European Data Protection Regulation and the Blockchain Analysis of the Critical Issues and Possible Solution Proposals

Nicola Fabiano
Studio Legale Fabiano
Rome, Italy
Email: info@fabiano.law

***Abstract*—The blockchain represents an Internet revolution in terms data usage, storage, anonymity, encryption, and so on. The technical evolution of the blockchain also has an impact on the Internet of Things (IoT) phenomena. However, we should take into account the legal issues related to the data protection and privacy law. Technological solutions are welcome, but it is necessary, before developing applications, to consider the risks to the fundamental rights and freedoms which we cannot dismiss. Personal data is a value. It is important to evaluate the European Regulation n. 2016/679, General Data Protection Regulation (GDPR) that applies from May 25th 2018. The GDPR introduces Data Protection by Design and by Default, Data Protection Impact Assessment (DPIA), data breach notification and significant administrative fines in respect of infringements of the Regulation. It is fundamental to evaluate the blockchain and its compliance with the GDPR principles. Regarding the data protection and security risks, there are some issues with potential consequences for data and liability. A correct law analysis allows evaluating risks preventing the wrong use of personal data. The contribution describes the main general principles according to the GDPR and the aspects related to the blockchain.**

Keywords–Data Protection; GDPR; Blockchain.

I. INTRODUCTION

Nowadays, the blockchain is a part of our life. More and more often people use the blockchain, especially in trading with crypto-currencies. We know that the blockchain is a distributed ledger database where encrypted data are stored. Several blockchain applications allow us to define this phenomenon as "blockchain as a service". In this context, it is important to consider the Regulation n. 2016/679 General Data Protection Regulation (GDPR) [4] about the protection of personal data. It is quite clear that the blockchain has been analysed only from a technical point of view, but there is another side to be considered that is the data protection law. In fact, the current blockchain framework considers technical aspects related to each kind of node and to the security measures adopted by avoiding disclosure of information. It is crucial to develop the blockchain infrastructure and set up the structure of the node. However, the developers pay attention to the technical aspects always ignoring the way to design the blockchain following the law obligations especially regarding the protection of personal data. This aspect is becoming increasingly relevant since the application of the GDPR starting from May 25th 2018.

The rest of the paper is structured as follows. In Section II, we describe the current European legislation on the processing of personal data. In Section III, we describe the differences between privacy and data protection. In Section IV, we analyse the blockchain and the relationship among the principles provided by the European Regulation 2016/679, trying to address possible solutions to be compliant with the law.

II. THE EUROPEAN LAW ON THE PROCESSING OF PERSONA DATA

In Europe, the protection of natural persons in relation to the processing of personal data is a fundamental right. In fact, Article 8 of the Charter of Fundamental Rights of the European Union (the Charter) [1] is related to the protection of natural persons in relation to the processing of personal data [4] (Article 8 - Protection of personal data).

Furthermore, the Charter also considers the respect for private and family life [1] (Article 7 - Respect for private and family life) as a crucial aspect of privacy.

Moreover, the Treaty on the Functioning of the European Union (TFEU) [2] considers the right to the protection of personal data (Article 16(1) says: "Everyone has the right to the protection of personal data concerning them").

This is the general legal framework, and the protection of personal data is under the Directive the Directive 95/46/EC [3] until May 25th 2018.

Nevertheless, in 2016, the European Regulation number 679/2016 has been published. It entered into force on May 25th, 2016, but it will be applied starting May 25th, 2018 [4]. According to Article 94, this Regulation will repeal the Directive 95/46/EC [3] with effects from May 25th 2018. Therefore, the Directive 95/46/CE will be applicable until May 25th, 2018.

The GDPR obviously mentions the Charter of Fundamental Rights of the European Union in the first Whereas (*The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her*).

The primary goal is to harmonise the legislation of each Member State: the GDPR will be directly applicable in each European State, avoiding possible confusion among the domestic law. The GDPR introduces numerous changes, such as the Data Protection Impact Assessment (DPIA), the Data Protection by Design and by Default (DPbDbD), the data breach notification, the Data Protection Officer (DPO), the very high administrative fines in respect of infringements of the Regulation, and so on.

 ISBN: 978-1-61208-644-6

Regarding the protection of personal data, apart from the before mentioned GDPR, there is also the Directive 2002/58/EC [5] concerning the processing of personal data and the protection of privacy in the electronic communications. In fact, according to Article 95 of the GDPR, there is a relationship with this Directive (*Article 95 says: "This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC".*).

Directive 2002/58/CE has the aim "*to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community*" (Article 1).

In this legal panorama, it is clear that technology and law are not at the same level because the first one (technology) is always ahead than the second one (law). The actions on the part of the legislator always follow the technological solutions, and so the rules have to be able to consider the technology evolution.

GDPR applies on May 25th 2018, and it is crucial to analyse it to comply with the new data protection Regulation. In fact, GDPR represents an innovative data protection law framework because of several legal purposes on which it is based.

III. Data Protection and Privacy

Often, people erroneously consider "privacy" and "data protection" as synonyms, confusing the real meaning indeed. "Privacy" and "data protection" are not the same because, apart from the terminological definition, they are different concepts. Both are fundamental rights in Europe, but there are differences between them. On one hand privacy is related to the personal life; on the other hand, data protection concerns the personal information.

It is not possible to address data protection and privacy issues adopting only technical solutions without any legal reference. Apart from the highly technical solution, hence, we cannot dismiss the law obligations, where they are applicable, like in Europe, according to the GDPR [4]. In fact, in terms of legal framework, "security" is not equal to "privacy". A system could be very secure but not in compliance with the data protection law. On the contrary, a system could be compliant with the data protection law and, hence, very secure (obviously only by the adoption of security measures).

IV. Blockchain and Data Protection

The IoT evolution realises an ecosystem and inside it there is an emerging phenomenon, basically a technical system, named blockchain [6]. The blockchain was imagined by Satoshi Nakamoto [7] and, probably, it is well-known because it is the technical structure used for the bitcoin (a crypto-currency). The blockchain has been primarily used for the crypto-currencies and it is a shared, immutable ledger for recording the history of transactions; it is a ledger of records. The blockchain can work as a distributed database, and its structure guarantees any modification or alteration due to the strong link and timestamp among each block.

However, apart from the crypto-currencies, the blockchain allowed to develop several applications in different fields (i.e., smart contracts, electronic identity, keeping of digital documents, e-Government, etc.). Hence, any interaction among the several blockchain application is possible. In this context, we can qualify the blockchain phenomenon in terms of "*blockchain as a service*" due to the potential to carry out diverse services. In fact, this development denotes the blockchain evolution from a technical structure under the crypto-currencies to a proper IT infrastructure that can be used to deliver services.

However, a distinction must be made.
Generally, there are:

1) public blockchain
2) private blockchain
3) combined blockchain (consortium blockchain)

Now all the blockchains are based on systems of proof of work or proof of stake. In the public blockchain, everyone can access and make transactions. In the private blockchain, the control is under the power of the organisation. In the combined blockchain, the control is under some nodes.

This scenario is important to privacy and the protection of personal data. In this general context, what about data protection and privacy? Regarding privacy, Satoshi Nakamoto [7] argues that *privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous*. However, the author says also that *The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner*. That represents a significant chink in the data protection and privacy perspective. Ensuring privacy and data protection is one of the main aims of any project which has to addressed by design, not leaving any possibility to compromise personal data and/or personal information. Given the structure of the blockchain, it seems that any subject or person or owner (as defined by Nakamoto) should be a controller and consequently bound to respect the privacy or data protection laws. From a business perspective, probably, personal data or personal information does not receive adequate protection, thinking also to grow the security measures. To set up high-security measures is a good solution but it is not the only one. Each organisation, before designing a project, has to consider the principles provided by the article 25 of the GDPR (data protection by design and by default). According to these principles the controller, before starting the processing of personal data, has to implement appropriate technical and organisational measures. In this way, the controller shall be compliant with the data protection by design and by default". It is wrong to address a compliance process with the privacy or data protection law after the project output because any evaluation must be during the design phase.

The security solution is always used by scientists and technicians to address data protection issues. However, it is crucial to consider the Data Protection obligations provided for by law and especially the GDPR. According to the EU Regulation n. 2016/679 from May 25th 2018 it will be mandatory to respect principles and rules required by the GDPR. Among the several principles provided by the GDPR, some general one do not

 ISBN: 978-1-61208-644-6

seem to be applicable to the blockchain. In fact, according to the article 5, paragraph 1, of the GDPR, there is the need to respect the following principles:

1) lawfulness, fairness and transparency
2) purpose limitation
3) data minimisation
4) accuracy
5) storage limitation
6) integrity and confidentiality

Paragraph 2 of the above mentioned article 5 states: "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)*". The principles mentioned above are so relevant that, in case of infringement, a hard administrative fine up to 10.000.000 EUR shall be applicable, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

Giving that, what about the blockchain?

In fact, in case of private blockchain or probably of the combined blockchain, it is possible to respect the principles as mentioned above, because there will be an identified controller. In case of a public blockchain, instead, it will be impossible to establish who is the controller. The identification of a controller is crucial for the "accountability", according to the article 5, paragraph 2, of the GDPR. The essential identification of the controller is closely related to the six principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality).

How is it possible to respect the principles as mentioned earlier without a controller?

The consequences will be that a public blockchain will not be in compliance with the data protection law (GDPR).

Another point is the respect of the first principle (lawfulness, fairness and transparency) and especially regarding the data subject's consent.

According to the article 6, paragraph 1, of the GDPR "*Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*".

In this scenario, there are some relevant questions, and the answers will be useful to correctly address the legal issues related to the compliance with the data protection law (GDPR).

In fact,

- to whom the data subject gives the consent?
- can the data subject withdraw the consent and how?
- how and to whom the data subject can ask the erasure of personal data or exercise the rights according to the GDPR?
- who are the parties and, mainly, who is the blockchain's representative party that is responsible and considered as a controller?

As mentioned earlier, none of the questions mentioned earlier have answers in compliance with the GDPR. It is not possible to consider every single node of a public blockchain based on a contract. If the data subject withdraws the consent, the node continues existing, and it will not be erased and removed. As there is no controller in the public blockchain, it is impossible for the data subject to address a request to erase personal data; the data subject will not be able to exercise the rights according to the GDPR. A public blockchain, giving its technical structure, is not configurable as a contract among the node's owners.

V. Applying the GDPR to the blockchain and possible solutions

As mentioned earlier, it is quite complicated to apply the GDPR fully to the blockchain because of its technical architecture. We want to highlight some critical issues related to the application of the GDPR to the blockchain and the possible solutions.

1) **The roles.** It is relevant to identify all the roles played in the processing of personal data and especially in the blockchain. In the blockchain, we absolutely must identify the controller and the processor(s), but this is impossible in the public blockchain. Who is the controller in a blockchain?
2) **The Data Protection Officer (DPO).** Moreover, by virtue of its nature, its scope and/or its purposes, the blockchain could imply regular and systematic monitoring of data subjects on a large scale, according to the article 37, paragraph 1 letter b) of the GDPR. In this case, it is mandatory to designate a data protection officer (DPO). However, due to the blockchain architecture and structure, it will not be easy - especially in a public blockchain - to identify the controller and consequently who is the subject obligated to designate a data protection officer. We think that this is criticality of the blockchain structure and it will be impossible to designate a data protection officer. Differently, in a private blockchain, the controller can and indeed must designate a data protection officer according to the GDPR. Designating a data protection officer means that this subject has to take at least the tasks mentioned in the article 39 of the GDPR. It is evident that the blockchain must allow the DPO to make all the tasks to be compliant with the GDPR.
3) **Transferring personal data to third countries.** Another key-point is related to the transfers of personal data to third countries or international organisations. In fact, according to the blockchain architecture, it is impossible to restrict its application to the European member States. According to the article 3, paragraph 2, (Territorial scope) of the GDPR
"*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union".
Hence, for example, if someone based outside the European Union offers goods or services to such

data subject in the Union, he must respect the GDPR rules. In this context, it will be challenging to localise a blockchain (better all the data) only inside the European Union. Consequently, the GDPR will apply to all over the world. The articles from 44 to 50 of the GDPR provide the rules for the transfer of personal data outside Europe. It is quite impossible to localise the data centre(s) where the blockchain data are stored, because of its technical structure and this can be a critical condition for the application of the GDPR rules in this matter.

4) **The liability.** Regarding liability, the article 82 states that "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"*. What kind of right is there to receive compensation in a public blockchain where there is no controller?
5) **Data breach.** According to the article 34 of the GDPR "*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*". In a public blockchain how is the rule applied? We must consider a data breach firstly and understand its causes. Secondary, we must know who is the controller according to the considerations as mentioned above.

Hence, there are a lot of critical issues in the application of the GDPR in the blockchain; in certain cases, it is possible to comply with the GDPR rules using some legal instruments as mentioned above, but, in other cases, it will be impossible. However, although it is difficult to consider a full application of the GDPR to the blockchain, we think that through some legal instruments, it is possible to be compliant with the data protection law. In fact, we can address some issues - where applicable - by policies and contractual solutions. It should be clear that it is not ever possible to use all these legal solutions because it depends on the kind of the blockchain. In a public blockchain, for example, we can use only policies applicable to all the participants (node owners'). Each policy should be issued according to the GDPR rules. In this way, each node owner's will be informed about the processing of personal data and eventually give the consent.

VI. Conclusion

On May 25th 2018, the GDPR starts applying. It is crucial to analyse now the GDPR to be ready and comply with the new data protection Regulation. In fact, the GDPR represents an innovative data protection law framework, because of several purposes on which is based.

As we have shown, in the public blockchain there is no supervisor and each subject working on the blockchain is the owner of his node(s). In this case, indeed, there is no controller because the node's owner cannot be the controller of himself. In this situation, apparently, could seem that the privacy and data protection law is not applicable. However, the node's owner could perform activities in the blockchain potentially harmful to the same blockchain and the other nodes. Therefore, there is the liability for the node's owner for any possible damages. Designing and setting up blockchain means that privacy and security policies should be created privacy and security policies applicable to all the node's owners. This solution could mitigate the lack of the law where it is not possible to apply it to the blockchain system.

In the private blockchain, instead, the privacy and data protection law shall apply to the organization with the consequence that it must respect all the legal obligations, including the information to the data subject, his consent and rights. However, it is highly recommended to set up privacy and security policies.

In the combined blockchain, due to the fact that the control is under some nodes, they could be considered controllers and, hence, they are required to respect the privacy and data protection law.

The adoption - by design - of data protection policies could overcome some critical issues of the blockchain addressing, in this way, the nodal points towards a true path of compliance with the data protection and privacy laws.

References

[1] Charter of Fundamental Rights of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN retrieved: June 2018

[2] The Treaty on the functioning of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN retrieved: June 2018

[3] Directive 95/46/ec of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN retrieved: June 2018

[4] 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) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN retrieved: June 2018

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, 2002 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en retrieved: June 2018

[6] IBM, Understand the fundamentals of IBM Blockchain - https://www.ibm.com/blockchain/what-is-blockchain.html retrieved: June 2018

[7] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system - https://bitcoin.org/bitcoin.pdf retrieved: June 2018

[8] AA.VV.: River Publishers, Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds, 2016

[9] L. Axon, University of Oxford - Privacy-awareness in Blockchain-based PKI (2015) - https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63bretrieved: June 2018

[10] K. Christidis and M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things - http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408 retrieved: June 2018

[11] M. Conoscenti, A. Vetr and J.C. De Martin - Peer to Peer for Privacy and Decentralization in the Internet of Things - In: 39th International Conference on Software Engineering, Buenos Aires (AR), May 20-28, 2017. pp. 1-3 - http://porto.polito.it/2665723/1/peer_to_peer_for_privacy_and_decentralization_in_the_internet_of_things.pdf retrieved: June 2018

[12] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou - Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts (2016) - https://eprint.iacr.org/2015/675.pdf retrieved: June 2018

 ISBN: 978-1-61208-644-6

[13] G. Zyskind, O. Nathan and A. Sandy Pentland - Enigma: Decentralized Computation Platform with Guaranteed Privacy (2015) - https://arxiv.org/pdf/1506.03471.pdf retrieved: June 2018

[14] European Convention on human rights - http://www.echr.coe.int/Documents/Convention_ENG.pdf retrieved: June 2018

[15] Gartner: Gartner Says 6.4 Billion Connected ”Things” Will Be in Use in 2016, Up 30 Percent From 2015 - http://www.gartner.com/newsroom/id/3165317 retrieved: June 2018

[16] Cyberhigiene project - https://www.petrashub.org/portfolio-item/cyberhygiene/ retrieved: June 2018

[17] A. Cavoukian: Springer, Identity in the Information Society. Identity in the Information Society, 2010

 ISBN: 978-1-61208-644-6