Research article
UDC 34:004:347.211:004.8
EDN: https://elibrary.ru/mloxmi
DOI: https://doi.org/10.21202/jdtl.2024.29

Overcoming the Friction between the "Right to be Forgotten" and Blockchain Technology through a New Approach

Fabio Severino
Traent SRL, Pisa, Italy

Ludovica Sposini ✉
Sant'Anna School of Advanced Studies, Pisa, Italy

Keywords

digital technologies,
European Union,
General Data Protection Regulation,
Hybrid blockchain,
law,
Legislation,
Personal data protection,
private blockchain,
public blockchain,
right to be forgotten

Abstract

Objective: this paper explores the challenges arising from the conflict between blockchain technology and the "right to be forgotten" as provided by the European data protection framework.

Methods: in the First Section, the author provides a brief description of the evolution of blockchain technology and the most pressing issues between traditional blockchain models and UE's legislations. Among the latter, the author analyzes the specific issue concerning the clash between the traditional blockchains (both private and public models), typically immutable, and the individual's right to cancellation or modification of own personal data. This section emphasizes the importance of personal data protection, which has always been one of the main tasks for supranational legislators. The legal regulation of data protection and the relevant judicial practice of the European Court of Human Rights is analyzed. The author raises the problem of expressing the free self-determination of an individual in the form of controlling their personal data on the Internet. The Second Section of this contribution is dedicated to the study of probable ways to solve the existing incompatibility and to make the distributed ledger system compatible with the European data protection legislation. An emphasis is made on the model provided by "Traent" company, which ensures the right to data cancellation or modification. The capability of this model to solve the said contradiction is analyzed.

✉ Corresponding author

Results: the study delves into the peculiar features of the new model to understand how it strategically utilizes the advantages of public and private blockchains guaranteeing not only the validity and authenticity of the chain where the transaction was performed, but, most importantly, the modification and granular cancellation of client's personal data. This innovative solution offers a potential path forward for navigating the complex intersection of data privacy and blockchain innovation in the European context.

Scientific novelty: Traent has implemented a "hybrid" model blockchain that, incorporating both public and private components, to achieve an effective compliance with the European Union regulations, especially those concerning data protection and privacy.

Practical significance: the obtained conclusions and proposals can be taken into consideration in improving the compliance of blockchain technologies with the European Union General Data Protection Regulation.

For citation

Severino, F., & Sposini, L. (2024). Overcoming the Friction between the "Right to be Forgotten" and Blockchain Technology through a New Approach. *Journal of Digital Technologies and Law, 2*(3), 565–584. https://doi.org/10.21202/jdtl.2024.29

Contents

Introduction

2008 represents a turning point in the era of the so-called "Digital Revolution" as it saw the publication of Satoshi Nakamoto's article entitled "Bitcoin: A Peer-to-Peer Electronic Cash System"[1]. The latter was part of the "cypherpunk" movement, which, in order to oppose the

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://clck.ru/3EGDkg

restrictions on individual freedoms and, in particular, on the right to privacy resulting from the new technologies, had identified bitcoin as a useful tool for this purpose: an electronic currency that would make use of cryptographic technologies on a large scale and that would make it possible to create exchange systems (goods, services and, above all, information) that were secure and respectful of irrefutable.

Nakamoto proposed the creation of a communication protocol, i.e. an immutable ledger organised into separate "blocks", each of which contains one or more transactions. These were linked together to form a chain, hence the name "blockchain". Each block had a "header" within which was contained the hash, an alphanumeric string, of all transactions recorded in that block; the time stamp and the hash of the previous block.

This technology utilised various technologies including: i) asymmetric key encryption which allows verification of the paternity of messages as well as its integrity; ii) the peer-to-peer system which has the advantage of eliminating the need for a central authority to validate transactions; iii) the "proof of work", a consensus-building mechanism based on the use of computational resources to solve a mathematical problem. In short, the node that first manages to propagate the correct solution to the rest of the network receives reward for the service rendered. At the same time, the system is sure of the correctness of this result precisely because a large number of resources had to be used to arrive at it[2].

It was based, then, on a network of computers sharing between them a distributed register containing a copy of all transactions made on the chain. In this way, it was possible to guarantee, on the one hand, a secure registration system since it would be very hard to rewrite all the blocks; on the other hand, it was transparent because each time a new transaction was made, it was recorded on each "copy" of the distributed register. This meant that each participant could verify the transactions and have access to the data without the necessary presence of a centralised higher entity. On the contrary, it redistributed validation power among users in substantially equal parts, contributing to the creation of an effectively transparent and, above all, more democratic system[3]. This technology, which was originally created for the exchange of cryptocurrencies, has, thanks to

[2] It should be noted that this is only one of many consensus mechanisms that have been developed, including: i) the so-called "Proof of Stake" (PoS) according to which the possibility of validating transactions is directly proportional to the amount of assets that node possesses; ii) the "Delegated Proof of Stake" which is based on a sort of vote whereby each user who possesses assets in the system can delegate the validation of the transaction to another; iii) the "Deposit-based consensus" whereby in order to add a blockchain block it is necessary to first make a binding deposit; iv) the "Proof of Existence" whereby only those with specific authorisations or documents can validate; v) "Proof of Authority" (PoA) whereby authorisation to validate transactions is granted solely on the basis of the identity of the node itself. For a comprehensive explanation of each mechanism, see (Sarzana & Nicotra, 2018).

[3] European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis, where it is said that: "Blockchains shift some control over daily interactions with technology away from central elites, redistributing it among users. In doing so, they make systems more transparent and, perhaps, more democratic" (4). See also (Lacity & Treiblmaier, 2022).

its potential, immediately spread far beyond the mere exchange of cryptocurrencies (Sarzana & Nicotra, 2018; Rajasekaran et al., 2022; Belotti et al., 2019; Michael et al., 2018; Ammous, 2016)[4]: from the financial services sector, healthcare, supply chain management, the so-called "e-voting"[5] and, recently, to digital goods (such as NFT) and product passports.

2015 marked the transition to its so-called "second generation" when Ethereum, the first programmable blockchain, was developed, contributing to the emergence of smart contracts and the development of decentralised applications on blockchain. Moreover, the merits of this technology were also soon recognised by the European legislator, who stated that its use could speed up the way transactions are negotiated and executed, with major advantages for the development of the internal market[6]. However, he also noted that EU legislation, which came into being before blockchain, was inadequate to deal with the possible risks and dangers that blockchain poses for fundamental rights and, above all, for the protection of personal data[7].

1. Definition, functioning, and basic features of Blockchain

Since 2008, several blockchains have been implemented, each with peculiar characteristics that differentiate them from one another. Due to this heterogeneity, it is very difficult (if not impossible) to provide a unified and shared definition of the phenomenon[8]. Nevertheless, some general considerations can be made.

First of all, blockchain technology is a sub-category of "Distributed Ledgers Technology" (henceforth DLT), i.e. special types of databases in which data are recorded, shared and synchronised on a distributed network of computers. The data can represent any exchangeable value susceptible to economic valuation such as money, contracts, medical records, buying and selling of goods and services as well as birth or marriage certificates. However, it should be noted that DLTs differ from blockchain in the way they record and verify information.

---

4 Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. https://clck.ru/3EGEp4

5 For an in-depth analysis of the areas mentioned, see (European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis; Gupta et al., 2023; Mccorry et al., 2021).

6 European Parliament. (2022). Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance).

7 Ibid.

8 (Walch, 2016). It is worth noting that the extreme diversity of blockchain does not allow for the construction of a universally accepted (and acceptable) inclusive definition of all platform types currently on the market (and those to come). However, if a definition of the phenomenon would make it possible to circumscribe it and thus treat it in a unified manner, it would, however, suffer from a rigidity that is ill-suited to technological change. It therefore seems preferable, as already observed by authoritative doctrine regarding the definition of a digital platform, to adopt a functional case-based approach. In this regard, see (Bertolini et al., 2021).

As just mentioned, they are distributed databases because they operate on a network of multiple nodes, typically installed on a single computer (technically a server). When a party wants to execute a transaction, it is transmitted to the network that validates it according to the consensus algorithm (Sarzana & Nicotra, 2018). In this way, each block in the chain that forms the ledger is immutably linked to the previous one as well as the next. In other words, once a block is added, it can no longer be modified without altering the subsequent part of the chain. More specifically, the integrity of the ledger is guaranteed because rewriting the following blocks would require solving the puzzle multiple times in a timely manner, an operation infeasible due to the cost and computational power required. Everything is then shared by every node in the network and is always updated and synchronised.

1.1. One technology, different classifications

In common parlance, the term "blockchain" is used to refer generically to technology based on distributed ledgers. In reality, this category contains different types of blockchain, each with its own characteristics and peculiarities.

There are the so-called "public" blockchains whose fundamental element is their "decentralization". First of all, they are typically "permissionless", meaning that users can do any operations, including reading and proposing new blocks as well as validating transactions. That is, these blockchains (e.g. the Bitcoin platform) do not require any central authority to act as an intermediary or to validate the transactions that take place in the network. On the contrary, it uses a peer-to-peer mechanism by directly connecting users, who become, at the same time, active subjects for the validation of transactions and passive ones because they hold all the information. As we mentioned above (Sarzana & Nicotra, 2018), it is a system based on the so-called "consensus mechanism" because all participants are obliged to verify and create transactions following specific rules that have already been encoded in blockchain software. For example, one of the most widely used consensus algorithms is Proof of Work (PoW) which relies on the computing or processing power of computers (called "miners") to solve mathematical problems (puzzle), which becomes increasingly complex after each validated transaction, as quickly as possible. Not only that, but each participant keeps a copy of the ledger, so that everyone can participate in the network and all their data is accessible anytime, anywhere.

This peer-to-peer system makes the system much more resistant to possible attacks because it would be necessary to hit the majority of the nodes distributed on the network (Aponte-Novoa et al., 2021). In fact, every change is quickly visible to all participants and cryptographic signatures guarantee the integrity and authentication of transactions (this is referred to as "tamper-resistant" (Austin & Di Troia, 2022)).

Therefore, various remuneration systems have been implemented for each correctly validated transaction as well as protocols to make it extremely difficult to engage in abusive conduct.

From these brief considerations, it is already possible to understand the advantages and criticalities of this type of open blockchain. Being based on a decentralized (and, therefore, distributed) system ensures both the integrity of transactions and greater security as it is more challenging to attack. Moreover, transactions are stored indefinitely to guarantee the verifiability of the entire chain. Finally, they are public and, thus, freely accessible, as there is no centralised control by an authority.

On the other hand, however, public blockchains tend to be very slow in handling transactions and, therefore, not entirely adequate to handle large volumes. This is because they have the major problem of scalability, i.e. as the number of nodes in the network increases, the speed of executing and handling transactions are reduced[9]. Not to mention the environmental impact that public models have[10].

Then there are "private" blockchains that are accessible only by specifically authorised users. Consequently, the personal (and other) data of network participants is shared within the network. In particular, it involves users whose identity is well known, since in order to become a node, it is necessary to fulfill a series of requirements and to have obtained the approval of a central administrator. Not only that, but those wishing to join the network are often required to subscribe to terms of service describing their respective rights and obligations. It is evident then why particularly stringent consensus mechanisms are not required in this case: here the system does not have to "earn" the trust of operators through costly consensus mechanisms because each node, being easily identified and recognisable, can be held responsible (Raymond Choo et al., 2020). In these types of systems, transaction validation is usually delegated to a trusted subset of nodes. In other words, if the public blockchain can in some ways be said to be the emblem of democracy and decentralisation, in the private ones the paradigm is that of oligarchy: not all nodes have equal importance.

This system undoubtedly has several technical advantages. First, it is much faster (as only a very small group of nodes are responsible to verify and propagate new blocks) and, secondly, thanks to the possibility of restricting access to the content of the blockchain, it appears to be more secure from a confidentiality and privacy point of view. However, one of the main weaknesses of private models lies precisely here. If it is true that the security of this technology derives from the distribution and decentralisation of the register, in private ones, the latter is not distributed but concentrated in the hands of a single (or few) entity.

---

9 Proof of Work (PoW) scalability issues stem from its design, which requires significant computational effort to validate transactions and add blocks. As more nodes join, they still must process and validate all transactions independently, not increasing overall throughput. Additionally, PoW's high energy consumption and latency in block propagation further constrain scalability, leading to longer transaction times and higher fees during peak demand. On the matter, see (Gramoli, 2022).

10 For more on the environmental impact of blockchain see Bitcoin Energy Consumption Index. Digiconomist. https://clck.ru/3EGHgF

Both categories just described can in turn be "permissioned" or "permissionless"[11]. Thus, one can have "public permissionless blockchains" in which anyone can participate in the consensus mechanism and propose transactions (this is the case, for example, of platforms such as Bitcoin or Ethereum) as well as "public permissioned blockchains" that allow all users to see the transaction log and conclude any type of operation, even though only a small number of nodes are allowed to participate in the consensus mechanism. A clear example of this is Ripple[12].

The same applies to private ones[13], where a distinction is made between "private permissioned blockchains" that limit the transaction and display capacity of the ledger to only those nodes that participate in the network, and it is the platform operator who chooses who to let participate in the consensus mechanism. This happens, for instance, in the case of Rubix[14]. Exactly the opposite happens in "private permissionless blockchains"[15], which limit the parties allowed to perform transactions and access the ledger, but unlike the former, here the consensus mechanism is open to anyone.

1.2. Public and private blockchains… and the third way

Both public and private blockchains have advantages and disadvantages. The former, as we have seen, is "universally" transparent (as transactions are visible to all participants in the network), reliable (due to their decentralised nature, they are less prone to single points of system failure), decentralised and accessible (they are managed by a globally distributed network of nodes which makes them highly resilient) and immutable; however, they are very slow because they suffer from scalability problems due to the volume of transactions and the need for decentralised confirmation, they have very high transaction costs and they do not guarantee privacy as they are public. Similarly, the latter are certainly more efficient because they are scalable and faster (this is explained by the fact that there is no need for decentralised confirmation and, therefore, transactions are processed faster), they guarantee the privacy of the information contained in the network and the network organisers have complete control over the governance and rules of the network; on the other hand, however, private blockchains are less transparent, centralised and less secure.

To solve some of the inherent problems of these two models, a third type of 'hybrid' blockchain has been developed that lies, we might say, somewhere in between the two.

11 Ismail, A. (2020). Permissioned Blockchains for Real World Applications. Lakehead University.

12 Ripple. https://clck.ru/3EGDyK

13 Nascimento, S. et al. (2019). Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies. European Commission. https://clck.ru/3EGDUk

14 Rubix. https://clck.ru/3EGE3L

15 However, it should be noted that this is a very rare case as A private permissionless blockchain is a bit of a contradiction in terms, as «private» typically implies restricted access, while «permissionless» implies open access. However, a blockchain could be designed with certain hybrid characteristics.

In other words, these models have characteristics of public and private blockchains, but offer greater flexibility and adaptability to a wide range of use cases. Firstly, they are flexible because they allow the degree of decentralisation and privacy to be customised to the specific needs of the application for which they are used. On the other hand, these systems are also more reliable because, by combining public and private elements, the overall robustness and resilience of the network can be increased (Smith, 2020). Moreover, they are interoperable and can address scalability issues by balancing control and decentralisation. However, the combination of public and private factors may lead to a higher degree of complexity in the system, from which, in turn, comes the risk of introducing new security vulnerabilities into the system. Finally, the design and implementation of a hybrid blockchain may require significant resources and very high costs.

1.3. Case study: Traent and advantages of hybrid blockchain

The move to hybrid blockchain represents an important point of evolution in the discipline, which is particularly flexible and adaptable. These objectives prompted Traent[16], an Italian company, to implement a hybrid blockchain model capable of cumulating the advantages (and solving the criticalities) of both public and private systems[17].

As mentioned earlier, in public blockchains each node participating in the network has a copy of the ledger, so that each replica contains all transactions and cryptographic evidence associated with each block in the chain. For this reason, the public blockchain is more secure, since to modify a transaction would require all nodes, which are in a potentially infinite number, to modify the chain ("fork-resistance"[18]). However, precisely because it is particularly difficult to modify the chain and rewrite it, once data has been published on it, it can no longer be modified or deleted.

On the other hand, private blockchains try to precisely solve this problem: since they are shared among a limited number of participants, it is possible to limit the sharing of data. The criticality of this mechanism stems precisely from the fact that users, by definition not impartial, are also those who validate the transactions that take place on the platform. This implies, therefore, that they could easily decide to change what is written on the chain, since there is no third party with a super partes controller function. The third-party user then has no way of verifying whether or not the chain has been altered.

---

16 Traent. https://clck.ru/3EGJHN

17 It should be noted that the description of the technical functioning of the platform is beyond the scope of this discussion, and therefore we refer to (Pelosi, 2023). However, it seems useful to attempt to describe only briefly how Traent's system operates so as to allow the reader to better appreciate the reflections on the right to be forgotten and blockchain.

18 Fork resistance is the ability of a blockchain network to withstand and recover from a hard fork, which is a permanent divergence in the blockchain caused by conflicting rules. Hard forks can be the result of contentious network upgrades and can lead to the creation of a new cryptocurrency. See (Golden et al., 2020).

The blockchain proposed by Traent, on the other hand, succeeds in achieving "external" (or even "public") auditability precisely by adopting a hybrid model. Specifically, the company provides interested users with a private blockchain to perform any transaction, which is materialised on the private ledger in a block together with a cryptographic proof. Subsequently, the latter is published – via a system component called Notary (Pelosi et al., 2023) – on an external public blockchain. This way, the cryptographic proofs associated with the individual blocks written on the (private) ledger are published on the (public) blockchain. Thus, when an outsider wants to participate in the chain, he can be sure that transactions have not been altered by others verifying on the external blockchain thanks to the externalised cryptographic evidence – that there has been no fork in the private chain.

2. The clash between blockchain technology and the "right to be forgotten" in the context of the European data protection legislation. The solution adopted by Traent

Recognition of the right to be forgotten as a fundamental element in the protection of personal identity and human freedoms is a recent achievement for modern society, which is based on the platform economy model (Xue et al., 2020; Cohen, 2017; Kenney & Zysman, 2016; Stark & Pais, 2020; Acs et al., 2021). The protection of personal data has always been a primary objective for supranational legislators, so much so that it has already been recognised in the EU Charter of Fundamental Rights as an autonomous and independent right[19] to private and family life[20]. To apply this principle effectively and, at the same time, ensure the free movement and protection of data within the Union, the Commission presented in 2012 a package aimed precisely at ensuring harmonisation between the Member States.

In this respect, an essential contribution came from the case law of the Court of Justice of the European Union (henceforth CJEU) and, in particular, the well-known Google Spain case[21]. The case concerned a Spanish citizen who had addressed both the internet site operator and Google – as search engine – to obtain the removal of his data published several years ago in a national newspaper. In particular, the plaintiff complained that the data were no longer up-to-date and claimed the right so that the search engine would not redirect users to the page that reported the inaccurate news. In this judgment, the Court laid down some basic principles for the effective implementation of the right of users to have their personal data deleted online. Among the various issues addressed in this decision, it recognised

19 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012 (pp. 391–407), Art. 8.

20 Ibid., Art. 7.

21 CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

the user's right to demand that certain harmful content was no longer available online and that, consequently, it was no longer indexed among the platform's results. This is because, according to the CJEU, the fundamental rights under Articles 7 and 8 of the Nice Charter must prevail over the economic interest of the provider as well as the public in information.

Although the supranational court is crystal clear in affirming the prevalence of the reasons of the user claiming the right to erasure, the same cannot be said in the jurisprudence of the European Court of Human Rights. An example is the case of Węgrzynowski and Smolczewski v. Poland where the conclusions were quite different[22]. In this decision, the ECtHR does not recognise the user's right to remove online information but rather tries to strike a balance between freedom of expression under Article 10 of the ECHR and the right to be forgotten. In other words, while the complete removal of the content was deemed disproportionate, the most appropriate remedy was found in requiring the online publisher to publish additional clarifications to the article in question, to provide an update of the subject matter.

Subsequently, in 2016 the EU adopted the General Data Protection Regulation 2016/679 (henceforth GDPR)[23], with which it was finally expressly recognised in Article 17 – headed "Right to erasure ('right to be forgotten')" – that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay"[24].

This provision thus recognises two precise rights: on the one hand, the right to "erasure of data", which allows the data subject to request the deletion of data concerning him on the assumption that after a certain period of time they are no longer of collective interest and no longer correctly represent his personal identity. On the other hand, this provision also recognises the "right to be forgotten" in the strict sense, which is broader than the former,

22 CEDU, Węgrzynowski and Smolczewski v. Poland, Application No. 33846/07, 16 July 2013. https://clck.ru/3EGJgf

23 European Parliament and Council. (2016). 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) (Text with EEA relevance).

24 The rule goes on to identify the prerequisites necessary for this right to be activated by the user: "(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)". In addition, Article 16 provides for the right to rectification of data. For an in-depth discussion of the right to be forgotten after the adoption of the GDPR, see (Alessi, 2017; Kocharyan et al., 2021; Mantelero, 2013; Politou et al., 2018; Finocchiaro, 2010; Peguera, 2019).

and which requires the data controller not only to delete all information concerning the data subject but also any link, copy or reproduction that may refer to that specific data. In other words, the intention is that the user should enjoy broader control over the management of his or her data on the web, as an expression of free individual self-determination.

2.1. The incompatibility between the right to be forgotten and blockchain

A fundamental characteristic of the blockchain is its immodifiability, which appears, however, to be completely at odds with Article 17 GDPR, which instead allows users to request and obtain at any time the modification of their data as well as their complete deletion. This is true for both public and private blockchain models. The former, in fact, are extremely secure because they make use of a distributed system where every participant in the network has a copy of the ledger. This advantage, however, has the downside that modifying or deleting data once it has been entered into the chain is not possible, because the information would have to be deleted from each node (the so-called principle of unchangeability of the public blockchain applies). The latter, on the other hand, tries to solve this problem by allowing users to choose which data to publish and which not to publish (and with whom to share it) at the expense, however, of a system that is not totally secure. The same can be said of the simple modification or correction of data because in the blockchain each block knows whether the previous one contains the data entered. This means that if an attempt were made to change the information in one block of the chain, subsequent blocks would fail verification.

Several alternative solutions were developed to make the system compatible with European data protection law, since Article 17 does not specify how the "erasure" of data is to be concretely achieved. Some considered that mere anonymisation of the data was sufficient, while others proposed "putting the data out of use", i.e. ensuring that the data controller is no longer able to use the information for decision-making purposes, does not pass it on to any other third party, takes technical measures to secure the data and, finally, is obliged to delete the data when possible. Others, on the other hand, suggest making the data completely inaccessible by destroying the private key corresponding to the public key that every user of the network possesses. In this regard, even the CJEU does not perfectly clarify the interpretation of the rule of the regulation, but seems to recognise, however, that erasure means the complete destruction of data. In particular, the case of Peter Nowak v Data Protection Commissioner recognised a candidate in a written examination "the right to ask the data controller to ensure that his examination answers and the examiner's comments with respect to them are, after a certain period of time, erased, that is to say, destroyed"[25]. On this point, also the European Parliamentary Research Service (EPRS)[26] stated that "whether

[25] CJEU, Peter Nowak v Data Protection Commissioner, Case C-434/16, 20 December 2017, ECLI:EU:C:2017:994.

[26] Service EPR. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?

this can be seen as a blanket statement that erasure always amounts to destruction in unclear, especially since the case at issue did not directly deal with the right to erasure. The statement could thus also be explained by the specific context at hand and the fact that outright destruction of the examination copy may be the most straightforward means of destruction (although the blackening out of the relevant information is another obvious option)"[27].

2.2. The model developed by Traent to guarantee the right to data removal and modification

An interesting solution to guarantee respect for the right to be forgotten is the one provided by Traent in its hybrid blockchain. This model does not provide for the entire data to be written in the block of the (private) ledger, but only a "reference"[28] to it, which refers to the outside of the chain where the entire data is actually saved. In addition, a cryptographic proof ("digest") is also inserted in the same block. In this way, thanks to the reference written in the (private) chain, the user concerned can access the complete externalised data and verify, thanks to the digest, that it has not been altered.

This dual mechanism not only makes the system more secure – because it allows the authenticity of the information contained in the blockchain to be ascertained – but also allows users to delete the data entered: since these are outside the private blockchain, it becomes possible to delete them without altering the chain. Thus, the verification of the blockchain remains valid because, in fact, the blocks of the ledger are never actually altered. However, since the digest is associated with those externalised data (which no longer exist because they have been deleted) it stops working. At this point, the hybrid model developed by Traent creates a new block – inserted in the private ledger – in which the data (to which the reference and the cryptographic proof refer) in the previous one is accounted for as having been deleted. Thanks to this system, the user can verify that the chain has not been fraudulently changed and, at the same time, that the data is genuine because it is clear from the next block that a data deletion operation has been performed.

Already from these brief considerations, it is clear that the solution proposed by Traent is the one that is certainly the most compliant with Article 17 GDPR because it allows the complete deletion of data but also their simple modification. It thus succeeds in fully implementing the European regulation as well as the interpretation that the CJEU seems to have given of it.

---

27 Ibid.

28 This could be, for instance, a URL.

Conclusions

The European Parliament recently passed the Artificial Intelligence Act (henceforth AIA)[29] intending to increase trust in AI systems and mitigate their risks. For this, it bans or severely restricts the use of those systems that present unacceptable risks to the safety, health, dignity, and autonomy of people. However, efforts are made to support innovation and the development of increasingly sophisticated technologies to exploit their full potential for the internal market[30].

Despite the adoption of this law, the accountability of AI systems remains an issue that continues to preoccupy experts in the field. This is mainly due to the lack of effective technical solutions to fully explain the reasoning that led an algorithm to provide a certain output rather than another, so much so that it is not uncommon to hear talk of "black box solutions" (Springer et al., 2017; Veale & Zuiderveen Borgesius). Blockchain can, then, be a valuable tool to achieve the goal of a "trustworthy AI"[31]. First, it can lead to greater transparency and visibility of algorithms since ledger status and transaction logs are stored securely, decentralized, and accessible to all node participants. Moreover, it can help guarantee the immutability of the results: the ledger is composed of numerous blocks, each of which contains a series of transactions and data and is protected by a cryptographic hash that refers to the same hash contained in the previous block. Therefore, even the smallest change to one of the blocks invalidates the entire chain.

In conclusion, it can be said that blockchain seems to be, to date, the most appropriate – and perhaps the only – solution to meet the requirements of the most recent European legislation on both data protection and AI systems. However, this technology still presents several challenges that need to be addressed, among which guaranteeing the user's right to delete and modify his or her information is particularly pressing. In this sense, then, the hybrid model implemented by Traent can provide, as briefly demonstrated, a particularly effective alternative to[32]. By doing so, it becomes possible to fully exploit the potential of blockchain for the development of truly explainable algorithms and AI systems, as well as to eliminate – or at least alleviate – any doubts about blockchain's compatibility with the GDPR.

---

29 European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

30 Ibid

31 Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), where it is said that: "This proposal aims to implement the second objective for the development of an ecosystem of trust by proposing a legal framework for trustworthy AI. The proposal is based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them" (1). See also (Nassar et al., 2019).

32 For a more in-depth look at Traent's technology and the benefits it can bring regarding specific case studies, see the following link: Traent. https://clck.ru/3EGKux

References

Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, *57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, *32*(1), 145.

Ammous, S. (2016). *Blockchain technology: What is it good for?* http://dx.doi.org/10.2139/ssrn.2832751

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, *9*, 140549–40564. https://doi.org/10.1109/ACCESS.2021.3119291

Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/comst.2019.2928178

Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, *51*, 133–204.

Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, *3*, 391–404. (In Italian).

Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. https://doi.org/10.1201/9781003004998

Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. https://doi.org/10.1007/978-3-031-12578-2

Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, *80*, 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61–69.

Kocharyan, H., Vardanyan, L., Hamuľák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, *21*(2), 96–115. https://doi.org/10.2478/iclr-2021-0015

Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4), 33. https://doi.org/10.1145/3461461

Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, *1*, 35–44.

Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, *10*(1), e1340. https://doi.org/10.1002/widm.1340

Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). https://doi.org/10.1109/wetice57085.2023.10477792

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*, 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-030-38181-3

Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).

Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium onDesigning the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).

Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, *14*(3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

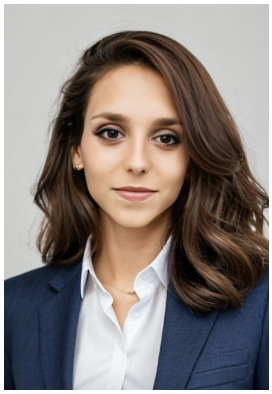
Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, *36*, 713–765.

Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, *2020*(1), 8877128. https://doi.org/10.1155/2020/8877128

Authors information

Fabio Severino – CTO, Traent SRL
Address: Borgo Stretto 3, 56127, Pisa, Italy
E-mail: fabio.severino@traent.com
ORCID ID: https://orcid.org/0000-0002-9538-1218



Ludovica Sposini – PhD Candidate (Law), DIRPOLIS Institute (Institute of Law, Politics and Development), Sant'Anna School of Advanced Studies
Address: Via Domenico Vernagalli 22R, 56127 Pisa, Italy
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: https://orcid.org/0000-0003-2188-8996
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The authors would like to thank Traent SRL for providing all the technical documentation concerning its technology for the purpose of this article. In addition, we would also like to thank the Jean Monnet Centre of Excellence on the Regulation of Robotics and AI (EURA) for the support.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 16, 2024
Date of approval – July 2, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:347.211:004.8
EDN: https://elibrary.ru/mloxmi
DOI: https://doi.org/10.21202/jdtl.2024.29

Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн

Фабио Северино

Traent SRL, Пиза, Италия

Людовика Спозини ✉

Школа перспективных исследований Сант'Анна, Пиза, Италия

Ключевые слова

блокчейн гибридный,
блокчейн публичный,
блокчейн частный,
Европейский союз,
законодательство
защита персональных данных,
Общий регламент по защите данных,
право,
право на забвение,
цифровые технологии

Аннотация

Цель: в статье рассматриваются проблемы, связанные с конфликтом между технологией блокчейн и «правом на забвение», предусмотренным европейской системой защиты данных.

Методы: в первом разделе кратко описаны эволюция технологии блокчейн, а также наиболее актуальные проблемы, возникающие между традиционными моделями блокчейна и законодательством Европейского союза. Среди последних проанализирован конкретный вопрос конфликта между природой традиционных блокчейнов (как частных, так и публичных моделей), как правило, неизменяемых, и правом индивида требовать удаления или изменения своих персональных данных. В этом разделе отмечается важность задачи по защите персональных данных, которая всегда была одной из главных для наднациональных законодателей. Приводится анализ правового регулирования защиты данных и соответствующей практики Европейского суда по правам человека. Поднимается проблема выражения свободного самоопределения личности в виде контроля над управлением персональными данными в Интернете. Второй раздел посвящен изучению возможных путей решения сложившегося противоречия, позволяющих сделать систему распределенных реестров совместимой с европейским законодательством о защите данных. Сделан акцент на модели, предложенной компанией Traent, гарантирующей право на удаление и изменение данных. Анализируются возможности данной модели по разрешению указанного противоречия.

✉ Контактное лицо

Результаты: рассмотрены особенности новой модели и ее возможности по стратегическому использованию преимуществ публичных и частных блокчейнов. Показано, что данная модель гарантирует не только достоверность и подлинность цепочки, по которой была проведена транзакция, но и, что особенно важно, изменение и полное удаление персональных данных пользователя. Это инновационное решение потенциально дает возможность справиться с противоречием между требованиями конфиденциальности данных и развитием блокчейна в европейском контексте.

Научная новизна: компании Traent удалось реализовать «гибридную» модель, которая включает в себя как публичные, так и частные компоненты блокчейна, что позволяет достичь эффективного соответствия нормам Европейского союза в отношении защиты и конфиденциальности данных.

Практическая значимость: полученные выводы и предложения могут учитываться при совершенствовании соответствия блокчейн-технологий принципам Общего регламента Европейского союза по защите персональных данных.

Для цитирования

Северино, Ф., Спозини, Л. (2024). Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн. *Journal of Digital Technologies and Law*, *2*(3), 565–584. https://doi.org/10.21202/jdtl.2024.29

Список литературы

Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, *57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, *32*(1), 145.

Ammous, S. (2016). *Blockchain technology: What is it good for?* http://dx.doi.org/10.2139/ssrn.2832751

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, *9*, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291

Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/comst.2019.2928178

Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, *51*, 133–204.

Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, *3*, 391–404. (In Italian).

Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. https://doi.org/10.1201/9781003004998

Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. https://doi.org/10.1007/978-3-031-12578-2

Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, *80*, 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61–69.

Kocharyan, H., Vardanyan, L., Hamuľák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, *21*(2), 96–115. https://doi.org/10.2478/iclr-2021-0015

Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4), 33. https://doi.org/10.1145/3461461

Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, *1*, 35–44.

Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, *10*(1), e1340. https://doi.org/10.1002/widm.1340

Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). https://doi.org/10.1109/wetice57085.2023.10477792

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*, 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-030-38181-3

Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).

Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium onDesigning the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).

Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, *14*(3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

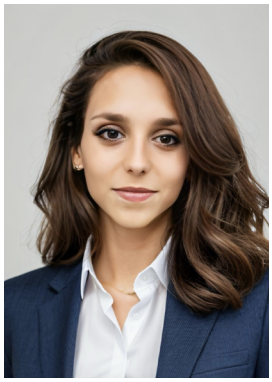
Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, *36*, 713–765.

Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, *2020*(1), 8877128. https://doi.org/10.1155/2020/8877128

Сведения об авторах

Фабио Северино – технический директор, компания Traent S.r.l.
Адрес: 56127, Италия, г. Пиза, ул. Борго Стретто, 3
E-mail: fabio.severino@traent.com
ORCID ID: https://orcid.org/0000-0002-9538-1218



Людовика Спозини – соискатель степени PhD в области права, Институт права, политики и развития (DIRPOLIS), Школа перспективных исследований Сант'Анна
Адрес: 56127, Италия, г. Пиза, ул. Виа Доменико Вернагалли, 22R
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: https://orcid.org/0000-0003-2188-8996
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность компании Traent SRL за предоставление всей технической документации, касающейся данной технологии, для написания статьи. Кроме того, авторы благодарят за оказанную поддержку Центр передового опыта в области регулирования робототехники и искусственного интеллекта имени Жана Монне (Jean Monnet Centre of Excellence on the Regulation of Robotics and AI, EURA).

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 16 июня 2024 г.
Дата одобрения после рецензирования – 2 июля 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.