International Journal of Law and Society
2022; 5(3): 251-256
http://www.sciencepublishinggroup.com/j/ijls
doi: 10.11648/j.ijls.20220503.12
ISSN: 2640-1894 (Print); ISSN: 2640-1908 (Online)

Re-Interrogating the Concept of Smart Contracts Through EU GDPR's Lenses

Olumide Babalola

School of Law, University of Reading, Reading, United Kingdom

Email address:
olumide@oblp.org

To cite this article:
Olumide Babalola. Re-Interrogating the Concept of Smart Contracts Through EU GDPR's Lenses. *International Journal of Law and Society*. Vol. 5, No. 3, 2022, pp. 251-256. doi: 10.11648/j.ijls.20220503.12

Received: May 21, 2022; **Accepted**: June 11, 2022; **Published**: July 29, 2022

Abstract: The term 'smart contracts' is superficially misleading. It does not connote 'contracts' as we know them, rather it is a technical coinage which represents computer codes automated to execute and consummate agreements to the exclusion of third parties. Since its proposition in the 90s, smart contracts have offered alternative and seamless channels of consummating economic and social transactions with the increased processing of personal data as an integral part of the system. By design, smart contracts function with many actors shouldering various responsibilities with data protection implications one one hand while the automated codes organically impact privacy when utilized for desired results. Even though there exists no generally acceptable definition of smart contracts, this article examines some academic attempts at defining the contemporarily technical term of smart contracts within the context of its recorded history as traced back to Nick Szabo's intervention in the 90s. Since smart contracts are predominantly transactional, the article analyses how they oblige users personal autonomy and control on the personal data processed and other techniques ensuring personal data is not compromised while utilizing smart contracts. Ultimately, the article discusses smart contract's interplay with data protection vis a vis some requirements of data controllers under the EU General Data Protection Regulation (GDPR) and the concludes that privacy must be of paramount consideration at the inception of every smart contract.

Keywords: Blockchain, Data Protection, GDPR, Privacy, Smart Contracts

1. Introduction

In recent times, the phenomenal concept of 'smart contracts' has gained an unusual manner of ubiquity in economic and legal circles owing to the pre-eminence of technology to the world's socio-economic activities.[1] This article briefly examines the relationship between smart contracts and data protection as envisaged under the General Data Protection Regulation (GDPR) regime by examining the various definitions of the concept in the light of their peculiarities and connotations while analysing some provisions of the GDPR that impact the concept of smart contracts. This article essentially amplifies the data protection concerns raised by the increasing utility of smart contracts for the contemporary exchange of goods and services.

2. Conceptual Definitions

The discovery of smart contracts is traceable to the invention of the Greek mathematician and engineer - Hero Ctesibus (of Alexandria) - who built a vending machine[2] in the first century. [1].

However, while some academics agree that vending machines are smart contracts, [2] others argue [3] that they merely offer goods and services to the entire world and not necessarily contracts as we understand the concept.[3]

[1] Gregory Voss, 'Data Protection Issues for Smart Contracts' in Marcelo Corrales, Marcelo Corrales, Mark Fenwick & Stefan Wrbka, (eds.) *Smart Contracts: Technological, Business and Legal Perspectives* (Hart Publishing/Bloomsbury, 2021), Lokke Moerel, 'Blockchain and Data Protection' in Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò (eds) The Cmabridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Cambridge University Press, Cambridge, 2019).

[2] The machine dispensed holy water in Egyptian temples after users inserted coins.

[3] A contradictory position was taken when the author, in one breathe agreed that vending machines can automate the making and performance of a contract yet argues that such automation does not make them smart contract.

Adding to the lack of consensus on the history of smart contracts, there is no universally acceptable definition of smart contracts, however, what is certain is that, coinage of the term is attributable to Nick Szabo - a computer scientist, legal scholar and cryptographer – who defined smart contracts as 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises.' [4].

Although Szabo agrees that vending machines are a specie of smart contracts, his definition contemplates the entirety of such contracts (from conception to completion) in digital form, hence disregarding examples of contracts with a mixture of manual and automated processing stages.[4]

In their own definition, Levi and Lipton refer to the concept as 'computer code that automatically executes all parts of an agreement and is stored on a blockchain-based platform.' [5] Ante also defines them as 'de-centrally anchored scripts on blockchain or similar infrastructure that allow the transparent execution of predefined processes' and 'a script that is anchored on a blockchain or similar distributed infrastructure … and validated across the network and executing predefined actions' [6] but these identical definitions lose sight of the fact that smart contracts[5] were utilized before the blockchain technology was invented even though they are now interconnected. [7].

Rather than define smart contracts, Cuccuru describes them 'as digitalization of assets, their representation by computer codes and dealing with them (including their transfer and exchange) via computer programmes which are executed across 'nodes of blockchain' without the input of third parties.' [8] All these attempts however unduly restrict the meaning of contracts to only goods at the expense of services which may be offered via smart contracts as well. Savelyev says it is 'an agreement whose performance is automated' but this intervention overlooks other components of contracts itself, especially the furnishing of consideration as an integral part of contract making process. [9].

While Zheng et al define smart contracts as 'computerized transactions protocols that execute the contracted terms of an agreement' which execution is 'automated to be self-executory when specified conditions are met,' [10] Paech notes that they are 'computer codes that are designed automatically to execute contractual duties upon the occurrence of a trigger event.' [11] Corrales et al define them as 'self-executing and autonomous computer protocols that facilitate the performance and execution of agreements between two or more parties' [12] and Schellekens simply defines smart contracts as 'codes' which do not necessary connote contract in legal parlance. [13] Xu et al note that smart contracts are 'computer protocols which can be self-executed and self-verified once developed and deployed without any human interventions.' [14].

Truong et al elaborately define smart contracts as 'computer programs deployed onto a blockchain network which automatically executes 'actions' when necessary 'conditions' are met, specifying business logic of a service that participants have agreed to' and that it is 'a form of decentralised automation that facilitates, verifies, and enforces an agreement in a transaction and records the results (i.e., state changes) into a ledger.' [15].

From the foregoing academic attempts[6], the aggregate conclusion on smart contracts is that they are digitalized agreements which are solely or partly executed by automated means without the intervention of third parties.

3. GDPR and Smart Contracts

The GDPR now represents a global standard for data protection legislation and regulations – the 'centerpiece of the reform of EU regulatory framework for protection of personal data' which has become a 'global benchmark' in data protection parlance. [16] Even though it is limited in scope, organizations outside the EU still envisage its remote application to their activities especially where they target customers within the EU or they have other business interests in the union.[7] Like every digital technology, the utility of smart contracts raises a number of privacy and data protection concerns but this is not to say that, smart contracts do not also conversely aid data protection in a number of ways. For example, decentralization of data in smart contracts aids confidentiality, integrity and control over data. [17].

[4] It is worthy of note that, before Szabo's conception of 'smart contracts' as a term, some contracts had already been integrated into the digital space. See Kevin Fandl, 'Can Smart Contracts Enhance Firm Efficiency in Emerging Markets?' (2020) 40 (3) Northwestern Journal of International Law & Business, 336, 348.

[5] The concept of smart contracts was introduced in 1996 while blockcain technology was invented in 2008 by 'Satoshi Nakamoto' – an alleged pseudonymous author of a White Paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System.'

[6] Other academic definitions are: 'self-executing electronic instructions drafted in computer code' see Reggie O'shields, 'Smart Contracts: Legal Arguments for Blockchain' (2017) 21 NC. Banking Institute, 177, 179; 'a piece of computer code that is capable of monitoring, executing and enforcing and agreement' see Tom Hingley, 'A Smart New World: Blockchain and Smart Contracts' < https://www.lexology.com/library/detail.aspx?g=3937c417-f5de-4a73-b030-09e1fa5301fd> accessed 20 July 2021; 'Software with which computer codes bind two or a multitude of parties in views of the execution of pre-defined effects and that is stored on a distributed ledger' see Gabriel Jaccard, 'Smart Contracts and the Role of Law' < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885 > accessed 25 July 2021; 'digital contracts allowing terms contingent on decentralized consensus that are self-enforcing and tamperproof through automated execution' See Lin William Cong and Zhiguo He, 'Blockchain Disruption and Smart Contracts' (2019) 32 (5) The Review of Financial Studies, 1754–1797; 'an event-driven program, with state that run a distributed, decentralized shared and replicated ledger (Blockchain) and that can take custody over and transfer assets on the ledger' see Jakub Szczerbowski, 'Place of Smart Contract in Civil Law. A few comments on Form and Interpretation' Proceedings of the 12th Annual International Scientific Conference New Trends, 2017 (Private College of Economic Studies Znojmo, 2017); 'contracts that are represented in code and executed by computer' Eliza Mik, 'Smart Contracts: Terminology, Technical Limitation and Real World Complexity' (2017) 9 (2) Law, Innovation and Technology, 269 - 300; 'automated software agents hosted on blockchains that are capable of autonomously executing transactions on the triggering of certain conditions' See Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct (2018) 29 Law and Critique, 141 - 149. 'Cryptographic boxes that contain value and only unlock if certain conditions are met'. Vitalik Buterin, 'Ethereum White Paper. A Next Generation' Smart Contract and Decentralized Application Platform' (2015) Ethereum White Paper, 1, 13. See generally, Ricardo De Carra, 'The Legal Meaning of smart contracts' (2019) 6 European Review of Private Law 731.

[7] GDPR, art. 3 (1)-(2) on its territorial scope.

Here, I will discuss some of the data protection issues[8] affecting smart contracts as contemplated under the GDPR. [18].

a) Personal autonomy and control.

This is one of the essential bye-products of data protection. It effectively grants data subjects (users) a measure of control over the use and access to their personal information by third parties. [19] The GDPR emphasizes the desirability for natural persons to assume effective control of their personal data by guaranteeing some rights which put the former in pole position to grant or deny access to their personal information, for what purpose and for what period.[9] Smart contracts exclude third party intermediaries by giving parties direct access to their transactional data, in this case personal and non-personal data, with the instrumentation of access control codes managed by peer-to-peer (P2P) network in the absence of any central body. [20] This contractual exclusivity enables the users determine the use and access to their personal data processed as part of the smart contract's functionalities.

Such control is further enhanced by Decentralized Online Social Networks (DOSNs) which are peer-to-peer digital networks that store users' personal data on multiple interconnected service providers thereby decentralizing the storage system and reducing the risk of manipulation or lack of control over personal information that are often stored on users' individual devices but remotely accessible. [17].

b) Anonymized and pseudonymized data

Smart contracts are (now) stored on blockchain technology where every party has a unique identification called 'self-sovereign identity.' [21] Although this identity is controlled by the user, it is stored on the blockchain - a public ledger - hence flagging the issue of identity management and the necessity of anonymity for such users especially from security point-of-view. To cater to this need, the self-sovereignty identity management system used in blockchains puts the users in effective control of their identities and other personal data. Zachary extensively addresses management of identity in smart contracts to contemplate: separate existence of user's identity from the representative codes used on the platform, exclusive control over personal identity, unhindered access which facilitates seamless retrieval of identity from ledger, consistency of identity and identity portability enabling similar use over other platforms etc. [22].

However, it has been argued that, executing smart contracts through blockchain may hamper the anonymity of parties since everyone on the network can access other users' data published on public ledger albeit without ruling out the use of de-identifiers like blind contracts, stealth addresses, embedded metadata etc. [23] Nevertheless, the effective use of identity management systems in blockchains on which smart contracts platforms are run, may guarantee effective anonymity to the satisfaction of users but to the detriment of coverage provided by data protection laws.

The GDPR declares that principles of data protection are not applicable to anonymous data which the regulation defines as 'information which do(es) not relate to an identified or identifiable natural person to personal data rendered anonymous in such manner that the data subject is not or no longer identifiable.'[10] GDPR does not protect anonymous data as far as they concern parties to a smart contract whose identities have been subjected to self-sovereignty identity management process and thereby de-identified. Conversely, although, anonymous data do not qualify as personal data protected by GDPR but for as long as smart contracts are stored on blockchains accessible to all, conversations on parties' anonymity must necessarily extend to inquiries as to whether those data qualify as personal data to bring smart contracts within the ambit of GDPR and whether anonymity in this context equates pseudonymization which has a different legal implication. [24] Rather than anonymized data, information used on blockchains (where smart contracts are stored) are pseudonymized data which still pose privacy and data protection problems since they only reduce the risk of identification as opposed to anonymized data which completely eradicates identification. [25].

c) Unidentifiable data controllers.

One of the main objectives of data protection laws is the apportionment of obligations and liabilities which underpins the identification of every player in the data protection enforcement ecosystem [26] The GDPR expects data controllers to take up a few obligations and bear some responsibilities in certain events[11] but smart contracts are decentralized, not controlled by any central entity outside the parties to the contract and this poses the question on identity of the controller. The GDPR defines a controller as 'the person' who determines the purposes and means of processing of personal data'[12] but in (public) smart contracts, there are no central controlling entities because the processing activities are decentralized via P2P networks, hence there are no 'controllers' within the definition of GDPR per se. Interestingly, Schellenkens theorizes that smart contracts are actually the middlemen in this context. [27] He however conversely argues that where a party offers services through smart contracts, such a party is easily the controller since the party determines the purpose (object of transaction) and means (the smart contract) of processing, however in scenarios where no distinct party offers a service or where such offer is an integral part of the 'code', then it may be difficult to identify the controller. [27].

It is however worthy of note that permissioned[13] smart contracts reveal the identities of the controllers (the central

[8] Other issues not discussed here are: transfer of personal data (GDPR, art. 44); extra-territorial application of GDPR to smart contracts when other parties are outside the EU (art. 4 (1); consent (art. 7 (4); right of access (art. 12-14); data portability (art. 20); privacy by design and default (art. 25 (1) etc.

[9] GDPR, art. 7. and 68.

[10] GDPR, rec. 36

[11] Controllers are duty bound to process data lawfully (GDPR, art 6 (1); comply with data processing principles; prohibited from processing special categories of data with exceptions. GDPR, art. 9 (1); respect data subjects' rights etc.

[12] GDPR, art.4 (7).

[13] In permissioned smart contracts, the 'controller' determines the parties of the contracts and the roles they can play i.e., confirmation of transactions.

entity) unlike public smart contracts which are accessible to the public without requirements for participation. [28].

d) Right to rectification and/or erasure.

Smart contracts are retained on decentralized and immutable digital storage ledgers on blockchains to ensure data provenance[14] for the purpose of perpetuity, transparency, and integrity. [29] Once smart contracts are activated, it becomes practically impossible or difficult for either party to amend or change them and this is occasioned by the manner in which the data sets are registered, confirmed and incorporated into a network. [20].

Conversely, the GDPR guarantees a number of data subject's rights, two of which are right to rectification and right to erasure[15] of data. [30] The former effectively entitles a data subject to request rectification of inaccurate data from a controller while right to erasure empowers data subjects to request absolute deletion of personal data from controller's database but with smart contracts, the exercise and/or enjoyment of these rights become impossible or difficult for three reasons:

First, as discussed earlier, in public smart contracts, since the processing activities are not controlled by a central entity who assumes the position of a controller as defined by the GDPR [16], it becomes practically impossible to request rectification or erasure from an unknown or non-existent controller - which is duty bound to honour the request 'without undue delay.' The decentralized nature of smart contracts makes it impossible to attribute the responsibility of a data controller to any entity, hence the exercise of such right cannot be activated. [31].

Secondly, the decentralized storage on P2P networks also makes complete erasure or wholesome rectification impossible since some data are stored on individual parties' personal devices. [32] Smart contracts do not resort to third parties to store, verify, transmit or communicate data but these activities are performed within the smart contracts' own distributed node especially since every party to a smart contract has a unhindered access to a decentralized and distributed ledger enabling users to write software which are self-executing and immutable across board. The peer-to-peer networking attributes of smart contracts gives the parties equal data processing powers and privileges; hence one cannot necessarily request the other to effect rectification or erasure of inaccurate data. Third, data exchange in smart contracts are inherently immutable and stored as nodes in encrypted form, hence, they cannot rectified or erased at will even where a user qualifies as a controller. Finck notes that, they are often 'append-only ledgers purposefully designed to render the deletion and modification of data extraordinarily burdensome.' [33].

e) Automated decision making.

By the nature of smart contracts, they are designed to run without human intervention on a partial or fully automated functionality. From conception to execution of agreements, smart contracts utilize the data imputed as nodes to consummate the commands without the input of third parties or natural persons. The GDPR addresses automated platforms processing personal data from a risk-management approach to afford a measure of protection for data subjects whose personal information are processed by automated means for the overall mitigation of 'serious risk of circumvention' especially where such platforms make decisions that legally affect the data subjects' rights or liabilities.[17]

Automated decision-making in this context, is a 'decision based solely on automated processing where there is no human involvement.' [34] Generally, the GDPR prohibits data processing by automated decision-making where there are legal consequences, but the regulation makes a number of exceptional situations where such processing is permissible:

First, controllers are mandated to inform[18] and arguably by extension, explain [35] to the data subjects the existence of such automated decision making but since smart contracts are decentralized and not controlled by a third party outside the autonomous parties, the identity of a GDPR-styled controller becomes illusory. Hence, there is no one to make such regulatory proactive disclosure and/or explanation. Secondly, part of the data subject's rights guaranteed by GDPR is the right not to be subject to automated decision-making which produces legal effect on such data subjects, albeit with exceptions.[19] This provision will be activated where: (i) a decision is made (ii) such decision is made on automated platform(s) and (iii) the decision has a legal effect on data subject.

In the case of smart contracts, the question that arises is whether they qualify as decisions to bring them under the ambit of article 26 of the GDPR but so long smart contracts culminate in a product/service or result anticipated by parties, then they qualify as a decision within the context of the GDPR. Nevertheless, smart contracts are not caught by the prohibition of automated decision making under the GDPR [20] where they are necessary for entry into or performance of contract, authorized by law or based on explicit consent. [36].

4. Conclusion

Smart contracts are one of the bye-products of technological innovations in businesses and service delivery. Even though, they have been around since the first century in the mould of vending machines, they continue to emerge and re-invent themselves especially as it concerns seamless data processing activities in what appears a yet-to-be-fully-regulated terrain. In this article, I have examined the various

[14] Data provenance is a historical record of the data and its origins showing which and how data item is stored and accessed and processed by whom and for what purpose.

[15] This also known as the right to be forgotten created by the Court of Justice of European Union (CJEU) in Google Spain's case which culminated in its debut in the GDPR.

[16] GDPR, art. 16 and 17

[17] GDPR, rec. 15.

[18] GDPR, art. 13 (2)(f), 14 (2) (g) and 15 (1) (h).

[19] GDPR, art. 22 (1).

[20] GDPR, art. 22 (2).

definitions of smart contracts from the economic and technological perspectives as well as an analysis of some data protection issues hovering around smart contracts under the GDPR regime in relation to users' rights and controllers' obligations where they are identifiable. Ultimately, from the issues considered in this article, smart contracts must be designed with privacy and data protection in mind right from the inception of the processes involved.

References

[1] Denny Rose and Rowan Allen, *Ancient Civilizations of the World* (Edtech Press, London, 2018) 73.

[2] Fabian Schar, Katrin Schuler and Tobius Wagner, 'Blockchain Vending Machine: A Smart Contract- Based Peer - to -Peer Marketplace for Physical Goods' (2020) MPRA Paper No. 101733, 1.

[3] Eliza Mik, 'Smart Contracts: Terminology, Technical Limitation and Real-World Complexity' (2017) 9 (2) Law, Innovation and Technology, 269-300.

[4] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) < https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html > accessed 25 July 2021.

[5] Stuart Levi and Alex Lipton, 'An Introduction to Smart Contracts and their Protectoral and Inherent Limitation' (2018) Harvard Law School Forum an Cooperate Governance, 1.

[6] Lennart Ante 'Smart Contract on the Blockchain - A Bibliometric Analysis and Review' (2021) 57 Telematic and Informatics, 1.

[7] Jaideep Gosh 'The Blockchain: Opportunities for Research in Information systems and Information Technology' (2009) 22 (4) Journal of Global Information Technology Management, 235-242.

[8] Pierluigi Cuccuru 'Beyond Bitcoin: An Early Overview on Smart Contracts' (2017) 25 (3) International Journal of Law and Information Technology, 179-195.

[9] Alexander Savelyev, 'Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law' (2017) 26 (2) Information and Communication Technology Law, 1.

[10] Zibin Zheng et al 'An Overview on Smart Contracts Challenges, Advances and Platforms' (2019) 105 Future Generation Capital Systems, 475-491.

[11] Philipp Paech, 'Law and Autonomous Systems Serves: What is a Smart Contract?' (2018) https://www.law.ox.ac.uk/business-law-blog/blog/2018/07/law-and-autonomous-systems-series-what-smart-contract accessed 17 July 2021.

[12] Marcelo Corrales et al 'Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework' in Marcelo Corrales, Mark Fenwickand Helena Hapio (eds) *Legal Tech, Smart Contracts and Blockchain* (Springer, 2019) 189- 220.

[13] Maurice Schellekens 'Conceptualizations of the Controller in Permissionless Blockchains' (2020) 11 JIPITEC, 215.

[14] Yongshan Xu et al, 'A Review of Smart Contracts Application in Various Industries: A Procurement Perspective' (2021) Advance inCivil Engineering, 1.

[15] Nguyen Binh Truong, 'GDPR-Compliant Personal Data Management: A Blockchain- Based Solution' (2020) 15 IEEE Transactions on Information Forensics and Security, 1746, 1748.

[16] Christopher Kuner, Lee A. Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary* (OUP, 2020) 2.

[17] Mohsin Ur Rahman, 'Protecting Personal Data using Smart Contracts' in Raffaele Montella, Angelo Ciaramella, Giancarlo Fortino, Dr. Antonio Guerrieri, and Antonio Liotta (eds) *Internet and Distributed Computing Systems* (Springer International Publishing, 2019) 100.

[18] Markus Kaulartz, 'The Tension Between GDPR and the Rise of Blockchain Technologies' (2019) < https://cms.law/en/int/publication/the-tension- between-gdpr-and-the-rise-of-blockchain-technologies> accessed 22 July 2021.

[19] Yvonne McDermott, 'Conceptualizing the Right to Data Protection in EU of Big Data' (2017) Big Data & Society, 1.

[20] Shafaq N. Khan et al, 'Blockchain Smart Contracts: Application, Challenges and Future Trends' (2021) Peer-to-peer Networking and Applications Journal, 1- 25.

[21] Niu Jianlin, 'A Self-Sovereign Identity Management Scheme Using Smart Contracts' (2021) 336 MATEC Web conf., 1-10.

[22] Diebold Zachary, 'Self Sovereign Identity using Smart Contracts on the Ethereum Blockchain' (Masters Thesis, University of Dublin, 2017).

[23] Yogita Borse, 'Anonymity: A Secure Identity Management Using Smart Contracts' (2019) International Conference on Sustainable Computing on Science Technology and Management, 497, 499.

[24] Michele Finck and Frank Pallas, 'They Who Must Not be Identified- Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 (1) IDPL, 11.

[25] Francisco Jose de Haro-Olmo et al,'Blockchain from the Perspective of Privacy and anonymisation: A Systematic Literature Review' (2020) 20 Sensors, 1.

[26] Lee Bygrave and Luca Tosoni, 'Article 4 (7). Controller' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds) *The EU General Data Protection Regulation (GDPR). A Commentary* (OUP, 2020) 148.

[27] Schellekens (n 13) 215.

[28] Lennart Ante, 'Smart Contracts on the Blockchain- A Bibliometric Analysis' (2021) 57 Telematics and Informatics, 1, 5.

[29] Yining Hu et al, 'Blockchain-Based Smart Contracts - Applications and Challenges' (2019) < https://arxiv.org/pdf/1810.04699.pdf> accessed 25 July 2021.

[30] Jef Ausloos, 'Getting Data Subject Right. A Submission to the European Data Protection Board from International Data Rights Academics to Informs Regulatory Guidance' (2020) 10 JIPITEC, 283.

[31] Frantziou, 'Further Development in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, Google Inc. v Agencia Espanola de Proteccion de Datos' (2014) 14 (4) Human Rights Law Review, 761.

[32] Gianluigi Maria Riva, 'What Happens in Blockchains Stays in Blockchain. A Legal Solution to Conflict Between Digital Ledgers and Privacy Rights' (2020) 3 (36) Hypothesis and Theory, 1.

[33] Michelle Finck, *Blockchain and the General Data Protection Regulation*' (European Parliamentary Research, 2019) 1, 72.

[34] Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling'

[35] Sandra Wachter, 'Why A Right to Explanation of Automated Decision-Making Does Not Exist in General Data Protection Regulation' (2017) 0 (0) IDPL, 1.

[36] Lee A. Bygrave,'Minding the Decision v.20: The EU General Data Protection Regulation and Automated Decision-making' in Karen Yeung and Martin Lodge (eds) Algorithm Regulation (OUP, 2019) 246; Michele Finck, 'Smart Contracts as a Form of Solely Automated Processing Under the GDPR' (2019) 9 (2) IDPL, 78.