Internet of Things and Blockchain: legal issues and privacy. The challenge for a privacy standard

Nicola Fabiano
Studio Legale Fabiano
Rome, Italy
Email: n.fabiano@studiolegalefabiano.eu

***Abstract*—The IoT is innovative and important phenomenon prone to several services ad applications, but it should consider the legal issues related to the data protection law.**
However, should be taken 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 which we cannot dismiss. Personal data is a value. In this context is fundamental to evaluate the legal issues and prevent them, adopting in each project the privacy by design approach. Regarding the privacy and security risks, there are some issues with potential consequences for data security and liability. The IoT system allows us to transfer data on the Internet, including personal data. In this context, it is important to consider the new European General Data Protection Regulation (GDPR) - already in force from 24 May 2016 - that will be applicable on 25 May 2018. The GDPR introduces Data Protection Impact Assessment (DPIA), data breach notification and very hard administrative fines in respect of infringements of the Regulation. A correct law analysis allows evaluating risks preventing the wrong use of personal data.
The IoT ecosystem is evolving quickly, developing several applications in different sectors. The main topics for the last time are Big Data and the blockchain. People are paying attention to the latest one because of its potential concrete use for services and applications, increasing the security measures to guarantee a secure system. However, it is equally important to analyse the legal issues related to them. Everyone has the right to the protection of personal data concerning him or her. In this context, we cannot dismiss to guarantee an adequate protection of personal data designing any application. The contribution describes the main legal issues related to privacy and data protection especially regarding the blockchain, focusing on the Privacy by Design approach, according to the GDPR. Furthermore, I resolutely believe that is possible to develop a worldwide privacy standard framework that organisations can use for their data protection activities.

***Keywords*-Internet of Things; Legal issues; Data Protection and privacy Law; Blockchain; Security; Risks; Legal framework; Privacy standard**

I. INTRODUCTION

To define the Internet of Things (IoT) could be a challenge due to its technical and conceptual complexity [1]. Basically, the IoT is a phenomenon founded on a network of objects linked by a tag or microchip that send data to a system that receives it.

In 2012 the Global Standards Initiative on Internet of Things (IoT-GSI) the Internet of Things (IoT) defined the IoT as "the infrastructure of the information society[1]." Not that the IoT phenomenon is realised only when two or more objects are linked to each other in a network such as the Internet. Apart from this kind of connection, an object could also be indirectly linked to a person, thereby setting up a ring network among objects and people. Its very simple, for example, to imagine a ring network that could link a person with one or more objects (a clock, a chair, a lamp, etc.) equipped with a technological system (RFID, near field communication NFC, etc.).
However, the IoT is a virtual reality that reproduces exactly what happens in the real world. Lets imagine that our clock, chair, and lamp all contain chips and are used by a person with special needs. From a medical point of view, it may be very important, for instance, to know how many times he uses the chair. At the same time, it is necessary to help him by automatically turning on the lamp when he sits in the chair. Using chips, it is possible for the objects to communicate among themselves (e.g., the lamp turning on when the chair sends data that the man is sitting down) and at the same time send data over the Internet for, say, medical analysis. The information provided by each object can be aggregated, thereby creating a profile for him. The profile may contain sensitive information about the man, which raises the possibility of his being monitored. This is a very important point for privacy.
This scenario could present a lot of legal issues related to privacy and data protection law. The main goal is to evaluate the impact of the IoT phenomenon on the fundamental rights such as the right to respect for private and family life according to the European Convention on human rights. There are others legals aspects to take into account developing a project on IoT.

April 30, 2017

[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 communication technologies [2].

A. Privacy: Big Data, legal issues and risks in the Internet of Things

Despite its many potential benefits, the Internet of Things poses significant privacy and security risks because of the technologies involved.
According to the Gartner Newsroom [3], 6.4 Billion Connected Things will be in use in 2016, up 30 percent from 2015 and the device online are estimated to reach 20.8 billion by 2020. This represents a scenario to be monitored not only for the big data phenomenon, but also for threats and risks to privacy and security.
A recent study on the threats to our privacy, security and safety, under the 'Cyberhygiene' project, carried out the report (not yet published) named '*Understanding end-user cyber hygiene in the context of the Internet of Things: A Delphi-study with experts*'. This report, in the beginning, says that '*This study aimed to establish expert consensus concerning the 1) key malicious IoT threats, 2) key protective behaviours for users to safeguard themselves in IoT environments, and 3) key risky user behaviours that may undermine cyberhygiene in IoT environments*'. In conclusion, this report says '*There was consensus on the need to consider behaviours across IoT lifecycles. By considering behaviour across each lifecycle, we have been able to identify key behaviours that users need to adopt when using IoT devices. Furthermore, we have been able to identify key threats that can, for example, put users sensitive information at risk and risky behaviours that may lead users to be at risk of a successful attack*'.
No doubt, therefore, that even in the IoT ecosystem there are relevant risks and threats to privacy and it should take appropriate precautions.
On the one hand, we can control devices such as vending machines and stereo speakers with our smartphones, manage devices in our homes (domotics for energy saving, security, comfort, communication) by remote control, and use smartphone apps to book reservations or purchase services. Larger-scale IoT applications might include public security systems or warehouse inventory control systems. It is evident the acceleration of the technological evolution in the last few years and the IoT phenomenon it is not exempt [2]. IoT considers a 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. In the last few years IoT has evolved from being simply a concept built around communication protocols and devices to a multidisciplinary domain where 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.
On the other hand, we have seen the fast and exponential data growth, data traffic and, hence, another paradigm well-known as Big Data. Big data implies data analysis and data mining procedures but working on big data values[3]. Nowadays it is very simple to develop apps that, by accessing to data, can execute data mining activities with every imaginable consequence.

In this context, the main goal is to protect data because of their highest value. Among the main risks we can certainly present the following:

- ***Identification of Personal Information***

The IoT system allows you to transfer data on the Internet, including personal data. The risk is when the object is not linked directly to a person but only indirectly through the use of information that belongs to that person.

- ***Profiling***

There are several risks and threats in the Internet of Things, but the main one is probably the risk of profiling [4], [5]. Profiling can also be an issue with the movement toward smart grids and cities, a phenomenon that is close in nature to the Internet of Things. From a legal perspective, there is the need to consider the privacy issues arising from these initiatives, such as consumer profiling, data loss, data breach, and lack of consent (consent is mandatory by law).

- ***Geolocation***

Geolocation is another risk because nowadays, by our device (first of all the smartphones) it is very simple to find precise details on the location, for instance, digital photos. In fact, each smartphone OS by default alerts the user that an app could use the GPS system and access personal data on the device.

- ***Liability for Data Breaches***

In Europe, there are numerous national and European Community (EC) laws relating to personal data breaches. Hence, the Internet of Things also has effects on liability in cases where the data being collected and transmitted lacks the appropriate security measures.

Another risk is a loss of data during processing. The consequences entail, obviously, liability for the data controller and data processor related to each specific situation. In fact, because the processing of personal data entails risks to the data in question (such as the loss of it), the EU Regulation n. 679/2016 [6] on data protection contains an article requiring data controllers to conduct a data protection impact assessment (DPIA)[4] an evaluation of data processing operations that pose particular risks to data subjects (Article

[2]IoT is a concept and a paradigm with different visions, and multidisciplinary activities

[3]Is well-known the Five Vs of Big Data: Volume, Velocity, Variety, Veracity and Value.

[4]In the rest of the world this is well-known as Privacy Impact Assessment (PIA).

35). This preventive action could avoid or reduce risks for the fundamental rights such as data protection and privacy.

II. The correct approach: privacy is not security

The main focal point to address a correct approach to any evaluation of privacy risks, in general, is to understand the differences between security and privacy. The correct equation is the following one:

$$security \neq privacy \tag{1}$$

where security is different from privacy.

In fact, according to this principle, it is possible to adopt very strong security measures, but this can not mean to respect privacy law neither protect users' privacy. Often this concept is every indication that it is necessary to intervene on the security systems to be compliance with privacy law. Obviously, this is a big misunderstanding and could create confusion on the privacy approach and its consequences.

Adopting security measures is certainly a value, but it is not the correct way to deal with privacy issues.

To address correctly privacy and data protection, it is necessary to start from the privacy by design (or data protection by design and by default) approach as further and better clarified below. Privacy is embedded into design[5]

A. Protecting privacy through the privacy by design approach

In October 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a resolution on Privacy by Design (PbD) [7] that is a landmark and represents a turning point for the future of privacy. Instead of relying on compliance with laws and regulations as the solution to privacy threats, PbD takes the approach of embedding privacy into the design of systems from the very beginning.

The main goal is to draw up two concepts: a) data protection and b) user. Regarding privacy, we have always thought in term of compliance with laws, failing to evaluate the real role of the user (and his or her personal data). To develop an effective data protection and privacy approach, we must start any process with the user the person who has to be protected putting him or her at the centre. This means that during the design process, the organisation always has to be thinking of how it will protect the users privacy. By making the user the starting point in developing any project (or process), we realise a PbD approach.

This methodological approach is based on the following seven foundational principles [8]:

1) **Proactive not reactive; preventative not remedial;**
2) **Privacy as the default setting;**
3) **Privacy embedded into design;**
4) **Full functionality positive-sum, not zero-sum;**
5) **End-to-end security full lifecycle protection;**
6) **Visibility and transparency keep it open;**
7) **Respect for user privacy keep it user-centric.**

We can see why the Privacy by Design approach is so important in the IoT environment. In fact, the Internet of Things should adopt the PbD principles and statements, always placing the user at the centre.

The European Data Protection Supervisor (EDPS) has promoted PbD, touting the concept in its March 2010 Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy [9] as *a key tool for generating individual trust in ICT*. It was not long after this endorsement that the 32nd International Conference of Data Protection and Privacy Commissioners adopted the PbD concept as well.

In Europe, This approach became *"Data Protection by Design and by Default"* (DPbDabD) in the EU Regulation 679/2016. Between "Privacy by Design" (PbD) and "data protection by design and by default" there are differences in term of methodological approach, but the main goal is to highlight how it needs to start from the user in any privacy project. These two expressions represent two different methodological approaches. The EU formulation is more descriptive and not based on a method; also, the by default concept is autonomous, whereas the PbD approach embeds the same concept into by design. Furthermore, the EU Regulation 679/2016 seems to pay a lot of attention to the technical and security aspects instead of the legal concerns, as seen in highlighting of the term security.

Hence, the Internet of Things should adopt the Privacy by Design principles and statements, always placing the user at the centre.

III. The IoT evolution and its applications: a challenge

The IoT phenomenon makes to spring several applications in different sectors (Personal, Home, Vehicles, Enterprise, Industrial Internet) [10]. This is a continuously evolving system, and we see to the development of many application in each sector. In the last few years, it arose the interest (the needing) to guarantee highest security levels both for the Industries and the users.

The fields of Big Data and Blockchain are the main emerging phenomena in the IoT ecosystem, but people paid attention more to the technical and security issues than the privacy ones.

Certainly, the security aspects are relevant to avoid or reduce the risks for data privacy. However, from a privacy point of view, we cannot dismiss the right approach, according to the PbD principles. In the first phase of analysis, any project has to be evaluated also thinking how to protect

[5]A. Cavoukian - Privacy by Design and the Emerging Personal Data Ecosystem - https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-pde.pdf. More clearly *"Privacy, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish"* [6].

privacy data and personal information applying the PbD principles.

In concrete, after the evaluation process, the project has to comply with the law and not after starting it. Once the project starts, it does not need any process of compliance with the law because, according to the PbD principles, the same project has to be already in compliance with the privacy law before starting it. In this case, (during the life cycle of the project) it is not required any evaluation of compliance with the law. In fact, any evaluation it is necessary during the design phase of the project, just for the nature of the approach "by design", applying the PbD principles correctly.

The IoT ecosystem allows developing several applications for different sectors. One of the most important sectors developed in the last few years is defined as "smart"; in fact, we talk about smart city, smart grid, smart car, smart home, etc.

In each of this field are developed applications that consent to interact objects among themselves, transferring information real time.

In the field of smart home, Industries have been developed sensors and applications by which is possible to control several household appliances, deciding they autonomously when it is time to turn on, or turn off and communicating also any operation to the owner. This phenomenon is well-known as domotics. Thinking to the smart grid, it is very interesting to transfer any information from the meter installed in the house to the electric central system. This has its benefits both for the provider and for the users. Another application is the development of the city automation by systems that consent to grow the quality of life for people.

From a technical point of view, these applications have to be developed guaranteeing a very strong security level to avoid any alteration. As the technology developments, so grow the attacks to the systems. However, we cannot dismiss the several threats on these systems. We read about hacker attacks to steal goods or information. In a case, a fridge communicated to the owner any information about it and the food in it. People intercepted the communication, and controlled data flows understanding once the owner went on a holiday because the fridge reduced the number of communication or, instead, it grew them due to the need to intervene for the rotten food. Through the illicit use of these information, it is possible understanding if the house is unoccupied, so giving the path for criminal activities.

From another side, the experts raised the alarm for possible attacks to the public lighting with imaginable consequences [11]. The effort to develop a smart system based - as in this particular case - on the public lighting has its advantages but, at the same time, it necessary to implement strong security measures to prevent any criminal activity. Let's image an attack to the smart grid: devastating consequences!

The IoT concept is wide, and it can also concern critical infrastructure: what about? It is clear that the technological evolution is a value, but at the same time, it is important to prevent any fraud attempt both using strong security measures and privacy solutions.

Recently there are a lot of news on the Internet about the blockchain. The blockchain was "*conceptualised by Satoshi Nakamoto in 2008 and implemented the following year as a core component of the digital currency bitcoin*" [**?**]. The IoT ecosystem registers another important phenomenon that is the blockchain applications.

This is a short scenario about the applications in the IoT ecosystem and the security risks, but what about privacy?

IV. Blockchain, privacy and legal issues: the new challenge

The blockchain "*is a shared, immutable ledger for recording the history of transactions*" [12]; it is a ledger of records. The blockchain was imagined by Satoshi Nakamoto [13]. Blockchain works as a distributed database, and its structure guarantees any modification or alteration due to the strong link and timestamp among each block.

The blockchain is a distributed database, and this technology underlies bitcoin. The blockchain has been the object of technical analysis from people in the IT sector, and so it has attracted the attention of them due to the potential applications. From a technical point of view, would emerge a very secure structure of the blockchain. In fact, due to the technical configuration, it seems founded on a very strong algorithm that should avoid any alteration. In the last few years, we have had several technical contributions that have provided different technical solutions regarding security. The blockchain structure seems very strong and exempt from compromising, but the weak point is the owner of each node. In fact, if the owner makes a mistake he compromises all the chain.

Academics and scientists [14] - [15] - [16] - [17] have developed many theories about the blockchain to demonstrate the absolute security of all the technical structure. One of the main issues is the need of computational power required by the blockchain because it is necessary to discover what is the algorithm on which is based the node and so linking it to the others and so on.

Among the main industries, IBM with Samsung Electronics have developed the ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) project and according to the document [18] titled "*Empowering the edge - Practical insights on a decentralized Internet of Things*", we read "*The primary objective of the ADEPT PoC was to establish a foundation on which to demonstrate several capabilities that are fundamental to building a decentralized IoT. Though many commercial systems in the future will exist as hybrid centralized-decentralized models, ADEPT demonstrates a fully distributed proof*". Hence, it is evident that we are

witnessing to the IoT evolution from a network of the object to a blockchain-based IoT.

In the before-mentioned document [18] we read

> "*Every blockchain participant can maintain its own copy of the ledger, although the amount of data stored will vary based on capability, need and preference. Every block on the ledger contains a hash of the previous block. This enables blocks to be traced back even to the first (genesis) block. It is computationally prohibitively difficult and impractical to modify a block once it is created, especially as the chain of subsequent blocks get generated. Blocks in shorter chains are automatically invalidated by virtue of there being a longer chain all participants adopt the longest available chain*".

This approach completes the scenario on the technical structure of the blockchain that is revealed a very strong system. However, the blockchain, still now, is designed to the financial services and/or transaction. We cannot forget that the blockchain is always sustained by the bitcoin and in the successive phases it has been implemented but thinking to a currency system. Now the blockchain implementation (such as Ethereum - https://ethereum.org/) is being developed about contracts.

However, the term "contracts" is related to one (or more) financial transaction(s) and not specifically to a legal agreement. This confirms how developing is much closer to the technology than the law and the legal world in general.

Giving that, it is clear what can be a legal approach to these phenomena. In this panorama, you can imagine technology and law as two different trains, but the first one (technology) is always much faster than the second one (law). A system development requires the technical intervention and almost never the legal support. People who deal with the law (lawyers, judges, notaries, consultants, professionals, etc.) have to analyse and verify how the law can be correctly applied to a particular case, but, almost always, after its complete development. It should be appropriate - in certain cases - to involve a legal to define previously such a compliance evaluation with the law.

A. Blockchain, privacy and data protection

Getting back to the blockchain, one of the legal issues is represented by the privacy law.

Regarding privacy, Satoshi Nakamoto [13] 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*". This represents a big chink in the 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.

Axon [17] argues that privacy issues can be dealt with "privacy-awareness" enabling "*two levels of anonymity: total anonymity, and anonymity to the neighbour group level*". However, "privacy-awareness" do not seem a valid solution because this way it is not enough to be compliance with the EU GDPR, according to the Article 25 (Data protection by design and by default).

In another technical contribution [23] you read "*Maintaining privacy on the blockchain is a complicated issue*". The authors propose "*A couple of ways to mitigate - but not completely eliminate - this issue, if privacy is important for the considered application*". Privacy is certainly important on the blockchain and for this reason it would be better to address the issue finding a "legal" solution to be compliance with the law.

Other authors [16] say:

> "*Despite the benefits provided by these services, critical privacy issues may arise. That is because the connected devices (the things) spread sensitive personal data and reveal behaviours and preferences of their owners. People's privacy is particularly at risk when such sensitive data are managed by centralized companies, which can make an illegitimate use of them ...*".

It is very appreciable these authors' approach [16] because they propose a technical solution is presenting it in terms of "private-by-design IoT". In fact, you read

> "*With the purpose of preventing this situation, the goal of our research is to encourage a decentralised and private-by-design IoT, where privacy is guaranteed by the technical design of the systems. We believe that this can be achieved by adopting Peer-to-Peer (P2P) systems.*"

Despite this proposed solution highlights the concept "by design", from a legal point of view it does not seem to take on the issue related to the obligation required by the EU GDPR.

This short scenario shows how on the blockchain there are certainly privacy issues addressed only providing technical solutions, without any legal reference. Apart from the strong technical solution, hence, we cannot dismiss the law obligations, where they are applicable, like in Europe, according to the above-mentioned GDPR. 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).

Apart from some contribution in which privacy is mentioned, the blockchain has been evaluated almost exclusively in technical terms. Often privacy and data protection are

considered synonymous, but obviously, there are significant differences between them. This is not the appropriate place to present the differences between privacy and data protection, but it is very important to underline that they are different about nature and the approach.

Furthermore, where developers and technicians argue about privacy, they probably refer to the need to consider strictly confidential any information and do not disclosure any of it. This is certainly a focal point, but we cannot dismiss that in Europe exists the right to the protection of personal data and it is a fundamental right (Article 8 of the EU Charter of Fundamental Rights [19]).

The compliance process cannot dismiss the EU Regulation n. 679/2016 (GDPR - General Data Protection Regulation) [6] that - already in force - will be applied from 25 May 2018. It is necessary to highlights that a correct analysis approach in terms of Privacy by Design or Data Protection by Design and by Default excludes any compliance with the law because this evaluation has to be made during the design phase. Privacy, hence, has to be considered as the main topic in each project.

Furthermore, in the design phase, it is necessary the following premise: due to the structure of the blockchain, it has to be verified if it the privacy law could be applicable. In fact, the blockchain - due to its nature and structure - is based on trust and democracy principles. There is not a general supervisor or "data controller". The blockchain works on complex algorithms that require a computational power for the mining activities to discover in the header such a change of the hash code SHA256. After this complex process, the node status changes, allowing other transactions. Giving that, the blockchain represents a computational operation apparently without any natural person involved in it. There are certainly several automatic operations execute by the software, but the blockchain cannot work without any input by a natural person. More deeply, the node's owner - a natural person - decides what kind of transaction he/she wants to execute.

This excludes, hence, that the blockchain can be considered as a totally automated process in the creation nodes phases.

After this introductory statement, it is clear that:

1) *the blockchain is a distributed database;*
2) *the blockchain adopts encryption and other strong security measures;*
3) *the blockchain contains personal information or data;*
4) *people do not know where data are stored because of the distributed database;*
5) *people do not know who manage their data;*

It is true that the blockchain is based on a software platform and works processing data, but at the same time, it processes personal data, just input by the owner's node.

The Article 1, paragraph 1, of the GDPR, says "*This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*".

Moreover, the Article 2, paragraph 2, letter (c) of the GDPR says "*This Regulation does not apply to the processing of personal data: . . . (c) by a natural person in the course of a purely personal or household activity*".

Furthermore, by a prior analysis, on the one hand, it can assume that there is no doubt about the fact that the blockchain realises a processing of personal data wholly by automated means. On the other hand, the analysis has to evaluate if, in the blockchain, the processing of personal data by a natural person does not appear in in the course of a purely personal or household activity. If both of these conditions will be realised, the GDPR will be applicable. However, it might happen that - instead - the processing of personal data is in the course of a purely personal or household activity. In this case, despite the processing of personal data is wholly by automated means, the GDPR will be not applicable.

If the case will be under the GDPR, it requires the data subject's consent. In fact, according to the Article 6 (Lawfulness of processing), par. 1, letter (a), 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*".

Moreover, the Article 7 (Conditions for consent), paragraph 3 of the GDPR, says "*Prior to giving consent, the data subject shall be informed thereof*".

In the blockchain scenario, who informs the data subject?

Is there any information on the blockchain platform?

Could be the data subject considered informed by himself/herself?

This hypothesis arises a lot of legal consequences and, among them, certainly that the node owner's can be considered as "controller", and consequently he/she has obligations and liabilities according to the GDPR. Therefore, due to the structure of the blockchain, about privacy, the owner of each node should be considered as "controller" of the processing of personal data according to the GDPR.

According to the Article 25 of the GDPR, as following mentioned, "*the controller shall . . . implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation . . .*".

On the one side, applying these principles, it is mandatory to take into account not only the technical but also the organisational measures. The development of the blockchain, hence, it has to consider also the organisational aspect.

On the other side, among the measures indicated in the aforementioned Article, there are the pseudonymisation

and the minimisation techniques that can be used in the blockchain. These measures should be considered samples and not mandatory. In fact, regarding the pseudonymisation, it seems in contrast to the purpose of the blockchain in certain cases. For the same thing also the minimisation could be not compliance with the blockchain nature and structure. This panorama demonstrates as it is necessary to adapt the data protection by design and by default to the system or the technical infrastructure, trying, in any case, to minimise the risks.

Regarding the structure of the blockchain as distributed database, this could pose the issues on the location where data are stored. According to the blockchain nature, due to its distributed database, data could be stored everywhere in the world. This implies some important consequences regarding the localisation and the application of the law. The data subject's rights could be compromised in case of - for example - his/her data are stored in a Country outside Europe where it is considered "third country".

Therefore, after this short analysis, about privacy and data protection, it is quite clear that in particular cases regarding the blockchain GDPR has to be applied.

B. Blockchain and electronic identification (eID)

Anyway, there are certainly others legal issues related to the blockchain and, among them, we can mention contracts and electronic identity (eID). One of the main important issues is the electronic identification of the user. The EU Regulation No 910/2014 [20] of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC defines (Article 3) the electronic identification as follows "*means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person*".

According to the before-mentioned EU Regulation (No 910/2014), it is possible to suppose the development of the blockchain for any application that guarantees the electronic identification of each node owner's. The blockchain has been developed to guarantee anonymity, but in certain cases or processes, there is the need to identify a person. For example, in a process related to a financial service, there might be the need to identify a person several times. In fact, in a financial service often are involved different operators and stakeholders. Each person has to be identified step by step from different stakeholders. Despite the certainty to have identified a person, however, this is a waste of time and resources.

Due to the blockchain very secure structure, it is possible to realise an identification system, based on the same blockchain structure and (maybe) on a Certification Authority, that guarantees the certainty of each person's identity once a time for all the steps.

In this way, it is sufficient that the person has been identified once a time in the process to guarantee his/her identity to all the stakeholder and operators. In a complex process or inside a framework, there is not the need to establish their identity several times if already there is at least once the certainty about the person's identity. It is possible to realise a secure electronic identity database - better, a secure electronic identity distributed database - that will be based on the strong security measures of the blockchain.

According to the EU above Regulation No 910/2014, we hope that legislators can adopt a law in the domestic law on the authorised use of the electronic identification based on a blockchain application. This will contribute developing the market, preserving the certainty on the person identity, the data protection and privacy, and - at the same time - realising a secure database, guaranteeing the access to the authorised subjects for the authorised uses.

V. Conclusion

The Internet of Things involves all stakeholders from companies to consumers. Focusing on the user (consumer) is particularly important to guarantee a level of confidentiality that will earn the user's trust. This is made possible by adopting the maximum level of security through the Privacy by Design (PbD or DPbDabD) approach and performing PIAs to evaluate the privacy risks of data collection and processing.

The industry may be wary of efforts to regulate the Internet of Things, as it regards the IoT phenomenon as a source of enormous business opportunities. For example, changes in lifestyle - such as the use of more technological services like domotics applications - can certainly increase the consumer's quality of life (and industry's profits). It will be up to consumers, regulators, and privacy professionals to convince the business sector that understanding the risks related to the IoT will produce the same business opportunities to protect privacy and increase the quality of life.

It is very important to set up a privacy standard to facilitate a methodological approach to privacy and data protection.

From a legal point of view, the main difficulty in setting up and using a privacy standard relates to existing laws, which are different in each nation (and even in different states and provinces within those nations). It is possible to develop a standard privacy framework that organisations can use for their data protection activities. This standard framework may be adapted to national legislation while keeping the main framework for all nation-states.

Since the Privacy by Design (or DPbDabD) approach is the foundational methodological approach to privacy protection, the privacy standard should be adopted according to PbD principles and statements.

A Privacy Management System (PMS) could be a reference model or a software system working on the PbD

principles. To develop a PMS confers a benefit to all the stakeholders because in this way it is possible to automate every process guaranteeing a good data protection level, by reducing the privacy and security risks. Furthermore, it is possible to use the Artificial Intelligence and Machine Learning principles to develop a software based on a PMS to facilitate professionals, public body, Industries and Organizations in their activities.

By this approach is conceivable a blockchain closer to the practical and professional needs.

REFERENCES

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

[2] ITU - Global Standards Initiative on Internet of Things (IoT-GSI): The Internet of Things (IoT) - http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[3] 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

[4] Ann Cavoukian: Springer, Identity in the Information Society. Identity in the Information Society, 2010

[5] Mireille Hildebrandt: FIDIS. Behavioural Biometric Profiling and Transparency Enhancing Tools, 2009

[6] 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

[7] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem - https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

[8] 7 Foundational Principles. "Privacy by Design" - https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[9] EDPS: Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy. European Data Protection Supervisor (EDPS) - https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_en.pdf

[10] What's The Big Data? - Internet of Things Market Landscape - https://whatsthebigdata.com/2016/08/03/internet-of-things-market-landscape/

[11] Why Light Bulbs May Be the Next Hacker Target - https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0

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

[13] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system - https://bitcoin.org/bitcoin.pdf

[14] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou - Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts (2016) - https://eprint.iacr.org/2015/675.pdf

[15] Guy Zyskind, Oz Nathan, Alex Sandy Pentland - Enigma: Decentralized Computation Platform with Guaranteed Privacy (2015) - https://arxiv.org/pdf/1506.03471.pdf

[16] Conoscenti Marco, Vetr Antonio; De Martin Juan Carlos - 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

[17] Louise Axon, University of Oxford - Privacy-awareness in Blockchain-based PKI (2015) - https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b

[18] Empowering the edge - Practical insights on a decentralized Internet of Things - https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

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

[20] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[21] Hahn Jim: The Internet of Things (IoT) and Libraries - Library Technology Reports; Chicago 53.1 (Jan 2017): 5-8,2.

[22] Cisco.com. San Francisco, California: Lopez Research, An Introduction to the Internet of Things (IoT), November 2013. Retrieved 23 October 2016 http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf

[23] Konstantinos Christidis and Michael Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things - http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408

[24] Castelluccia, Claude et al.: Privacy, Accountability and Trust - Challenges and Opportunities - https://www.enisa.europa.eu/publications/pat-study

[25] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en

[26] Ann Cavoukian, Jules Polonetsky, Christopher Wolf: Identity in the Information Society, Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation.