Blockchain and Data Protection: the value of personal data

Nicola FABIANO
Studio Legale Fabiano
Rome, 00179, Italy

ABSTRACT

It is a challenge to define the Internet of Things (IoT) due to its technical and conceptual complexity. The IoT system allows you to transfer data on the Internet, including personal data. In this ecosystem there is an emerging phenomenon, basically a technical system, named blockchain. There are public blockchain and private blockchain, but we know that it could also be a combined blockchain (consortium blockchain). Apart from the highly technical solution, hence, we cannot dismiss the legal obligations, where they are applicable, like in Europe, according to the General Data Protection Regulation (GDPR). It is important to highlight the differences between privacy and data protection: they are not the same. We cannot dismiss that personal data is a value and it needs adequate protection. The focal point is to highlight if the privacy and data protection law (especially the GDPR) could be applied to the blockchain considering its technical structure. Consequently, it is important to emphasize that the security measures are not enough to comply with privacy and data protection existing laws. Artificial Intelligence systems may facilitate every single step in the processing of personal data.

Keywords: Blockchain; Data Protection; Privacy; Legal issues; Personal data

1. INTRODUCTION

It is a challenge to define the Internet of Things (IoT) due to its technical and conceptual complexity.
In 2012 the Global Standards Initiative on Internet of Things (IoT-GSI) the Internet of Things (IoT) defined[1] [1] the IoT as ”the infrastructure of the information society.”
In the last few years IoT has evolved from being simply a concept built around communication protocols and devices to a multidisciplinary domain. Consequently, it is an emerging aspect of the Industry 4.0.
The Internet of Things (IoT) considers the “pervasive presence in the environment of a variety of things, which through wireless and wired connections and unique addressing schemes can interact with each other and cooperate with other things to create new applications/services and reach common goals. Devices, Internet technology, and people (via data and semantics) converge to create a complete ecosystem for business innovation, reusability, interoperability, that includes solving the security, privacy and trust implications”. [2]
Our life, hence, is fully affected by the devices linked among them transmitting data over the Internet.

Nowadays, several applications are developed using the Artificial Intelligence and this on one hand can help us and on the other hand may be dangerous for our personal data and sensitive information. Furthermore, we must consider another paradigm well-known as Big Data due to the fast and exponential data growth and data traffic. Big data implies data analysis and data mining procedures but working on big data values[2].
There are several risks and threats, but the main one is probably the risk of profiling. If objects are linked to a person, it will be possible to obtain personal information about that person through the information transmitted over the Internet by each of those objects. The consequences entail, obviously, liability for the data controller and data processor related to each specific situation.
We highlight only two of the several risks, but it is enough to underline the needing of the subject’s consent. The consent is a very important point of the data protection law into force.

2. DATA PROTECTION AND PRIVACY

It is important to highlight the differences between privacy and data protection: they are not the same. But it is one thing privacy, another data protection. People, often, confuse privacy with data protection as if they were synonyms. In fact, privacy is related to the personal life and data protection concerns the personal information.
Giving that, there are certainly data protection and privacy issues addressed only providing 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 [3]. This panorama confirms the equation according to security is different from privacy; a system could be very secure but not compliance with the privacy law. On the contrary, a system could be compliance with the privacy law and, hence, very secure (obviously if it has been adopted the security measures).
However, although this diversity people talk about privacy than data protection, but they are conceptually different.

3. PERSONAL DATA IS A VALUE

Personal data is an absolute value.
In Europe, according to the European Union Charter of Fundamental Rights, privacy and protection of persona data are fundamental rights. In fact, the Article 7 is titled "The right to respect for private and family life " and the Article 8 is titled “Protection of personal data”. We often do not think about the extreme importance of our personal data. Personal data is a value both intrinsic and extrinsic, also in economic terms.

[1] The Internet of Things (IoT) has been defined in Recommendation ITU- T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communica- tion technologies

[2] Is well-known the Four V’s of Big Data: Volume, Velocity, Variety and Veracity (IBM). Considering data as value it is possible extend the approach to 5 V (last V as “value”).

Regarding the intrinsic value of personal data, it is precisely the nature of personal information that attributes it an absolute value because it is related to a natural person. With the term "value", in this case, we intend to affirm a value that distinguishes personal information, personal data. It is therefore a very personal value and closely related to the person. To better understand this concept, it is sufficient to compare a person's life.

What is the life value?

We believe that life is an absolute and inviolable value because it is its very nature that allows us to assert it. This is an ontological element, life is a value. Likewise, personal data refer to highly personal information of a natural person and should be considered an ontologically absolute value. Who could have your personal data, if not just the person concerned? The person is at the center of a system based on social, work, sports, etc. activities. Very often, incorrectly, we consider personal data as unique personal data (name, surname, date of birth, residence, citizenship). However, there are numerous information (study, work, communication, sports and social activities, etc.) that allow you to uniquely identify a subject. Any information so that identifies the person is considered personal. We can freely choose to provide some or all of the personal information to one or more subjects, but we must be aware of this.

We said that personal data is an absolute value, but more recently it has emerged a trend to attribute it, also an economic value. The "monetization" process is particularly accentuated with the services available on the Internet. Very often, we can find free services or software, but it is required to provide personal data as a registration. In fact, the "free" is apparent, since the consideration that it is constituted by the personal data provided.

Unfortunately, In Europe, this phenomenon is subject for standardization because in the proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content of 9/12/2015[3], Article 3, paragraph 1, we read "*This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data*". Several amendments have been tabled for this Directive, currently under consideration by two Committees working on a compromise solution. The European Data Protection Supervisor (EDPS) has delivered the Opinion no. 4/2017 of 14/3/2017[4], arguing - rightly - that the word "counter-performance" should be avoided because In Europe the protection of personal data is a fundamental right[5].

We witness, therefore, a phenomenon connected to the digital market in which people often consider personal data as "counter-performance" for services.

The monetization of personal data, however, is not only related to the digital market and the Internet but unfortunately even to the real exchange of goods or services. The data subject, therefore, must pay close attention to whom he or she provides his / her personal data and to the information about the processing of the personal data. In fact, each data subject must always have the control over his/her personal data.

After this short introduction about IoT and Big Data, there are no doubts that the actual value is "data" especially considering our as a data-flow where data is a value, but a special value that deserves protection.

4. BLOKCHAIN AND DATA PROTECTION

The IoT evolution realize an ecosystem and within which it there is an emerging phenomenon, basically a technical system, named blockchain.

The blockchain was imagined by Satoshi Nakamoto [4] and, probably, it is well-known because is the technical structure used for the bitcoin (a cryptocurrency). The blockchain has been used mainly for the cryptocurrencies and it "is a shared, immutable ledger for recording the history of transactions"[6]; it is a ledger of records. The blockchain can works 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 cryptocurrencies, the blockchain allowed to develop several applications in different fields (f.i., cryptocurrencies, smart contracts, electronic Identity, keeping of digital documents, e-Government). Regarding the e-ID, for instance, the blockchain applications are very important both in the field of immigration and for any situation where there is the needing to verify the subject's identity. Furthermore, the blockchain applications are a good solution for the Public Bodies.

It is quite clear that it is possible to realise any interaction among the several blockchain application.

This scenario allows qualifying the blockchain phenomenon in terms of "*blockchain as a service* " [5], [6] due to the potential to be discharged of the most diverse services. In fact, this development denotes the blockchain evolution from a technical structure under the cryptocurrencies to a right IT infrastructure that can be used to deliver services.

However, a distinction must be drown.

Generally, there are **public blockchain** and **private blockchain**, but we know that it could be also a combined blockchain (**consortium blockchain**).

This scenario is important to privacy and the protection of personal data.

In fact, according to the data protection and privacy law, it should be mainly identified the controller, his obligations and the user's rights.

Now all the blockchain can be 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 organization.

In the **combined blockchain** the control is under some nodes.

In this general context, what about data protection and privacy?

Regarding privacy, Satoshi Nakamoto argues that "privacy can still be maintained by breaking the flow of information in

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015PC0634&from=EN

[4] https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf

[5] From the EDPS Opnion: "There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction".

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

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 address "by design", not leaving any possibility to compromise personal data and/or personal information.

Giving 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.

In 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 organization has to consider also that a project must be privacy or data protection "by design" and hence since the design phase.

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.

5. THE EUROPEAN LAW ON THE PROTECTION OF PERSONAL DATA

In Europe, the protection of natural persons in relation to the processing of personal data is a fundamental right. In fact, the Article 8 of the Charter of Fundamental Rights of the European Union (the 'Charter') [7] is related to the protection of natural persons in relation to the processing of personal data[7].

Furthermore, the Charter considers also the respect for private and family life[8] as a crucial aspect of privacy.

Moreover, the Treaty on the Functioning of the European Union (TFEU) considers the right to the protection of personal data[9].

This is the general legal framework, and the protection of personal data is under the Directive 95/46/EC [8].

Nevertheless, in 2016 has been published the European Regulation number 679/2016 that entered into force on 25 May 2016, but it shall apply from 25 May 2018 [3].

According to the Article 94, this Regulation will repeal the Directive 95/46/EC [8] with effects from 25 May 2018. Therefore, the Directive 95/46/CE will be applicable till 25 May 2018.

The GDPR obviously mentions the Charter of Fundamental Rights of the European Union in the first Whereas[10].

The primary goal of the GDPR is to harmonize the legislation of each Member State; in fact, the Regulation n. 679/2016 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.

Regarding the protection of personal data, apart from the before mentioned GDPR, there is also the Directive 2002/58/EC [9] concerning the processing of personal data and the protection of privacy in the electronic communications. In fact, according to the Article 95 of the GDPR there is a relationship with this Directive[11].

The 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"[12].

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 followed the technological solutions, and so the rules have to be able to consider the technology evolution.

Despite it might seem that it takes a long time to 25 May 2018, it is crucial to analyze now the GDPR to be ready and comply with the new data protection Regulation. In fact, the General Data Protection Regulation (GDPR) represents an innovative data protection law framework, because of several purposes on which is based.

Giving that, in the public blockchain there is not a supervisor and each subject working on the blockchain is the owner of his node(s). In this case, indeed, there is not a 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 be 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 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.

---

[7] Article 8 - Protection of personal data.
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[8] Article 7 - Respect for private and family life. Everyone has the right to respect for his or her private and family life, home and communications.

[9] Article 16(1) says: "Everyone has the right to the protection of personal data concerning them".

[10] 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.

[11] The 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".

[12] Article 1

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

6. CONCLUSIONS

In conclusion, regarding the blockchain, it is important to pay attention to the data protection and privacy risks.

According to the technical structure of the blockchain, all the system has not any controller because of the lack of a central controller (a general "supervisor") who is responsible for all the nodes. Each owner, hence, is a controller for the data processing of his node. In this perspective each owner, apart from the general securities profiles of the blockchain, has to respect the law and he is himself is a data processing controller. Due to the blockchain technical configuration, in the event of a node was compromised, it is possible to amount to a controller's liability and, in this case, there are certainly other consequences for the owner's node.

Regarding the personal data, how to manage data privacy or personal information risks, avoiding the law infringement?

It is possible to develop a Data Protection Management System (DPMS) to address correctly and according to the law the data protection and privacy processes. This solution should be based on a very powerful software engine, a robot software, capable to acquire information, analyze data, learn by himself and finally drive the user to the correct data processing. After each operational process the robot learns and, on the next requests, is able to propose solutions more and closer near to the correct approach for data processing. This is a reference model software strictly related to privacy and data protection that can work according the data protection or privacy law. The automated processes can be easily managed by a DPMS.

Thus, we cannot dismiss that personal data is a value and it needs adequate protection.

9. REFERENCES

[1] International Telecommunication Union, "Overview of the Internet of things," *Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model.*, p. 22, 2012.

[2] F. P. Vermesan Ovidiu, *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*. River Publishers, 2016.

[3] European Union, "Regulation 2016/679 of the European parliament and the Council of the European Union," *Off. J. Eur. Communities*, pp. 1–88, 2016.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.

[5] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," in *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, 2017, pp. 433–436.

[6] L. Horwitz, "Blockchain as a service may be in your future -- like it or not," *TechTarget*, 2016.

[7] EUR-Lex, "CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION," *Official Journal of the European Union*, 2012. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT.

[8] European Parliament, "Directive 95/46/EC," 1995.

[9] European Parliament and the Council of the European Union, "Directive 2002/58/EC," *Off. J. Eur. Communities*, pp. 37–47, 2002.