architecture in a way which would enable the GDPR-compliant processing of data, while at the same time also enabling the AML/CFT screening. The national FIU should be allowed by law to accept such a tool if a network offers it.

If there were any other approach or tool, which would enable reaching the AML/CFT goals concerning privacy-blockchains, in that situation the network's community should be free with respect to the decision of which technological option and network architecture to implement. If available and helpful in meeting AML/CFT needs, the FIU should also use any other tools, approaches, or surveillance data sources external to the networks in a given set of circumstances. That is crucial for allowing technological innovation to flourish. As pointed out above, that approach is similar to that accepted by the GDPR: the regulations should set the general goals and should require general effects but should not regulate the technology itself.

Embedded reporting should be optional for network as long as other effective AML/CFT tools or sources of surveillance data were accessible for FIU. When a network does not grant exceptional access to a given government and, at the same time, if any other AML/CFT measures or sources of surveillance data are not accessible for FIU, the government should be allowed by the law to combat privacy-coins. On the other hand, a government or international organization which has gained exceptional access to that network's transactional data should refrain from combating the cryptocurrency of such a financial platform. The VASPs which are under the supervision of that state (or international organization) should be allowed to accept privacy-coins underlying by that DLT infrastructure.

Implementing exceptional access will likely discourage most criminals, as well as participants in a shadow economy, from using that network and its cryptocurrency. Often it may be a massive section of users who abandon the network. Thus, the decision to implement the proposed tool may not be made easily, if at all. However, if the community of a privacy-blockchain has opted not to grant FIU exceptional access, and if, at the same time, effective AML/CFT verification would not be possible using any other means accessible to the FIU, that network's cryptocurrency can be, and should be, combated by the government, including activities aimed at undermining value of the network's cryptocurrency.

Who should take care of an embedded reporting feature?

Implementing any features into the blockchain protocol, including any further updates, depends on the decision on the whole community adopted according to its own rules of off-chain governance. The decentralized governance of networks is a broad issue widely described and analysed in the literature [64]. As a rule, the technical details of the changes to blockchain protocol are proposed by blockchain developers. In highly decentralized networks, the updates are implemented only when a broad consensus is reached, and this consensus is so evident that formal voting is not needed because the major part of the community is cooperating towards the agreed goals [98]. In decentralized governance, there is no central point of decision within the community. Any significant decision regarding the network architecture is discussed, as a rule, within the whole community, including end-users. However, the rules of off-chain governance are different for each blockchain community. The same rules, specific to a given network, would apply to the decision concerning the implementation of a reporting feature into the network's protocol.

Impact of proposed solution on the situation of transparent permissionless blockchains

As emphasized above, exceptional access to masqued data is a reasonable tool only for privacy-blockchains. That tool would not interfere with the status quo of such permissionless DLT-based networks, which are sufficiently transparent for the VASP or FIU to mitigate the ML/TF risk using any other means or approaches. The level of network transparency for AML/CFT purposes today is verified in practice by VASPs, which delist or reject some cryptocurrencies assessing them as not traceable enough. In turn, the position of VASPs is profoundly impacted by the supervisory FIU's assessment.

Each FIU should assess whether the transparency of a given ledger is sufficient for the mitigation of ML/TF risk without granting exceptional access (reporting functionality).

However, as already pointed, we should bear in mind that members of transparent blockchain communities face the legal risk be qualified as (joint) controllers or processors under the GDPR. In case of such qualification, infringement of the GDPR by processing personal data on permissionless transparent ledgers is highly likely. It may be definitely decided only on case-by-case basis.

Qualification of reported transactional data under the GDPR

The qualification of data as pseudonymous or anonymous under the GDPR is presented in detail above, including different possible approaches. According to the relative approach accepted here, providing governments with exceptional access to transactional data on public ledgers would not exclude the possibility of classifying such data as anonymous from the perspective of community members. As indicated by the CJEU in the Breyer case [78], information held by a third person (in this case, the government) could be omitted when assessing whether the data controller (e.g. dApp operator) could use the information to identify a data subject if it was 'prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant' (para. 46 in [78]). In the case of granting exceptional access to the FIU, the possibility of obtaining reported data by the dApp operators or by any other member of the blockchain community from the FIU would be—and should be—prohibited by law.

Outlawing the use of anonymity-enhanced virtual assets and their underlying technology

Presently, the FATF does not recommend banning the anonymity-enhanced virtual assets and blockchains, but it also does not exclude such a solution. States have the discretion to prohibit virtual assets activities or virtual assets service providers [27]. The main reason for the recommendation is that banning such activities and services would not reduce the states' obligations regarding AML. After the outlawing of anonymity-enhanced virtual assets and blockchains, states will still need to actively monitor cyberspace to detect and prosecute violations of the ban, just as they currently do when detecting and prosecuting unregistered VASPs.

In a study prepared for the European Parliament [99], introducing the ban was considered as a possible AML/CFT policy measure Experts warn that 'we must avoid being naïve, even if a ban would be imposed, how do we detect a breach, given that the purpose of the object of the ban just is to obscure identities' [99]. Eventually, they are against the general bans on cryptocurrencies because '[t]hat would go too far' [99]. Instead, they suggest imposing a ban 'on specific aspects facilitating the illicit use of cryptocurrency' [99].

The above indicated proposal to ban only 'certain aspects' facilitating the abuse of technologies and anonymization techniques associated with permissionless DLT networks, however, carries the same 'risk of naïveté' as would a general ban. When prohibiting the use of privacy-coins or 'only' the use of anonymization features, it seems to be equally tricky, and sometimes impossible, to detect users violating each of these bans. Therefore, limiting the ban on the use of anonymity-enhanced features does not solve problems relating to the enforceability of such a ban. The ban on the use of anonymity-enhanced cryptocurrency and its underlying DLT-based network would not be a reasonable tool if the sanctions for failing to comply with the ban were limited to traditional criminal sanctions. The enforcement of these sanctions requires bringing an accused person to court. Such a person often would not be detected, as long as they effectively continue to break the ban using anonymity-enhanced permissionless blockchains. Nevertheless, as the experts indicate, it is worthwhile to consider introducing a ban because 'if authorities bump into the prohibited activities, they have a legal basis for prosecution, insofar not yet available' [99].

Imposing such a ban on the use of anonymity-enhanced cryptocurrency, where reporting features are not provided and any other AML tools or sources of surveillance data are not available to FIU, is vital for a different reason, as presented below.

Towards effective tools for combating non-transparent permissionless DLT-based networks

It is emphasized in the literature that while backdoors seem technically feasible, it is unlikely that they can be sustained in decentralized systems, whose raison d' être is the rejection of privileged parties with special access rights [91]. I see the needs to create means which could motivate decentralized systems to accept limited access rights needed for the achievement of AML/CFT objectives. It should induce the process of shaping the permissionless networks in the direction required by law, to make the systems respectful of some fundamental values which are protected by systems of law, for example, of privacy and public security (the AML/CFT risks minimization).

Why people comply with laws and regulations is complex and controversial within criminology. Empirical research projects have identified variables that are critical for law-abidingness in individuals. Researchers have found that although the severity of punishment is an effective deterrent [100], the probability of punishment is also a crucial factor. '[S]ome significant level of legal enforcement is essential in generating and assuring compliance' [101]. Therefore, regulators may induce shaping the architecture of permissionless DLT-based networks in the direction required by the law only if legal requirements were feasible and if sanctions for non-compliance could be effectively enforced. As indicated above, the use of anonymity-enhanced technologies, such as, for example, zero-knowledge proofs, would result in low enforceability of criminal sanctions. Such technologies are continually being developed and implemented into new platforms. In my opinion, the impact of threatening communities' members with criminal sanctions would not be sufficient to induce shaping the blockchain protocol and architecture in the direction desired by the governments. Moreover, even successful enforcement of a criminal sanction against some individual members of the ecosystem will hardly affect the efficiency and operation of the highly decentralized network. Consequently, traditional criminal sanctions from government, which had to be enforced individually against particular members of ecosystems, appear to no longer be sufficient to motivate all members of globally decentralized community to shape architecture of networks in the direction expected by governments. As decentralized network governance is sometimes it is summarized '[n]o regulatory agency has the resources to go after that type of Medusa-like entity' [102].

Targeting the privacy-cryptocurrency, not its users

Taking into account the above findings, instead of going after privacy-blockchains communities' members to punish them, these tools should be, in my opinion, directed against privacy-cryptocurrency that creates ML/FT risks which cannot be overcome using any available approaches. The focus should be on the direct source of risk to public safety, not on the people which create that risk. An analogy to the off-chain world is where enforcement law agencies directly targeted the building constructed in violation of building regulation, and destroyed it rather than—or in addition to—targeting people responsible for the building's construction. The ultimate aim of new tools in the blockchain space should be to reduce the economic value of the outlawed native cryptocurrency whose value drives the operation of a given platform, in particular by reducing trust in the stability and security of the network. If effective, means that reduce the value of the cryptocurrency will therefore reduce the number of the network's users and nodes. The decreasing number of users and nodes (and thus the decreasing infrastructural and political decentralization [66]) should automatically reduce blockchain security. Networks underlying the privacy-coins will then become more vulnerable to further attacks on their currencies or any activities reducing the value of given privacy coins, which can be systematically repeated by a government until the virtual assets cease to be accepted for payments or used for investment purposes. There is a need for in-depth interdisciplinary research to identify and analyse in detail the whole spectrum of different tools which may help policy makers to govern the permissionless privacy-blockchain space without going after the members of the communities. The nature of possible conceivable tools that can reduce the value and trust in the outlawed (or blacklisted) virtual assets vary significantly, including technological, economic, fiscal, sociological, and legal means. As indicated above, this article is not intended to describe and analyse all these possible tools. This article's goals in that scope are to indicate this direction (targeting the value of privacy-cryptocurrency, not its users), where the effective tools can be found, as in my opinion most promising for further exploration by policy makers. The second goal of the article is to indicate some of these tools to consider by regulators, namely embedded reporting (presented above) and state attacks on outlawed privacy-coins.

State attacks on the value of outlawed privacy-coins

Each permissionless network's security and the value of its native cryptocurrency depend on the mass usage of that network and its cryptocurrency, which, in turn, depends on the prospective trust of persons in and around blockchain ecosystems regarding the network's security and their acceptance of a given currency as a means of payment. The users' confidence in the networks may be significantly undermined by successful attacks on networks which could undermine the trust of the blockchain community in the ability of the network's protocol to ensure smooth operation of the network. By smooth operation I mean particularly the operation without the double-spending of coins, with high level of scalability, and without the risks of gathering by one or few governments enough control to could manipulate the system.

The effects, chances, and costs of successful attack vary significantly—they depend on the network size (level of decentralization) and type of network consensus (e.g. 51% or Sibil attack for networks based on the proof of work [103, 104] or the proof of stake [105]), but also on many other elements of the system's architecture. The levels of decentralization also differ substantially within networks. The idea of decentralization of permissionless DLT-based networks is aimed at excluding all central points of failure within a network's architecture. However, in practice, some elements of centralization do occur [66], which is observable, for example, in relation to different consensus algorithms. Permissionless networks' points of failure usually result from various compromises in the architecture of a given blockchain [106], which are needed to simultaneously ensure many desirable network properties such as scalability, decentralization, security (including anonymity or strong pseudonymity), and low operation costs. The need to strengthen some of these properties often, at the same time, weakens others, causing networks to be vulnerable to different type of attacks [106]. As researchers point out, despite common arguments about the prevalence of blockchain technology in terms of security, privacy, and immutability, in reality, several attacks can be launched against these networks [107]. Attacks on some permissionless blockchains have failed so far because attacking them is cost-effective for attackers who launch an attack to gain profits. However, the profitability of an attack would not be the primary determinant for the states.

This article is not intended to describe the technology of attacks nor to suggest states use one of them. The AML/CFT policy should adopt a technology-neutral approach in that scope and should avoid determining the techniques of attacks on cryptocurrency. The security experts should decide which technology is appropriate to be used on a case-by-case basis. To return to the building metaphor, specific methods of building demolition by law enforcement bodies are not determined by legal regulations because the appropriate means depends on the targeted building's architecture. The same is true for DLT permissionless platforms. Some features are similar among networks, but some are different, for example, different cryptography methods and architectures, varying levels of decentralization and different off-chain governance. No two permissionless distributed ledgers are identical, so the appropriate methods of attack could more or less differ.

As DLT continues to develop quickly and network decentralization increases, the challenges in identifying and developing a successful method of attack on the value of a cryptocurrency will continue to grow [108]. Facebook's current effort to launch the permissionless DLT-based network, which will underly OpenLibra cryptocurrency, shows the possible scale of the challenges faced by governments worldwide. Because of the possible colossal decentralization of some networks in the future, it might be impossible for a single government to impact those networks' ecosystems effectively. In such a situation, cooperation among many governments may become fruitful.

Outlawing of certain virtual assets

The outlawing (banning) of the use of certain virtual assets and their underlying network is, in turn, a legal measure useful for combating a privacy-cryptocurrency if AML/CFT purposes may not be achieved in relation to a particular network in any other ways. However, I do not see the primary purpose of such regulation creating a basis for criminal prosecution against people who breach that law. That ban will likely be so consequential that the outlawed cryptocurrency will not be used in transactions which parties intend to report to FIU or any other supervisory body. Moreover, such a law may also discourage the participation of a significant number of those network's users who prefer to comply with regulations

regardless of threatening sanctions. The outflow of some users from the network can weaken that network's security. Effective attacks on a network cryptocurrency, distorting the network's operational stability, will demonstrate the state's ability to implement such tools. In turn, this should further reduce the outlawed cryptocurrency's value, thereby reducing the economic significance of a given cryptocurrency. The proposed solution will not have a physical impact, and any hardware infrastructure and the targeted DLT-based network can continue to operate until the last single node (and user) records transactions on its ledger. However, the trust and currency value of such a network can drop to zero. Such a cryptocurrency may no longer be accepted as a means of payment and may cease to have the legal status of being a virtual asset. If cryptocurrency is no longer qualified as within the realm of virtual assets, the AML/CFT rules do not apply to it because such a cryptocurrency no longer poses ML/FT risks. In that case, governments should refrain from further interference in that network's operation because such a network has lost the character of a financial platform.

Legal basis for combating a problematic cryptocurrency

To combat some cryptocurrency, including state activities aiming at reducing the value of cryptocurrency, the governments need to adopt a legal basis for interference in several human rights of community members. A necessary element of such regulation is setting out prerequisites for using such a tool towards certain privacy-coins. At minimum, such prerequisites should refer to the lack of availability of any other tools, approaches, or external sources of surveillance data that could effectively allow the FIU to limit the AML/CFT risks in relation to a given network. If a given network enables anonymization of processed data (as defined by the GDPR), it is highly likely that there are no other tools and approaches that would allow for the achievement of AML/CFT objectives; however, it cannot be excluded *a priori*. All circumstances related to a given network must be assessed.

Defining sanctions for non-compliance of privacy-blockchains with AML/CFT requirements should be the second element of such regulations. As pointed out above, these sanctions should not be targeted only against individual actors within the network, but rather against its currency. In the off-chain world, we use similar sanctions, regardless of the possibility of identifying and punishing the individuals who are responsible for breaching the rules.

State attacks on cryptocurrency as a last-resort policy tool

The attack on cryptocurrency is proposed to be included in national or international policies towards permissionless privacy-blockchains as a last-resort tool. It should be targeted only against those DLT-based financial platforms where no other means are available to achieve AML/CFT objectives. If any available approaches of minimizing AML/CFT are effective, there is no reason to attack, nor should be legal grounds for attacking, any network nor its cryptocurrency. In such a case, an attack could be non-proportional interference in human rights (as it is elaborated in the next subsection).

Concept of gradual application of different AML/CFT policy tools can be understood with an analogy used earlier. If somebody built a building with such serious breaches of construction law that the building jeopardized public security, demolishing this building is (and should be) the means of last resort for a law enforcement body. The regulations usually require other means to be applied before the building is destroyed as a law enforcement tool. These other measures, which should be used primarily if they are accessible and efficient, are aimed at maintaining the building by means of ordering the owner to bring the building into compliance with the construction regulations. That is, and should be, a consequence of the requirement of proportional interference with human rights (see the next section). The above considerations could also relate to permissionless blockchains that underlie virtual assets (financial platforms). If governments could use any other effective means to minimize AML/CFT risks on privacy-blockchains, then those means should be primarily used. In a situation where there are no feasible means which may ensure achieving AML/CFT objectives in relation to a given network and if embedded reporting will not grant, the state should be entitled to use effective measures to combat the network, including state attacks on its cryptocurrency.

It would be worthwhile to discuss in the future whether attacks on permissionless networks may and should be used as a policy tool to protect privacy if a network does not ensure GDPR-compliant processing of data. It is doubtful whether it would be a proportional interference in human rights. Today, the sanctions for GDPR non-compliance are primarily severe fines for GDPR non-compliance (although these sanctions can hardly reach most of the controllers' and processors' assets if they are located outside the EU or if they are located on permissionless ledgers and obfuscated by advanced anonymization technologies). Using such a tool may perhaps be acceptable in light of human rights rules if a transparent DLT-based network community does not implement into the network architecture any effective tools which would allow for fast removal of at least content which is treated as illegal worldwide, such as child abuse content. However, I leave this problem for a future discussion.

Proportionality and necessity of the interference with fundamental rights

Regulatory adoption of new AML/CFT policy tools and, in a more general sense, the adoption of new tools to combat crime, always requires the tools' prior assessment in light of several fundamental human rights. Any state's interference that affects software which operates in cyberspace, including permissionless and open-source software, may also potentially interfere in the rights and freedoms of the people creating these ecosystems. The fundamental rights and freedoms of persons in and around permissionless DLT-based ecosystems that may potentially be affected by AML/CFT policy tools are already identified in the literature [13]. These rights and freedoms include, among others, the right to property for owners of virtual assets, freedom to pursue a trade or profession for owners and operators of platforms, freedom of expression (in the context of software design), freedom of telecommunication, data privacy rights, freedom of association within blockchain communities organized as peer-to-peer systems, and freedom of information [13].

However, these rights and freedoms are not protected unconditionally by legal systems. Taking here a European perspective, I focus on the Charter of Fundamental Rights of the EU (henceforth, the Charter) [109] and the European Convention on Human Rights (the Convention) [110]. The Charter is strictly consistent with the European Court of Human Rights (ECHR). According to Art. 52(3) of the Charter, insofar as the Charter contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights under the Charter, including authorized

limitations, are the same as in the Convention [111]. In any case, the level of protection afforded by the Charter may never be lower than that guaranteed by the Convention [111].

According to Art. 52 (1) of the Charter [82], which relates to the scope of protection and interpretation of rights and principles, 'any limitation on the exercise of the rights and freedoms recognized by the Charter must respect the essence of those rights and freedoms; subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others'. The text of the Convention does not contain a similar general provision, but a similar rule may be interpreted from limitations of protected rights and freedoms included in detailed provisions relating to the specific rights or freedoms. For example, the Convention's Art. 8 allows for interference in private life 'if it is necessary for a democratic society'. The ECHR has clarified this requirement, stating that the notion of 'necessity' for the Convention's Article 8 means that the interference must correspond to a pressing social need, and, in particular, must remain proportionate to the legitimate aim pursued (§212 in [112), 113]. To be deemed compatible with Article 1 of Protocol No. 1 to the Convention, the interference in property rights must fulfil certain criteria: it must comply with the principle of lawfulness and pursue a legitimate aim by means reasonably proportionate to the aim sought to be realized (§108–114 in [114), 115]. Such legitimate aims constitute, for example, the prevention of disorder or crime and the protection of the rights of others [116]. Thus, the fundamental rights of an individual should always be weighed against the public interest and the rights and freedoms of others. An examination of the incursion limitations upon fundamental rights in terms of their proportionality and necessity is needed. The search for this balance is inherent in the whole of the Convention [115].

As pointed out above, on the one hand, combating the privacy-coins (and as a result, combating permissionless privacy-blockchains) by AML/CFT policy tools would not be appropriate where there are any other approaches or any other sources of surveillance data accessible to the FIU. The governments should actively search for such tools, including exploring data sources external to networks. It follows from ECHR case law that to determine the proportionality of a general measure taken by the state, the court must primarily assess the legislative choices underlying it (§82–84 [117]). On the other hand, however, if no other effective tools were available for FIU, state attacks on a given privacy-cryptocurrency can be justified in the light of the Convention and the Charter, even if it involves interference with the rights and freedoms of actors in anonymous DLT-based ecosystems.

When assessing the need to interfere with the fundamental rights of the actors of these ecosystems, we should not rely on the traditional model relating to the scope of protection of the fundamental rights of Internet users. In many respects, Internet spaces differ significantly from those of permissionless DLT-based networks. Current AML instruments are ineffective in anonymous or strongly pseudonymous spaces. Furthermore, in the case of the Internet, law enforcement agencies have (limited) possibilities to access personal data through the centralized operators of systems used to provide financial or telecommunication services. In the case of permissionless blockchains, no such centralized administrators exist from which law enforcement agencies could obtain surveillance data. Sometimes Internet Service Providers are indicated as a possible source of surveillance data [16]. However, Internet access is not necessary to use permissionless DLTs. Some of these network' users emphasize that 'the internet is a vulnerability', continuing, 'They are using satellites, ham radios, and mesh networks to stay current on the cryptocurrency... For those wary of tracking and censorship, analogue signals—through satellites and land-based radio devices—offer a welcome buffer from central control' [118]. The proportionality and necessity of crime-combating policy tools within Internet ecosystems significantly vary when compared with permissionless DLT-based space. Consequently, limitations to governmental interference in the fundamental rights and freedoms of these ecosystems' actors may also be different.

When assessing the legality of infringement by AML/CFT tools with the fundamental rights of networks' members, we must also bear in mind that the elementary functions of these networks are much closer to financial institutions (banks, payment institutions) than they are to messenger applications. One of the main differences between traditional financial institutions and permissionless DLT-based networks is that the latter operate under decentralized governance. However, in my opinion, different technology (network) governance is not a sufficient reason for exemption of permissionless privacy-networks from the scope of AML/CFT policy. The new AML/CFT tools should be adopted to the permissionless privacy-networks. If any measures minimizing ML/TF risks (as blacklisting, exceptional access or any other source of transactional surveillance data) are not accessible in relation to a given platform, either for the VASP or for the FIU, such financial platform should be effectively combated by governments.

Concerning the assessment of legality relating to proposed embedded reporting, it is also important to note that the access would cover only pseudonymized data. Governments should not allow these data to be used beyond the need arising from the AML/CFT policy. Presently, financial institutions worldwide constantly collect and analyse all our data before reporting them to governmental agencies. Gathering these data by FIU, directly through embedded reporting and without the use of intermediaries, would be justified when the VASPs are not able to mitigate the AML/CFT risks, as in the case of privacy-blockchains.

Subject the above conditions, if any effective AML/CFT measures are not available for FIU in relation to a given privacy-blockchain, then combating by the states the value of its privacy-coins (including using state attacks on the cryptocurrency as a last resort tool), can constitute a proportional and necessary interference with the fundamental rights of persons in and around DLT-based permissionless networks.

Compliance with public international law

According to the United Nations Convention against Transnational Organized Crime (UNTOC)[29] [119], states must carry out their UNTOC obligations in a manner consistent with the principles of sovereign equality and territorial integrity of states and that of non-intervention in the domestic affairs of other states. The Charter of the United Nations (UN Charter) elaborates on the principle of non-intervention for matters that are 'essentially' within the domestic jurisdiction of any state [120]. According to the judgement of the Permanent Court of International Justice in the 'Nationality Decrees in Tunis and Marocco' case [121], the term 'essentially' in the UN Charter's non-intervention clause reflects an evolutionary conception of this principle. Whether a given matter is within a state's domestic affairs depends on the development of international law.

29 Article 4(1) UNTOC.

Whenever a subject area is regulated by treaty-based or customary rules of international law, it ceases to belong exclusively to the domestic jurisdiction of states that are bound by those rules (Art. 2(7) No. 20 in [122, 123]). Thus, combating transnational organized crime such as ML/FT is not solely within the scope of a state's domestic affairs.

State jurisdiction is an emanation of sovereignty [124]. The jurisdiction in international law encompasses three distinct powers: jurisdiction to prescribe, jurisdiction to execute, and judicial jurisdiction. The first describes state competence to prescribe legal rules, while the second implies state authority to enforce the prescribed rules [124, 125]. The difference between them is significant. Prescriptive jurisdiction may be exercised extraterritorially without the consent of other states. The state may, for example, prohibit and threaten sanctions for the conduct which directly harms its public interest, even when perpetrators are abroad. It is accepted in international law that the state may criminalize conduct without any direct connection to it if that conduct harms the international community as a whole [126]. The ML/FT activity often harm the international community as a whole. Thus, the 'jurisdiction to prescribe' would allow national legislators to include in their national regulations, as AML/CFT tools, the proposed optional embedded reporting or state attacks on cryptocurrency of privacy-blockchains.

In contrast, a state may not exercise its 'jurisdiction to execute' on the territory of another state without the other state's consent [124–126]. That rule creates the need to determine where the 'territory' of a state extends in cyberspace. More and more attention is dedicated to the question of whether and to what extent the rights and duties derived from the principle of 'territorial' sovereignty do apply to cyberspace [127]. The discussions are underway [127–129]. Neither the UN Charter nor any other convention provides an answer. The UNTOC and the 2001 Convention on Cybercrime [130, 131] are quite old and do not take into account the specificity of DLT. Fast technological development hampers reaching a clear and unified position on this matter at an international level. There seems to be consensus amongst states only that customary international law is, in principle, applicable to cyberspace, although there may be a need for a consensual adaptation its rules to the specific characteristics of cyberspace [127].

Although jurisdiction in cyberspace is debated between states, more and more claims are brought before the courts where the question of the borders of sovereignty in cyberspace needs to be answered without waiting for conclusions from an international debate.

The CJEU recently issued a judgement related to the jurisdictional problem in cyberspace in the case 'Google versus Commission Nationale de l'Informatique et des Libertés (CNIL)' [132]. According to the GDPR,[30] this regulation applies, *inter alia*, to the processing of personal data of data subjects who are in the EU, by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to data subjects in the EU, irrespective of whether a payment is required. CNIL served formal notice to Google indicating that, when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted based on that person's name, Google must apply that removal to all its search engine domain name extensions, all over the world (para. 30–31 in [132]). Google challenged this decision, arguing that the right to data removal does not require that the links at issue are to be removed, without geographical limitation, from all its search engine's domain names. Besides, Google argued, by adopting such an interpretation, the CNIL disregarded the principles of courtesy and non-interference recognized by public international law (para. 38 in [132]). During the proceedings, Google implemented a new layout for the national versions of its search engine, in which the domain name entered by the Internet user (e.g. 'google.fr' or 'google.com') would no longer determine the national version of the search engine accessed by that user. The Internet user, being on EU territory, would now automatically be directed to the national version of Google's search engine that corresponds to the place from which the user is presumed to be searching, and the results of that search are displayed according to that place, which is determined by Google using a geo-location process. The CJEU eventually stated that, following the rules of international law, the GDPR does not extend the subject data rights beyond the territory of the EU, and it does not impose on an operator (which, like Google, falls within the scope of that regulation) an erasure obligation which also concerns the national versions of its search engine that do not correspond to the EU Member States (para. 70 in [132]). It is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the protection of the data subject's fundamental rights. Those measures must have the effect of preventing or, at the very least, seriously discouraging Internet users in the EU from gaining access to the links in question using a search conducted based on that data subject's name (para. 70 in [132]).

The GDPR does not define the notion of 'the territory' in cyberspace. Thus, the cyber borders, in which the national data supervisors may enforce the law, were reconstructed by the CJEU in the Google case as the accessibility of data from a physical territory. Where the access to the data from the EU territory is not possible or at least 'seriously discouraging', the EU territory in cyberspace ends.

It is easy to note that this approach results in overlapping jurisdictions of many states in cyberspace. If some data in cyberspace are accessible (without seriously discouraging access) from the physical territory of a certain state, the data are within its cyberterritory. If the data are accessible from the territory of many states (e.g. from the territory of the USA and the EU), the data controller must accept that law enforcement bodies of all these states will execute tools prescribed in their national laws. Thus, the possible conflicts of law enforcement tools executed by different states seem unavoidable and may be resolved by courts in future disputes, which may, in turn, induce more detailed regulations on an international level.

According to the current position of the European Commission, the diversity of cases that can lead to the tension between a global Internet and national jurisdictions means that they may and should not be addressed by one single mechanism (point 10 in [128]). In my opinion, the criterion of determining the borders of jurisdiction to execute, accepted by the CJEU in 'Google vs CNIL', should be applied respectively also to permissionless blockchains. Certainly, it is not an appropriate criterion to be applied in the cyber domain in all cases where there is a need to determine the borders of states' jurisdictions to execute. However, that criterion seems to be appropriate for the AML/CFT policy tools proposed here. When a privacy-blockchain does not grant exceptional access for a state from whose territory that blockchain is accessible, nor there are any other tools or sources of surveillance data able to limit the ML/FT risks, the application of the tools proposed here to combat such a financial platform (its cryptocurrency) should be covered by that state's jurisdiction to enforce. That claim relates only to the means of combating a cryptocurrency because implementing exceptional

30 Article 3(2) GDPR.

access is not possible to enforce and should be left to the free decision of a network as an optional instrument. Therefore, for the platform which enables, by design, data anonymization, but at the same time does not grant exceptional access, nor are any other data sources for AML/CFT screening are available for FIU, that network will suffer the threat of attacks from the side of all the states from whose territory the system is accessible (except for seriously discouraging access). I do not see any other reasonable criterion that could be the basis for determining the borders of the states' enforcement jurisdictions in relation to the analysed problem in permissionless blockchain spaces. Following the prevalent view, I also reject the positions that the borders and the state's jurisdictions disappear in the permissionless blockchain sphere, and that any state would not be allowed in any case to interfere with such blockchain activity without the consent of all other states. This position (rejected here) would result in the excluding effective law enforcement activity in permissionless blockchain spaces.

It is also worth emphasizing that proposed attacks should eventually aim at the value of specific privacy-coin. They cannot interfere with the integrity or functionality of the systems—what is often qualified as violations of territorial sovereignty [127]. The attacker is not able to erase data or change data written on hardware located on the territory of the state, because the unified version of the ledger is distributed and agreed upon between all nodes worldwide. The distributed architecture ensures the safety of the ledger content. The attacker, using its computational power or its own 'stake' (as a coin holder), may try, however, to reach a double-spending effect. The attacker, proceeding in a manner that is determined by the system's protocol, adds a new 'double spending' transaction to the ledger, as any other user may do having enough computational power, stake, or other resources (depending on the given protocol and the type of attack). By doing so, the attacker exploits the features of the protocol according to its rules. It is very doubtful whether using the public and permissionless system according to its rule could be qualified as a violation of territorial sovereignty of all the states where the nodes (and hardware) of that network are located, even though such activity usually causes a drop in the value of the underlying cryptocurrency. Recent studies show that it is not clear in light of international law whether any unauthorized cyber intrusion would violate the target state's sovereignty, or whether there is a threshold in operation [133]. The analysed activity can be compared to the situation where a state starts to play a publicly accessible game and constantly wins against other players using its huge computing power. As a result, that state discourages other players from using that game, and in turn, the value of the game and the value of the game's tokens fall down. A public announcement of that state that in a few days the state will start to play another similar game may hardly be qualified as a violation of the territorial sovereignty of the states where the nodes are located, even though most players abandon that game immediately after that announcement. The measures aimed at devaluing a national currency of another state, as well as any other fiscal restriction against the currency of another state, is not qualified as an intervention on the 'territory' of another state in the meaning of public international law.

It is pointed out that further state practise and *opinio iuris* may give rise to an emerging cyber-specific understanding of sovereignty. Because the prospects of a general treaty in this area are still far away, there would be easier to adopt limited rules before tackling broad principles [133] (for example, on a prohibition on attacking critical infrastructure). Following this approach, it would be desirable to achieve consensus on an international forum about an interpretation according to which the state attacks on permissionless privacy-DLT networks for AML/CFT goals, as a last-resort tool, do not infringe upon any state's territorial integrity. In the absence of such a consensus, the courts' case law will shape cyber borders.

Comparison to the blacklisting approach

When comparing the proposed solution to the blacklisting approach, both are going in a similar direction, not targeting the users but only the value of cryptocurrency. The results of applying the blacklisting system are much more precise because it is not the whole cryptocurrency that is targeted, but only those non-fungible coins that were involved in criminal activity [47, 92].

However, as indicated above, the blacklisting system based on transactions' traceability is not feasible, taking into account its current state of development, where advanced cryptography methods, such as zero-knowledge proofs, are used. In contrast, the solution proposed here is addressed to privacy-blockchains because those networks are likely to enable the GDPR-compliant processing of data when reaching the anonymization threshold (or, at least, stronger pseudonymization than transparent blockchains). The approaches are not antagonistic, but rather, they can be supplementary. The search for AML/CFT tools which are feasible in an anonymous (or strongly pseudonymous) sphere aims at enabling the privacy-coins to be accepted by intermediaries while at the same time assuring protection of data written on ledgers, per the GDPR. Implementation of such tools may facilitate the privacy-blockchains come further into the mainstream use in financial sector. When comparing the proposed solution to the blacklisting approach, the first one is aiming at enabling stronger protection of privacy/personal data by feasibility of that approach within privacy-blockchains, especially within the networks which would enable GDPR-compliant data processing. The blacklisting system, however, interferes less with the fundamental rights of community members because blacklisting approach does not need any features to be implemented into the networks protocols, and consequently the approach does not need to threaten the networks' communities with sanctions if desirable features were not embedded. However, both approaches do not constitute mutually exclusive policy tools for governments to choose between, because they are addressed to different kind of DLT networks (transparent and non-transparent), complementing one another in the scope of AML policy tools in permissionless blockchain spaces.

Discussion of common concerns

In this section, I address some main concerns which may arise in a discussion relating to the proposed tools.

Concern: hindering innovation

The common concern which should be addressed is that personal data protection regulations and the AML/CFT public policy priorities impede innovation by imposing wide-scale restrictions on technology development. In order to reduce that tension, the regulations should adopt a technology-neutral approach. The law should regulate not technology but only its use: the general purposes and values which should be protected by the users of technology, regardless of the technological developments.

The tools proposed in this article are addressed only to the permissionless DLT-based privacy networks. Thus, the scope of the proposal is limited to financial platforms on which virtual assets are transferred and where there is no central point of corporate

responsibility to which AML/CFT obligations may be addressed. There is no reason to impede the technology itself, but only some means of use under decentralized governance. I propose to adopt the technology-neutral approach in AML/CFT regulations as well. They should create only the possibility (and not the obligation) for DLT-based permissionless networks to grant exceptional access for the FIU, without determining the technology of that instrument.

Taking into account the high GDPR requirements and the current development of technology, I find exceptional access to be today the only possible solution likely to allow reconciling the GDPR with AML/CFT needs in the sphere of permissionless networks. However, if any other tools will be identified as being capable of effectively minimizing AML/CFT risks on privacy-blockchains, these tools should be accepted by AML/CFT policies as an alternative to exceptional access. The embedded reporting should remain optional for networks as long as any other effective AML/CFT measures can be exploited by FIU or by the VASPs to minimize the AML/CFT risk. These measures are not yet identified (as presented above in the section 'Searching for solutions: Analysis of existing proposals'), and as a consequence, the regulated VASPs in their practice refrain from trading privacy-coins. Identification of such measures is, and still should be, addressed by interdisciplinary research on these matters. Only if (i) any effective AML/CFT tools are not available and (ii) exceptional access is not granted to FIU, combating of privacy-coins by state attacks should be allowed. Combating privacy-blockchains infringes upon the fundamental rights of community members and should be a tool of last resort (as mentioned in the previous section).

To determine whether a particular infringement with fundamental right is necessary, balancing the interests of the state against the rights of the individual is needed. The ECHR clarified that 'necessary' in this context does not have the flexibility of such expressions as 'useful', 'reasonable', or 'desirable', but rather it implies the existence of a 'pressing social need' for the interference in question. National authorities have to make the initial assessment of the pressing social need in each case, but their decision remains subject to review by the ECHR [113]. I would argue that 'pressing social need' combating a privacy-coins does not exist as far as there exist any possibilities to achieve AML/CFT needs, for example, exceptional access if offered by a network, or use of any other available approach or surveillance data source is possible.

As regards the exceptional access, it is aimed at creating the possibility for privacy-networks to avoid being targeted by states if there are no other means accessible for an FIU to reach AML/CFT objectives. Enabling privacy-networks to flourish is essential from the privacy point of view. Only if any AML/CFT effective measures or sources of surveillance data are not accessible for the FIU in relation to privacy-blockchains, granting exceptional access by networks should become mandatory and should be combined with the threat of combating privacy-coins. That position seems to be similar to the position taken by security and policy experts in the 'Going Dark' debate [134]. The experts indicated that the government should explore new opportunities which arise from technological developments to gather surveillance data from different accessible sources and should do so instead of providing law enforcement with 'exceptional access' to encrypted communications [134, 135]. I propose in the article that exceptional access should stay optional for privacy-focused networks as long as there are accessible for FIU any other effective AML/CFT tools. That proposal is aiming to create a proper balance between public security, data protection, and innovation. However, the difference between the messenger applications and the smartphones, on the one hand, and privacy-blockchains, on the other hand, is that in relation to these former technologies the experts indicate that alternative sources of surveillance data exist [90, 134]. The feasible AML/CFT tools which can be an effective alternative to exceptional access as regards privacy-focused networks that use anonymity-enhanced technology have not yet been identified. It is always possible that the development of research will create such alternative tools feasible in privacy-blockchain spaces.

Concern: Jeopardizing cybersecurity

The famous 'Going Dark' debate [134] touches the ongoing concern on how to reconcile exceptional government access with the increase in cybersecurity risks. Many cybersecurity and policy experts, such as Landau, warn that 'exceptional access is dangerous' [135].

This article is not intended to negate the accuracy of cybersecurity concerns related to messenger applications and smartphones. However, most of the arguments raised in that debate are not relevant or are less relevant for the DLT-based permissionless networks.

First, all participants in the 'Going Dark' debate accept the need for and possibilities of embedding the exceptional access to software used by the financial institutions, such as banks. Exceptional access embedded in financial institutions' systems is dangerous for the assets recorded on bank accounts. However, there seems to be a consensus on the global level that in relation to financial sector, the AML/CFT interest prevails over the others. The DLT-based networks underlying virtual assets are much closer to the financial institution than to messenger applications. In contrast to them, publicly viewable and immutable DLT ledgers of permissionless blockchains are not designed to be used for communication purposes or storing confidential intellectual property. Their primary goal is to enable the transfer of value, as well as to create a trustful proof of the immutability of any data, usually stored off-chain.

Second, exceptional access to data written on such networks does not put confidential intellectual property at risk, if it is stored off-chain as is common practice.

Third, the proposed embedded reporting relates only to the pseudonymized data on privacy-blockchain ledgers. These data are today publicly visible on transparent blockchain ledgers, and transparency of the data did not endanger the security of the most popular networks. The value of such data is significantly reduced for the average (non-state) attacker. In order to be helpful, these data need to be further analysed, which requires a tremendous amount of external data and the use of advanced analytical systems. In practice, those resources are not commonly accessible.

Fourth, in contrast to providers of communication services and products in the Internet space, the economic model of permissionless DLT-based financial platforms does not rely on access to user data to create revenue streams and product functionality, but instead, it relies on mass use of cryptocurrency. Thus, network communities are not motivated to reduce the strength of data encryption. On the contrary, it seems that the strength of anonymity technologies in newly launching networks is continuously growing. That is a trend that should be supported by regulators because it helps to protect personal data written on permissionless blockchains on a high level, possibly a GDPR-compliant level. There is a need to adopt AML/CFT tools as feasible in anonymous space without compromising privacy protection. Allowing only transparent blockchains to grow is not a desirable direction of developing this technology because, as a result, we may have (and, in fact, we already have) publicly viewable databases in cyberspace with non-removable content possibly deeply infringing privacy, including child abuse content [52, 86].

Five, to reduce the risk of third-party attacks on the access granted to the FIU, the FIU may consider using other communications channels, outside the Internet. To improve security and control over internal database management, the government should use permissioned DLT technology. Further analyses of the proposed tools in the light of cybersecurity concerns are desirable.

Concern: access to pseudonymized data only

Exceptional access is proposed to grant to pseudonymized data only. That restriction is an advantage in light of cybersecurity and the protection of privacy, but at the same time, it is a significant drawback from the AML/CFT perspective. As pointed out above, to minimize ML/FT risks, advanced analysis of pseudonymized transactional data and a large amount of external data are needed. However, even if these resources are accessible and are used to analyse the ledger, they do not ensure the transactions' traceability nor users' identification in each case. It is a desirable subject for further research. Extensive research is being conducted worldwide to improve the effectiveness of forensic analysis of data written on distributed ledgers (e.g. see the Titanium project [31]).

Concern: cooperation from all governments and legal systems

One of the main concerns related to the proposed tools may be that proposed tools require cooperation from all governments and the respective legal systems. In my opinion, however, strict organizational or regulatory cooperation between states is not absolutely needed but can be highly fruitful.

As pointed above in the subsection 'Automated reporting addressee: Government(s)', exceptional access may be granted by a network to one or many countries. It would be the network's independent decision. Countries that have been given access can share the required data with other countries, based on multilateral cooperation agreements concluded between many states in the scope of exchanging information in criminal matters. The cooperation between countries may result in the conclusion of 'mutual recognizing agreements' relating to permissionless DLT networks underlying virtual assets, states without access to a permissionless network may commit to respect it as long as the state which has such access will cooperate in the scope of exchanging information in criminal matters.

As indicated in the subsection 'Compliance with public international law', to enforce proposed tools of combating some privacy-coins (as presented above), especially in relation to state attacks on cryptocurrency, it is desirable to reach an international consensus regarding the interpretation of jurisdictional borders in permissionless DLT space. States' practice, *opinio iuris*, and international courts' case law can pave the way for such a consensus to be reached sooner rather than later.

Regarding the purely organizational aspect, attacks on a cryptocurrency can be launched by one state. It eventually depends on which cryptocurrency is targeted and on the volume of necessary resources and know-how. Highly decentralized and popular cryptocurrencies may, indeed, be resistant to attack from the country that does not possess enough resources, such as, for example, computing power, stake (tokens), or knowledge of cyber systems. In order to gather enough resources, the cooperation of many countries is not needed but may be highly desirable—either concerning a given network or in general.

The forums for such international cooperation are already present. For example, the FATF seems to show strong determination to resolve the ML/FT problems generated by permissionless DLT.

Concern: regionality of blockchain networks

If the observed differences between systems of law (for example, in the scope of data protection) are not be overcome by the permissionless DLT, it can lead to the emergence of territorial blockchains. That result has been envisaged by Zamfir, as one of the possible direction of permissionless blockchains development: one day, for example, the 'Ethereum USA' might enforce US economic sanctions, 'Ethereum Europe' might enforce GDPR, while 'Ethereum China' might enforce capital control policies [98]. That would be undesirable effect because it would reduce the practical significance of permissionless DLT. However, as indicated for instance above in regards the territoriality of the GDPR in the Internet space (see section: 'Compliance with public international law'), the regionalization of technology is an unwanted but ongoing process which is present not only in the scope of financial systems but even within the communication technologies.

Summary

The article shows how the GDPR pushes permissionless DLT-based networks to deploy anonymization or, at the very least, strong pseudonymization technologies to enable compliance of data processing with GDPR requirements. At the same time, FATF's anti money-laundering policy instruments aim to combat these privacy-focused networks. As a result, the regulations discussed are on a collision course when it comes to permissionless DLT spaces.

To reconcile these policy objectives—the protection of personal data and ML/FT prevention—I suggest adopting new policy measures as presented in this article. AML/CFT policymakers should make an effort to find and establish the AML/CFT tools which would allow the governments and the VASP to refrain from combating the privacy-focused networks which use anonymity-enhanced technologies, such as zero-knowledge proof cryptography. Use of anonymization or strong pseudonymization technologies is needed to develop GDPR-compliant (or, at least, near GDPR-compliant) permissionless networks. In turn, in order to establish growth conditions for these networks, the VASPs should be allowed to trade the privacy-coins.

One of the AML/CFT tools which may enable the VASP to accept the privacy-coins is embedded reporting: that is, exceptional access for FIU. Blockchain communities themselves should decide on the technological solutions appropriate for a given network for the deployment of proposed new functionalities in their protocols. Legal regulations should not determine the technological details of such solutions. The proposal of exceptional access is aimed at helping privacy-networks to reconcile the requirements of the GDPR and the needs of AML/CFT policy if the network is looking for such tools. As a result of deployment of this tool, a privacy-blockchain should become acceptable for VASP from the AML/CFT point of view, as well as for data protection supervisors, removing or at least minimizing the risk of the GDPR non-compliance that community members face today.

At the same time, it is also necessary to adopt enforceable sanctions if no effective AML/CFT tool or external source of surveillance data is available for FIU in relation to a given privacy-focused network, and if the network does not grant exceptional access to FIU. The sanctions for non-compliance should not, however, be aimed at

or enforced against individual community members. Criminal penalties, which require bringing the individuals to court, have low enforceability within anonymous and globally decentralized environments. Instead, effective measures may directly target the privacy-coins (virtual assets) and its value. The adoption of appropriate legal regulations is needed to create a legal basis for governments to use such measures, including state attacks on cryptocurrency as a tool of last resort.

Acknowledgements

The author thanks to the two anonymous reviewers for their useful comments and critique.

Funding

The open-access publication of this article was funded by the Priority Research Area Digiworld under the program Excellence Initiative – Research University at the Jagiellonian University in Krakow.
Publikacja niniejszego artykułu w trybie otwartego dostępu została sfinansowana ze środków Priorytetowego Obszaru Badawczego Digiworld w ramach programu „Inicjatywa Doskonałości – Uczelnia Badawcza" w Uniwersytecie Jagiellońskim.

Conflict of interest statement. None declared.

References

1. The Financial Action Task Force—Mandate. https://www.fatf-gafi.org/media/fatf/content/images/FATF-Ministerial-Declaration-Mandate.pdf (1 June 2020, date last accessed).
2. 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. *Off J Eur Un* 2018;**L156**: 43–74 (Vth AMLD).
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
4. Li H, Yu L, He W. The impact of GDPR on global technology development. *J Glob Inf Tech Manag* 2019;**22**:1–6.
5. Bennett CJ, Rab CD. Revisiting the governance of privacy: contemporary policy instruments in global perspective. *Regul Gov* 2018; 14(3): 447-464. 10.1111/rego.12222.
6. Goldman E. *An Introduction to the California Consumer Privacy Act (CCPA)*. Santa Clara Univ. Legal Stud, 2019. http://dx.doi.org/10.2139/ssrn.3211013 (10 March 2020, date last accessed).
7. The New York Senate. *Proposal of the Bill "New York Privacy Act" 2019*. https://www.nysenate.gov/legislation/bills/2019/s5642 (10 March 2020, date last accessed).
8. Wang HS, Bakar MA. Information security technology—personal information security specification: China's version of the GDPR. *Eur Data Prot L Rev* 2018;**4**: 535. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl4&div=88&id=&page= (10 March 2020, date last accessed).
9. Abelson H, Anderson R, Bellovin SM, *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. *J Cybersecur* 2015;**1**:69–79.
10. Auer R. Embedded supervision: how to build regulation into blockchain finance. *Bank of International Settlements, Working Papers*, 2019, No. 811.
11. European Securities and Markets Authority. ESMA report on trends, risks and vulnerabilities: No. 1. Paris: European Securities and Markets Authority, 2019. https://www.esma.europa.eu/sites/default/files/library/esma50-report_on_trends_risks_and_vulnerabilities_no1_2019.pdf (10 March 2020, date last accessed), 46, 47.
12. Broeders D, Prenio J. Innovative technology in financial supervision (suptech)—the experience of early users. *FSI Insights* 2018;**9**: 1–19.
13. Rueckert C. Cryptocurrencies and fundamental rights. *J Cybersecur* 2019; 5(1): 1–12. 10.1093/cybsec/tyz004.
14. Quiniou MB. *The Advent of Disintermediation. Innovation, Entrepreneurship and Management*. London: Wiley-ISTE, 2019.
15. Swan M, De Filippi P. Towards a philosophy of blockchain. In: Swan M, De Filippi, P (eds.), *Towards a Philosophy of Blockchain in Metaphilosophy*. London: Wiley, 2017.
16. Finck M. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2018, 15, 45, 46, 48.
17. European Union Blockchain Observatory and Forum. Legal and Regulatory Framework of Blockchain and Smart Contracts, 2019. https://www.eublockchainforum.eu/reports (10 March 2020, date last accessed), 15, 16.
18. Luther WRB. On what grounds? In: Peirce, H, Klutsey, B (eds), *Reframing Financial Regulation: Enhancing Stability and Protecting Consumers*. Arlington, VA: Mercatus Centre at George Mason University, 2016, 391–415.
19. Guadamuz A, Marsden C. *Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies*, 2015. http://firstmonday.org/article/view/6198/5163 (10 March 2020, date last accessed).
20. Luu J, Imwinkelried E. The challenge of Bitcoin pseudo-anonymity to computer forensics. *Crim L Bull* 2016. http://papers.ssrn.com/sol3/papers.cfm?abstract_id¼2671921 (10 March 2020, date last accessed).
21. Reid F, Harrigan M, An analysis of anonymity in the Bitcoin system. In: Altshuler Y, *et al.* (eds.), *Security and Privacy in Social Networks*. New York: Springer, 2013, 197–223.
22. Ober M, Katzenbeisser S, Hamacher K. Structure and anonymity of the Bitcoin transaction graph. *Future Internet* 2013; **5**:237–250.
23. Finck M. Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? *Study for EU Parliament, Panel for the Future of Science and Technology*. Brussels, 2019, 20, 24, 25, 35, 36, 44–49, 51–58, 69, 76, 98.
24. Barsan I. Public blockchains: the privacy-transparency conundrum. *Rev Trimestrielle de Droit Financ* 2019, 45, 48, 53.
25. Japan Times. *The G20 Osaka Leaders' Declaration*, 2019. https://www.japantimes.co.jp/news/2019/06/29/national/full-text-g20-osaka-leaders-declaration/#.XimWoGhKhnI (10 March 2020, date last accessed).
26. FATF. Report on ML/FT risks associated with virtual assets: virtual currencies—key definitions and AML/CFT risks. Paris: FATF, 2014.
27. FATF. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF, 2019. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html (10 March 2020, date last accessed), 11, 6, 18, 20, 23, 26, 28.
28. Purtova N. The law of everything broad concept of personal data and future of EU data protection law.. *Law Innov Technol* 2018;**10**:1–42.
29. Narayanan A, Shmatikov V. Myths and fallacies of personally identifiable information. *Commun ACM* 2010;**53**:24–26.
30. Hinteregger A, Haslhofer B. An empirical analysis of Monero cross-chain traceability. *CoRR*, 2018. http://arxiv.org/abs/1812.02808 (10 March 2020, date last accessed), 22.
31. The Titanium Project. TITANIUM: Tools for the Investigation of Transactions in Underground Markets, 2020. https://www.titanium-project.eu/ (10 March 2020, date last accessed).
32. Conti M, Kumar E, Lal C, *et al*. A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 2017. https://arxiv.org/pdf/1706.00916.pdf?utm_source=securitydailynews.com (10 March 2020, date last accessed).
33. Li W, Chen L, Xin J. Traceable and linkable ring signatures, traceable range proofs and applications on regulatable privacy-preserving blockchains. *IACR Cryptol ePrint Arch* 2019;**925**: 1–28.
34. Ibáñez L, O'Hara K, Simperl E. *On Blockchains and the General Data Protection Regulation*. Southampton: University of Southampton.

https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (10 March 2020, date last accessed).
35. Noether S, Mackenzie A. The Monero research lab. *Ring Confidential Trans Ledger* 2016;**1**:1–18.
36. Bünz B, Bootle J, Boneh D, *et al*. Bulletproofs: short proofs for confidential transactions and more. In: *2018 IEEE Symposium on Security and Privacy (SP), San Francisco CA*, 2018., 315–34.
37. Wu H, Wang F. A survey of noninteractive zero knowledge proof system and its applications. *Sci World J* 2014;**2014**:1–7.
38. Guan Z, Wan Z, Yang Y, *et al*. BlockMaze: an efficient privacy-preserving account-model blockchain based on zk-SNARKs. *IACR Cryptology ePrint Archive*, 2019. https://eprint.iacr.org/2019/1354.pdf (10 March 2020, date last accessed).
39. Ben-Sasson E, Bentov I, Horesh Y, *et al*. Scalable, transparent, and post-quantum secure computational integrity. *Arch Tech Rep* 2018;**46**: 1–83.
40. Xie T, Zhang J, Zhang Y, *et al*. Libra: succinct zero-knowledge proofs with optimal prover computation. In: Boldyreva A, Micciancio D (eds.). *Advances in Cryptology—Crypto 2019, Lecture Notes in Computer Science*. New York: Springer, 2019.
41. Gao Y, Chen X, Chen Y, *et al*. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access* 2018;**6**:27205–13. 10.1109/ACCESS.2018.2827203
42. Kumar A, Fischer C, Tople S, *et al*. A Traceability Analysis of Monero's Blockchain. In: Foley S, Gollmann G, Snekkenes E (eds), *Computer Security—ESORICS 2017, Lecture Notes in Computer Science*. New York: Springer International Publishing, 2017, 153–73.
43. Möser M, Soska K, Heilman E, *et al*. An empirical analysis of traceability in the Monero blockchain. *Proc Priv Enhanc Technol* 2018;**2018**: 143–63.
44. Buterin V. *Ethereum 2.0 Promises Better Privacy, Scalability in* 2020. https://forkast.news/vitalik-buterin-ethereum-2-0-promises-better-privacy-scalability-in-2020/. https://forkast.news/vitalik-buterin-explains-ethereum-2-0's-four-phases:-sharding,-scaling,-proof-of-stake-and-more/ (10 March 2020, date last accessed).
45. Bitcoin. Protect Your Privacy, 2020. https://bitcoin.org/en/protect-your-privacy (10 March 2020, date last accessed).
46. Yousaf H, Kappos G, Meiklejohn S. Tracing transactions across cryptocurrency ledgers. In: *28th USENIX Security Symposium*, 2019, 7–850. https://www.usenix.org/system/files/sec19-yousaf_0.pdf (1 June 2020, date last accessed).
47. Möser M, Böhme R, Breuker D. Towards risk scoring of Bitcoin transactions. In: Böhme R, Brenner M, Moore T, Smith M (eds), Financial Cryptography and Data Security, 1st Workshop on BITCOIN Research. Vol. **8438**. *Lecture Notes in Computer Science*, 2014, 16–32.
48. Truong N, Sun K, Lee GM, *et al*. GDPR-Compliant Personal Data Management: a Blockchain-based Solution. *IEEE Trans Inf Forensics Secur* 2020;**15**:1746–61.
49. Mirchandani A. The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR, 29 Fordham Intell. *Prop Media Ent LJ* 2019;**1201**: https://ir.lawnet.fordham.edu/iplj/vol29/iss4/5 (1 June 2020, date last accessed).
50. Kuner Ch, Bygrave LA, Docksey Ch, Drechsler L. (eds), *The EU General Data Protection Regulation (GDPR). A Commentary*, 2020.
51. Hoofnagle CJ, van der Sloot B, Zuiderveen FJ. *The European Union General Data Protection Regulation: What it is and What It Means*, 2018. UC Berkeley Public Law Research, Ch Paper. http://dx.doi.org/10.2139/ssrn.3254511 (1 June 2020, date last accessed).
52. Child Abuse Images Hidden in Crypto-currency Blockchain, BBC, 6 February 2019. https://www.bbc.com/news/technology-47130268 (1 June 2020, date last accessed).
53. Finck M, Pallas F. They who must not be identified—distinguishing personal from non-personal data under the GDPR, Max Planck Institute for Innovation & Competition Research Paper No. 19-14, International Data Privacy Law, 2020, 17–18.
54. Rampone F. *Data Protection in the Blockchain Environment: GDPR is not a Hurdle to DLT solution*s, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3383619 (1 June 2020, date last accessed), 1.
55. International Telecommunication Union, Focus Group on Application of Distributed Ledger Technology. Technical report: distributed ledger technology regulatory framework, 2019. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf (1 June 2020, date last accessed), 17.
56. Judgement of CJEU in case C-210/16 Wirtschafsakademie Schleswig-Holstein, 2018, EU:C:2017:796.
57. Judgement of CJEU in case C-25/17 Jehovan todistajat, 2018, EU:C:2018:551.
58. European Parliament. Report on blockchain: a forward-looking trade policy, 2018, AB-0407/2018.
59. Bacon J *et al.*, Blockchain demystified: a technical and legal introduction to distributed and centralised ledgers. *Rich J L Technol* 2018;**25**(1): 71–72.
60. Judgement of CJEU in case C-40/17 Fasion ID, 2019, ECLI:EU:C:2019:629.
61. European Union Blockchain Observatory and Forum. Blockchain and the GDPR, 2018. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (10 March 2020, last accessed), 14.
62. Wirth C, Kolain M. Privacy by BlockChain design: a blockchain-enabled GDPR-compliant approach for handling personal data. In: Prinz, W, Hoschka, P. (eds), *Proceedings of the 1st ERCIM Blockchain Workshop* 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design. https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf (1 June 2020, last accessed), 5.
63. Article 29 Working Party. Opinion on the concepts of "controller" and "processor", 1/2010, WP 169, 00264/10/EN.
64. De Filippi P. Blockchain technology and decentralised governance: the pitfalls of a trustless dream. *Decentralised Thriving: Governance and Community on the Web 3.0*. http://dx.doi.org/10.2139/ssrn.3524352 (1 June 2020, date last accessed).
65. Bano S, Catalani C, Danezis G, *et al. Open Technical and Economic Challenges*, 2019. https://libra.org/en-US/permissionless-blockchain/#open_technical_and_economic_challenges (10 March 2020, date last accessed).
66. Buterin V. *Different meaning of Decentralisation*, 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralisation-a0c92b76a274 (10 March 2020, date last accessed).
67. *The GDPR—Adequacy Decisions of the European Commission*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (10 March 2020, date last accessed).
68. Judgement of CJEU in case C-311/18 Facebook and Schrems, 2020, ECLI:EU:C:2020:55
69. Austrian Data Protection Authority. DSB-D123.270/0009-DSB/*2018*, 2018. https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html (10 March 2020, date last accessed).
70. Commission Nationale Informatique et Libertés. *Blockchain and the European Union General Data Protection Regulation—the CNIL's Perspective*, 2018. https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (10 March 2020, date last accessed).
71. European Union Agency for Cyber Security. *Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation*. Brussels: ENISA, 2018. https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions (10 March 2020, date last accessed).
72. Article 29 Data Protection Working Party. *Opinion 4/2007 on the Concept of Personal Data*, WP 136, 01248/07/EN, 2007. https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf (10 March 2020, date last accessed).
73. Dworkin MJ. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, 2015 (10 March 2020, date last accessed).
74. European Union Agency for Cybersecurity. Pseudonymisation techniques and best practices. *Recommendations on Shaping Technology According to Data Protection and Privacy Provisions*. Brussels: ENISA,

2019. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (10 March 2020, date last accessed), 9, 15, 26.
75. Millard C. *Cloud Computing*. New York, USA: Oxford University Press, 2013, 182.
76. Opinion of AG Campos Sanchez-Bordona in Case C-582/14 *Breyer* (2016), EU:C:2016:339.
77. Spindler G, Schmechel P. *Personal Data and Encryption in the European General Data Protection Regulation*, 2016, 7 JIPITEC 163.
78. Judgement of CJEU in case C-582/14 *Breyer* (2016) EU:C:2016:779.
79. Article 29 Working Party. *Opinion 05/2014 on Anonymisation Techniques*, WP 216, 0829/14/EN, 3.
80. Stalla-Bourdillon S, Knight A. Anonymous data v. personal data—a false debate: an EU perspective on anonymization, pseudonymization and personal data. *Wis Int Law J* 2017;**34**:284–322.
81. ISO Standards. *Health Informatics—Pseudonymization, ISO/TS 25237*, 2017. https://www.iso.org/obp/ui/#iso:std:iso:25237:ed-1:v1:en (10 March 2020, date last accessed).
82. European Union Agency for Cybersecurity. *Recommendations on Shaping Technology According to GDPR Provisions: An Overview on Data Pseudonymisation*. Brussels: ENISA, 2018. https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions (1 June 2020, date last accessed).
83. Mourby M, Mackey E, Elliot M, *et al.* Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Comp L Secur Rev* 2018;**34**:222–8.
84. Deuber D, Magri B, Aravinda S, *et al.* Redactable Blockchain in the Permissionless Setting. *IEEE Symposium on Security and Privacy (SP)* 2019;645–659. https://arxiv.org/pdf/1901.03206.pdf (10 March 2020, date last accessed), 3.
85. Tziakouris G. Cryptocurrencies—a forensic challenge or opportunity for law enforcement? An Interpol perspective. *IEEE Secur Privacy* 2018;**16**: 92–94.
86. Matzutt R, Henze M, Ziegeldorf J, *et al.* Thwarting unwanted blockchain content insertion. In: *Proceedings of the 2018 IEEE International Conference on Cloud Engineering (IC2E)*, 2018. Vol. **1**, 364–70.
87. FATF. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012-2019)*. Paris: FATF, 2019. www.fatf-gafi.org/recommendations.html (10 March 2020, date last accessed).
88. FATF. Public Statement on Virtual Assets and Related Providers, 2019. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html (10 March 2020, date last accessed).
89. Mizrahi A. *European Crypto Exchange Bitbay Ends Monero Trading due to Anonymity Features*, 2019. https://news.bitcoin.com/european-crypto-exchange-bitbay-ends-monero-trading-due-to-anonymity-features/ (10 March 2020, date last accessed).
90. Segal A, Feigenbaum J, Ford B. *Open, Privacy-Preserving Protocols for Lawful Surveillance*, 2016. https://arxiv.org/abs/1607.03659 (10 March 2020, date last accessed).
91. Keller P, Florian M, Böhme R. *Colaborative Deanonimisation*, 2020, arXiv:2005.03535
92. Möser M, Narayanan A. *Effective Cryptocurrency Regulation Through Blacklisting*, 2019. https://pdfs.semanticscholar.org/07ca/977361ba58e67f21be53865f4bcf1dcb04ef.pdf (1 June 2020, date last accessed), 1, 14, 15.
93. Matzutt R, Henze M, Ziegeldorf JH, *et al.* Thwarting Unwanted Blockchain Content Insertion. In: *Proceedings of the 2018 IEEE International Conference on Cloud Engineering (IC2E)*, 2018, Vol. 1, pp. 364–70.
94. Z Cash. How it Works, 2019. https://z.cash/technology/ (10 March 2020, date last accessed).
95. Concordium, 2020. https://concordium.com/ (10 March 2020, date last accessed).
96. European Union Blockchain Observatory and Forum. Blockchain and Digital Identity, 2018. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf (10 March 2020, date last accessed).
97. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *Off J Eur Un* L, 2016;**119**:89–13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 (10 March 2020, date last accessed).
98. Zamfir V. *Blockchain Governance 101*. https://blog.goodaudience.com/blockchain-governance-101-eea5201d7992 (1 June 2020, date last accessed).
99. Houben R, Snyers A. *Study for EU Parliament, Cryptocurrencies and blockchain - Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. Brussels: European Parliament, 2018. http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (10 March 2020, date last accessed), 83, 99.
100. Friesen L. Certainty of punishment versus severity of punishment: an experimental investigation. *South Econ J* 2012;**79**:399–421.
101. Kagan R, Gunningham N, T D. Fear Duty and regulatory compliance: lessons from three research projects. In: Parker C, Nielsen VL (eds.). *Explaining Compliance: Business Responses to Regulation*. Cheltenham, UK: Edward Elgar Publishing, 2011, 37–58.
102. CleanApp. SEC V. *EtherDelta{Big Picture}*, 2018. https://medium.com/cryptolawreview/sec-v-etherdelta-big-picture-da9ba070efa2 (10 March 2020, date last accessed).
103. Ye C, Li G, Cai H, *et al.* Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. In: *Proceedings of the 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian,* 2018. 15–24. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8563187&isnumber=8563172 (10 March 2020, date last accessed).
104. Tayebeh R, Mohammad Hossein M, Mohammad D, *et al. On the Feasibility of Sybil Attacks in Shard-Based Permissionless Blockchains*, 2020, arXiv:2002.06531v1. https://www.researchgate.net/publication/339324146_On_the_Feasibility_of_Sybil_Attacks_in_Shard-Based_Permissionless_Blockchains (1 June 2020, date last accessed).
105. Kanjalkar S, Kuo J, L Y, *et al. I Can't Believe It's Not Stake! Resource Exhaustion Attacks on PoS*. Urbana Champaign: University of Illinois. http://www.ifca.ai/fc19/preproceedings/180-preproceedings.pdf (10 March 2020, date last accessed).
106. Neudecker T, Hartenstein H. Network layer aspects of permissionless blockchains. *IEEE Commun Surv Tutor*, 2018; 21(1): 838–856. 10.1109/COMST.2018.2852480.
107. Deirmentzoglou E, Papakyriakopoulos G, Patsakis C. A survey on long-range attacks for proof of stake protocols. *IEEE Access*, 2019. 7: 99.
108. Gilad Y, Hemo R, Micali S, *et al.* 2017. Algorand: scaling byzantine agreements for cryptocurrencies. In: *Proceedings of the 26th Symposium on Operating Systems Principles (SOSP '17)*. Association for Computing Machinery, New York, NY, USA, 51–68. https://doi.org/10.1145/3132747.3132757 (1 June 2020, date last accessed).
109. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.**2012**, 391–407.
110. *The Convention for the Protection of Human Rights and Fundamental Freedoms*. https://www.echr.coe.int/Documents/Convention_ENG.pdf (1 June 2020, date last accessed).
111. *Official Explanations of the Charter Articles*. https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles (1 June 2020, date last accessed).
112. *Judgement of ECHR in case Piechowicz v. Poland*, 2012. http://hudoc.echr.coe.int/eng?i=001-110499 (1 June 2020, date last accessed).
113. Council of Europe/European Court of Human Rights. *Guide on Article 8 of the European Convention on Human Rights*, 2019, https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (1 June 2020, date last accessed), 12.
114. *Judgement of ECHR in case Beyeler v. Italy [GC]*, 2000. http://hudoc.echr.coe.int/eng?i=001-58832 (1 June 2020, date last accessed).

115. Council of Europe/European Court of Human Rights. *Guide on Article 1 of Protocol No. 1 to the European Convention on Human Rights*, 2020. https://www.echr.coe.int/Documents/Guide_Art_1_Protocol_1_ENG.pdf (1 June 2020, date last accessed), 17, 26.
116. *Judgement of ECHR in case Pendov v. Bulgaria*, 2020. http://hudoc.echr.coe.int/eng?i=001-201890 (1 June 2020, date last accessed).
117. *Judgement of ECHR in case A.-M.V. v. Finland*, 2017. http://hudoc.echr.coe.int/eng?i=001-172134 (1 June 2020, date last accessed), 15.
118. Barbe G. *The Cypherpunks Tapping Bitcoin via Ham Radio*, 2019. https://www.wired.com/story/cypherpunks-bitcoin-ham-radio/ (10 March 2020, last accessed), 2.
119. *The United Nations Convention against Transnational Organized Crime, Adopted by General Assembly resolution 55/25 of 15 November 2000*. https://www.unodc.org/unodc/en/organised-crime/intro/UNTOC.html (1 June 2020, date last accessed).
120. *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime, United Nation Office on Drugs and Crime*. https://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html (1 June 2020, date last accessed), 16.
121. *Nationality Decrees in Tunis and Marocco (French zone)*, (1923), PCIJ, Series B, No. 4, 24.
122. Simma B, Khan D, Nolte G, *et al.* (eds.). *The Charter of the United Nations*: A Commentary (3rd edn), Vol. **I**, 2012.
123. Rose C, Kubiciel M, Landwehr O. (eds), *The United Nations Convention against Corruption: A Commentary*. New York, USA: Oxford University Press, 2019, 45.
124. Cassese A. *International Law*. New York, USA: Oxford University Press, 2005, 49–51.
125. Lowe V. Jurisdiction. In: Evans, M. (ed.), *International Law*. Oxford, UK: Oxford University Press, 2006, 338–339.
126. Milanovic M. *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policies*. New York, USA: Oxford University Press, 2011, 24–25.
127. Heintschel v. H W. Legal implications of territorial sovereignty in cyberspace. In: Czosseck C, Ottis R, Ziolkowski K, (eds), *Proceedings of the 4th International Conference on Cyber Conflicts*, 2012, NATO CCD COE Publications, Tallinn, 7.
128. European Commission. *Digital Single Market Factsheet: Internet Policy and Governance in Plain Language*, 2014, Point 10: Internet and Jurisdiction. https://ec.europa.eu/digital-single-market/en/news/internet-policy-and-governance-plain-language (1 June 2020, date last accessed).
129. Patrick G, Bana A. Rule of law versus rule of code: a blockchain-driven legal world. *IBA Legal Policy & Research Unit Legal Paper*, 2017.
130. Convention on Cybercrime, ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (1 June 2020, date last accessed).
131. Council of Europe. Explanatory report to the convention on cybercrime (ETS No. 185).
132. Judgement of CJEU in case C 507/17 Google v. CNIL, 2019, ECLI:EU:C:2019:772.
133. Moynihan H. *The Application of International Law to State Cyberattacks—Sovereignty and Non-Intervention*. London: The Royal Institute of International Affairs Chatham House, 2019.
134. Gasser U, Gertner N, Goldsmith J, *et al. Don't Panic: Making Progress on the 'Going Dark' Debate*. Cambridge, MA: Berkman Klein Centre for Internet & Society, 2016.
135. Landau S. The national-security needs for ubiquitous encryption. In: Gasser U, Gertner N, Goldsmith J, Landau S, Nye J, O'Brien D, Olsen M.G, Renan D, Sanchez J, Schneier B, Schwartztol L, Zittrain J (eds.), *Don't Panic: Making Progress on the 'Going Dark' Debate*. Cambridge, MA: Berkman Klein Centre for Internet & Society, 2016.