GDPR, BLOCKCHAIN AND THE FRENCH DATA PROTECTION AUTHORITY: MANY ANSWERS BUT SOME REMAINING QUESTIONS

Sonia Daoui,* Thomas Fleinert-Jensen,** and Marc Lempérière***

ABSTRACT

This Essay aims at highlighting the preliminary guidance issued by the French Data Protection Authority on the interplay between the GDPR and blockchain technology. This Essay also provides a snapshot of the reflection conducted at the European level as of March 2019.

INTRODUCTION

In September 2018, the Commission Nationale de l'Informatique et des Libertés ("CNIL")—the French Data Protection Authority—issued a report about blockchain and the General Data Protection Regulation,[1] also known as the GDPR.[2]

The GDPR is a comprehensive set of data protection rules applicable in the European Union since 25 May 2018. It must be complied with as soon as personal data is processed wholly or partly by automated means[3]; for instance, if it is stored on servers. Personal data encompasses a large spectrum of data. Not only is information which can directly identify a

* Attorney, member of the Paris Bar; Stanford Ignite EEP, Stanford Business School.
** Founding Partner at Almain AARPI, member of the Paris Bar; Blockchain Committee member, French Standardization Association (AFNOR).
*** Partner at Almain AARPI, member of the Paris and New York Bars.

[1] CNIL, BLOCKCHAIN, PREMIERS ELEMENTS D'ANALYSE DE LA CNIL (Sept. 2018), https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

[2] 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

[3] *Id.* at Article 2.

natural person, such as his or her name, considered to be personal data, but also any information which can identify the person indirectly. Personal data includes identification numbers, location data and online identifiers.

The GDPR has widened the territorial scope of European data protection laws. It (1) applies to data processing carried out by data controllers or data processors established within the territory of the EU, whether the data processing actually takes place within the EU; and (2) also covers the processing of personal data of data subjects located on the EU territory by data processors or controllers which have no physical presence within the EU, but are offering goods or services to EU data subjects or are tracking EU data subjects' behaviours, so long as these behaviours happen within the EU.

Blockchains are no exception. As soon as they process personal data, they are subject to the protection rules of the GDPR if one actor of the blockchain has an establishment within the EU, or personal data of data subjects located in the EU is processed by the blockchain.

Blockchains also raise a number of questions with respect to the GDPR. The GDPR has often been presented as independent from technology. The regulation was nonetheless conceived with the classical centralized database in mind, where there is almost always an entity that determines the purpose and means for processing, sets up the systems to do it and processes the data.[4]

Then there are distributed ledgers. With blockchains, the paradigms upon which the GDPR is conceived are altered. When personal data is processed in a blockchain, who is liable for compliance with the data protection rules? How does immutability, which is a core principle in blockchains, work together with the right for any data subject to have his or her personal data modified or erased? These are some of the questions which have been raised in light of the growing interest in blockchains in the past few years. The way such questions will be answered might have a significant impact on the development of blockchains in the EU.

The CNIL report offers a welcomed first analysis of how the GDPR should be applied for blockchains. As might be anticipated, it appears from the report that the main issue concerns the right to personal data erasure. It seems that the other GDPR rules to a large extent can be adapted to permissioned blockchains, and less so to public, permissionless blockchains. But the first question answered by the CNIL concerns accountability: who is liable for blockchain compliance with respect to the GDPR?

[4] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Blockchain and the GDPR* 17 (Oct. 16, 2018), https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

I. Who is Liable under the GDPR?

In GDPR language, answering this question requires a determination of who is the "data controller." The GDPR defines the controller as follows: "Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data..."[5] Based on this definition, the CNIL considers that participants in the blockchain with write permissions who can decide to submit data for validation by nodes are data controllers.

More specifically, the CNIL considers that a participant is a controller: (1) when the participant is an individual who processes personal data for the purposes of a business, i.e. when the processing is not exclusively for personal purposes; (2) when the participant is a legal entity who writes personal data on a blockchain.

For example, the CNIL states that a French *notaire*—a public officer with a monopoly on the sale of real estate—who registers a property deed of a client on a blockchain shall be considered as a controller. Similarly, when a bank registers client data on a blockchain, it shall be considered as a controller.

Validating nodes are not considered data controllers by the CNIL, as they do not determine the purposes and means of the processing of personal data. This position reflects the common view of the blockchain community.[6] According to the CNIL, an individual who purchases or sells bitcoin for his/her own benefit is not a data controller, either. Indeed, the GDPR is not applicable to the processing of personal data by a natural person during a purely personal or household activity.[7]

The CNIL's position is important as the data controller has a central role. As previously suggested, the data controller is the person or entity who is ultimately responsible for compliance of the blockchain with the GDPR rules. According to the GDPR, the controller shall implement appropriate technical and organizational measures to ensure that the data processing is performed in accordance with the data protection rules.[8] In this capacity, the controller shall be liable for the damage caused to any data subject by processing.[9] In addition, the controller faces substantial fines in case of non-compliance, which can reach up to 20 million Euros or 4% of the total worldwide annual turnover of the preceding financial year for undertakings, whichever is higher.[10]

[5] GDPR, *supra* note 2, at Article 4.
[6] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *supra* note 4, at 17.
[7] GDPR, *supra* note 2, at Article 2(2)c.
[8] *Id.* at Article 24.
[9] *Id.* at Article 82.
[10] *Id.* at Article 83.

Independently from the administrative fines, EU member states may also apply other national penalties. In France, for instance, infringement of data protection rules is punished by up to five years in prison and a 300,000 Euros fine for natural persons,[11] although these criminal penalties have, until today, been very rarely applied and never to their full extent. The CNIL's statement will enable data subjects to know who to turn to for the exercising of their rights.

Should all network users oppose consideration as data controllers, the CNIL advises that they agree on who will have this role and carry the associated responsibilities. Alternatively, the users can create a legal entity who will have this role. Once the data controllers of a blockchain are determined, the protective rules of the GDPR can be applied. This raises the main issue of how blockchains can comply with the data subject's right to erasure.

II. The Main Issue—the Right to Erasure

Under the GDPR, the data subject has a right to obtain from the data controller the erasure of personal data concerning him or her.[12] This right exists in particular circumstances, including when the personal data is no longer necessary in relation to the purposes for which it was collected, and when the data subject withdraws consent to process his or her personal data, when consent is the legal basis of the data processing.

On the opposite end, blockchains are based on the immutability principle, according to which information can be added through new blocks but cannot be deleted.

The CNIL acknowledges that it is technically impossible to comply with an erasure request when the personal data is registered on the blockchain. The CNIL, however, considers that there are technical means which come close to erasing the personal data. This is the case when the data is registered on the blockchain by hashing or any state-of-the-art encryption. If, for instance, the private key is deleted, there will be in practice no risk regarding the confidentiality of the personal data.

The CNIL remains cautious: whether such means can be considered as equivalent to a right of erasure still needs to be examined, according to the report. In any case, the CNIL strongly advises not to register personal data directly on the blockchain without encryption. Because of the so-called privacy by design principle,[13] non-protected personal data shall be recorded elsewhere, for instance in the network users' own database, where it can be

[11] Article 226-16 of the French Criminal Code.
[12] *Id.* at Article 17.
[13] *Id.* at Article 25.

erased in compliance with the regulation. The blockchain shall only contain information noting that such data is located in the database.

Similarly, in order to minimize the erasing issue, the participants should stick to one of the cornerstone principles of the GDPR according to which the processing of personal data shall be limited to what is necessary in relation to the purposes for which they are processed.[14] On the basis of this rule, the CNIL guidelines examine how users and nodes are identified in blockchains, which takes place esentially through a public key and a confidential private key. The public identification of the users and nodes can always be seen, as this is a technical requirement for blockchains. According to the CNIL, there are no ways to further minimize such identification.

However, another analysis based on a close reading of article 17 of GDPR could be made of the conciliation of the right to erasure with the blockchain. The right to be forgotten indeed exists only in six precisely defined cases, five of which do not apply to most blockchain operations:

(1) Offers of information society services towards children younger than 16; (2) obligation to delete the data in accordance with the applicable national law; (3) illegal processing of the data; (4) the data subject opposes the data processing which was legally based on the fact that this data processing was necessary to the exercise of a public services mission or to the legitimate interests of the data controller; (5) data processing based on consent.

The processing of data for blockchain services is generally based on the fact that the processing is necessary for the performance of a contract to which the data subject is a party, or to the performance of pre-contractual measures adopted at his/her request. Therefore, the only justification for a request of deletion of the data from a blockchain would arise when the personal data is no longer necessary in view of the purpose for which it was collected.

It could thus be argued that when deciding to participate in the blockchain, the data subject knows that his/her personal data will have to be processed for the duration of the blockchain. This duration is not infinite (French law forbids infinite term contracts), since at some point—in a more distant future than what we usually consider but still at some point—all of the devices wherein part of the blockchain is stored will be physically destroyed, and the data will be deleted.

Therefore, it can be considered that blockchains retain personal data for their duration and that until the last server on which the part of the blockchain is stored is destroyed, the personal data of each member of the blockchain is necessary for the purpose of data processing, and therefore no right to be forgotten applies. This transfers the debate from the right to be

[14] *Id.* at Article 5(1)c.

forgotten to the obligations of information of data subjects, which include information on the duration of the data retention.

In the case of blockchain services, data subjects must indubitably be informed that their data will be retained until the last server on which the blockchain is stored is physically destroyed, but if this information has been provided, it could be argued that the right to erasure does not necessarily apply to data processing for blockchain services purposes. But more generally, all information registered on the blockchain, even encrypted, should be kept to a minimum.

As could be expected, the right of erasure is a challenge for blockchains. The CNIL's report does, however, leave room for further experimentation and for further thought, urging stakeholders to be creative. But as far as the other data protection rules are concerned, they seem to a large extent compliant with blockchains, at least for private, permissioned blockchains.

III. The Other Data Protection Rules

The CNIL addresses several such rules and considers them from a blockchain perspective.

A. Contract with data processors

Data processors are entities which process personal data on behalf of data controllers.[15] In this capacity, they are subject to specific rules under the GDPR.

According to the CNIL, smart contract developers that process personal data on behalf of network users shall be considered as data processors. The CNIL takes the example of a developer who offers to an insurance company a smart contract solution which automatically pays a compensation to insured travellers upon a delayed flight. Such a developer is considered as a data processor by the CNIL.

Validating nodes also can be considered as data processors "in certain cases" according to the CNIL, which is rather unprecise. When running the protocol, validating nodes are considered as instructed by the network users. Consequently, network users will have to enter into an agreement with both smart contract developers and validating nodes. Such agreement between the data controller and the data processor is a requirement of the GDPR.[16]

The contract contains a number of provisions intended to protect personal data processing, including the subject-matter and duration of the

[15] *Id.* at Article 28(1).
[16] *Id.* at Article 28(3).

processing, the nature and purpose of the processing, and the type of personal data. The contract also must stipulate that the processor shall process personal data only on documented instructions from the controller.

From a practical standpoint, entering into such a contract should not be a major issue in most of private, permissioned blockchains. The previously mentioned French notaire taken as an example by the CNIL could enter into an agreement with the validating nodes and the smart contract developers. Entering into an agreement seems much more of an issue for public, permissionless blockchains. When the only requirement for a validating node is to install a piece of software and download a full copy of the blockchain, chances are that no agreement will ever be entered into with the network users.

The CNIL is aware of this practical difficulty. In the guidelines, the CNIL states that this issue is currently under more thorough investigation.

B. Security of processing

Among the duties of the data controller and the data processor under the GDPR, they shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.[17]

The CNIL guidelines address this issue. Blockchains are transparent, decentralised, unfalsifiable and disintermediated. According to the CNIL, these features depend on two factors: the number of participants and validating nodes, on the one hand, and encryption on the other hand. In order for blockchains to comply with the GDPR security requirements, the CNIL has issued several recommendations, including: (1) For permissioned blockchains, assessment of the minimum number of validating nodes in order to avoid coalitions controlling over 50% of the nodes. The right number depends on whether the participants have common or divergent interests; (2) documention of any modifications of the software; (3) the network users' confirmation that the private keys are kept secret and secure.

C. Right of access and right to data portability

The GDPR provides for a right of access for the data subjects, whereby they shall have the right to obtain from the controller information on whether personal data is processed, and—should it be the case—access to such data and various information, including purposes of the processing and the recipients to whom the personal data will be disclosed.[18]

[17] *Id.* at Article 32.
[18] *Id.* at Article 15(1).

The GDPR also allows the data subject to receive his or her personal data in a structured and machine-readable way, as well as the right to transfer such personal data to another controller.[19] The CNIL holds that the right of access and the right to data portability do not raise any particular issues for blockchains.

D. Right to human intervention

Smart contracts are a type of automated processing and are widely used in blockchains. The use of smart contracts is covered by the GDPR which, as an exception to the general rule, allows automated processing if necessary for the performance of a contract between the data subject and the data controller.[20] This is acknowledged by the CNIL but with some safeguards. According to the guidelines,[21] the network user will have to implement the measures which allow the data subject to obtain human intervention in view of challenging the automated decision—even if the smart contract has already been performed—and independently from what is registered on the blockchain.

This approach complies with the GDPR, which provides the data subjects with a right not to be subject to a decision based only on automated processing.[22] The rule is particularly noteworthy with respect to blockchains.

E. Right of information

Under the GDPR, the data controller shall provide detailed information to the data subject at the time where personal data is obtained.[23] The CNIL holds that this right of information does not raise any particular issue for blockchains. The data controller in a blockchain shall consequently provide the data subject with information including:

(1) the identity and the contact details of the data controller; (2) the purposes of the processing for which personal data is intended and the legal basis for such processing; (3) the right to lodge a complaint with a supervisory authority; (4) the existence of automated decision-making.

In practice, this information seems indeed rather straightforward to provide. However, other information requirements seem more difficult to deal with. The GDPR requires that the data controller provide the data subject with information on the period for which the personal data will be

[19] *Id.* at Article 20.
[20] *Id.* at Article 22(2)a.
[21] *See id.* at Article 22(3).
[22] *Id.* at Article 22(1).
[23] *Id.* at Article 13.

stored.[24] As information cannot be deleted on blockchains, this requirement will be difficult to fulfil.

Similarly, the network user has to inform the data subject of its right to request access to and rectification or erasure of personal data.[25] On the blockchain, information cannot be rectified but only modified by adding a new block to the chain—the information cannot be erased. The CNIL does not address how to provide such information to data users.

F. Transfer of data outside of the EU

The CNIL also addresses the issue of participants who are located outside of the EU. Thus raised is the matter of data transfers beyond the EU, to countries where personal data protection might be less stringent.

This question does not concern non-EU countries or territories for which the European Commission has decided that it ensures an adequate level of protection. In such cases, the GDPR allows the transfer of personal data without any specific authorization.[26] It consequently would not raise any concern if some of the blockchain users or nodes are located in such places.

However, only eleven countries benefit from adequacy decisions: US companies subject to the Privacy Shield, Canada, Japan, Isle of Man, Argentina, New-Zealand, Guernsey, Andorra, Faroe Islands, Switzerland, Uruguay. It must be noted that the majority of these countries are very small and that the Privacy Shield, which allows transfers towards US companies which are self-certified under it, is subject to a very serious legal challenge—following the decision by the Irish Commercial High Court to refer to the European Union Court of Justice[27] a question for a preliminary ruling concerning the legality of this adequacy decision.

In the absence of such authorization, adequate protection can be obtained through various means set out by the GDPR, including:

Binding corporate rules[28]: such rules shall be entered by every concerned corporation and specify the data transfers and the application of the general data protection principles, among other points.

Standard data protection clauses adopted by the European Commission.[29]

[24] *Id.* at Article 13(2)a.
[25] *Id.* at Article 13(2)b.
[26] *Id.* at Article 45.1.
[27] The High Court Commercial, The Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, 3 October 2017; 2016 No4809.P.
[28] GDPR, *supra* note 2, at Article 46(2)b and Article 47.
[29] *Id.* at Article 93(2).

An approved code of conduct[30]: such a code may include information regarding fair and transparent processing, the pseudonymisation of personal data and the exercise of the rights of data subjects.

Following Brexit, transfers of data towards the United Kingdom may also be subject to these constraints. The CNIL, however, emphasizes that such protection can be adequate for permissioned blockchains. They are much less easy to implement for public, permissionless blockchains, since it can be difficult for network users to control where nodes are located. The CNIL consequently recommends using permissioned blockchains instead.

In sum, far from rejecting blockchains use cases as non-GDPR compliant, the guidelines of the CNIL can be seen as an attempt to reconcile blockchains and data protection. The CNIL answers some questions but leaves others open.

IV. An Engaged Reflection to Bridge the Gap

Numerous comments on the presumed irreconcilable nature of the GDPR with blockchain (particularly public, permissionless blockchains) have accompanied the entry into force of the GDPR. Conceptually, integrating blockchain's value proposition of decentralization within the centralized model underpinning the GDPR was perceived as an attempt at squaring the circle. In the reflection engaged to overcome the frictions between blockchain and data protection, the CNIL's initial analysis is helpful to reframe the approach towards compatibility between blockchain and the GDPR.

Indeed, the French authority recalls that the GDPR's objective is not to regulate technologies but to consider the use cases by the stakeholders in a context involving personal data.[31] In line with this use case-centered approach, the European Union Blockchain Observatory and Forum makes clear that "there is no such thing as GDPR-oompliant blockchain technology. There are only GDPR-compliant use cases and applications."[32]

Therefore, these issues will certainly need to be settled on a case-by-case basis. However, for the sake of consistency, CNIL recommends cooperation with its European counterparts to propose "a strong and harmonized approach."[33]

[30] *Id.* at Article 40.
[31] CNIL, BLOCKCHAIN ET RGPD QUELLES SOLUTIONS POUR UN USAGE RESPONSABLE EN PRESENCE DE DONNEES PERSONNELLES (Sept. 24, 2018), https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles.
[32] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *supra* note 4, at 16.
[33] CNIL, *supra* note 31.

At the European level, the European Data Protection Supervisor ("EDPS") in its 2018 report[34] reaffirmed the application of the GDPR when blockchain is used to process personal data. Furthermore, EDPS is currently investigating a "number of data protection challenges, relating to areas such as storage limitation, controllership and individual's rights."[35] Thus, a constructive reflection at the European level seems ongoing, though it cannot be confirmed when this expected guidance will become available.

To mitigate this uncertain situation, the European Union Blockchain Observatory and Forum has proposed, in its "Blockchain and the GDPR" report, four rule-of-thumb principles[36] recommending: (1) assessing the actual need for blockchain; (2) avoiding storing personal data on a blockchain and making full use of data obfuscation, encryption, and aggregation techniques to anonymize data; (3) collecting personal data off-chain, or if the blockchain cannot be avoided, on private, permissioned blockchain networks; (4) being as clear and transparent as possible with users.

Though non-binding, these recommendations—further developed in the report—constitute a useful actionable guidance to entrepreneurs.

The intricacies raised by the interplay between the GDPR and blockchain eventually highlight a broader challenge posed to regulators: the design of flexible regulatory responses able to juggle the legal issues raised by the incursion of unprecedented technologies. In this respect, some inspiration might be found across the Channel where the Information Commissioner's Office ("ICO"—the UK data protection authority) is pioneering the creation of a regulatory sandbox on data protection. The ICO regards the sandbox as "a safe space where organizations are supported to develop innovative products and services using personal data in innovative ways."[37]

On September 2018, the ICO launched a consultation on establishing a regulatory sandbox, and the feedback received showed the necessity of including in the sandbox "the use of personal data in emerging and developing technologies like internet of things, automated vehicles, artificial intelligence, blockchain."[38] Then the ICO published in January 2019 a discussion paper on the sandbox beta phase, which explains the ICO's approach for the purpose of the regulatory sandbox and the operating model

[34] Issued on February 26, 2019.
[35] EUROPEAN DATA PROTECTION SUPERVISOR, ANNUAL REPORT 48 (2018), https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf.
[36] THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *supra* note 4, at 28.
[37] INFORMATION COMMISSIONER'S OFFICE, *ICO's call for views on building a sandbox: summary of responses and ICO comment* (September 10, 2018), https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf.
[38] *Id.* at 5.

of this beta phase. The beta phase is designed to include around ten organizations of different types and sizes and seeks to attract "applications for products and services that address specific data protection challenges central to innovation."[39]

Among these challenges, the ICO cites the use of personal data in emerging or developing technology and the perceived limitations or lack of understanding of the General Data Protection Regulation provisions on automated decision-making, machine learning or AI. Blockchain is no longer referenced in the discussion paper, though the ICO mentions that these issues are not exclusive.

However, it is premature to draw conclusions considering the very early stage of the process. Indeed, applications to the beta phase will open around the end of April 2019, and the beta phase will run from July 2019 to September 2020,[40] *i.e.* potentially following Brexit. Therefore GDPR at this date would be applied in the UK as national legislation, and the ICO will have lost its seat at the European Data Protection Board, as well as much of its capacity to influence the other European national data protection authorities.

Although it is certain that participants will not be released from the obligation to comply with the GDPR, the sandbox intends to create the conditions for a close collaboration between innovators and the regulator and the opportunity for adaptations. Therefore, it would be highly beneficial for this regulatory sandbox in data protection to include at least one participant using blockchain technology. Indeed, the GDPR and blockchain share the common objective of empowering data subjects with respect to their personal data,[41] and this regulatory sandbox should be leveraged to explore the practical modalities allowing blockchain GDPR-compliant use cases and applications.

[39] INFORMATION COMMISSIONER'S OFFICE, *Sandbox beta phase discussion paper* 1 (Jan. 30, 2019), https://ico.org.uk/media/about-the-ico/documents/2614219/sandbox-discussion-paper-20190130.pdf.
[40] *Id.* at 6.
[41] Michèle Finck, *Blockchains and Data Protection in the European Union* 7 (Max Planck Institute for Innovation and Competition, Research Paper No 18-01, Nov. 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322.