The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global 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 and 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 it 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 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) that will be in force 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 contribution describes the main legal issues related to privacy and data protection focusing on the Privacy by Design approach, according to the GDPR. Furthermore, I resolutely believe that is possible to develop a global privacy standard framework that organisations can use for their data protection activities.**

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

I. INTRODUCTION

To define the Internet of Things (IoT) could be a challenge [1] due to its technical and conceptual complexity [2]. 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.

The IoT includes every connection among objects, so we have machine-to-machine (M2M) systems, where each machine talks with other machine(s), communicating real-time data and information. Nowadays we are faced with several devices but mainly such as smartphones and apps, sensors, chip, and any other electronic system. We read [3]

> *The concept was simple but powerful. If all objects in daily life were equipped with identifiers and wireless connectivity, these objects could communicate with each other and be managed by computers.*

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 crucial, 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 [4]. There are others legal aspects to take into account developing a project on IoT.

[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 [5].

978-1-5386-2064-9/17/$31.00

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 high-security measures, but this can not mean to respect privacy law either 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 privacy and data protection correctly, 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[2]. More clearly *"Privacy, having been embedded into the system before the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish"* [3].

III. Protecting privacy through the privacy by design approach

The Internet of Things represents a global revolution: the objects that people use in the real world can talk to other objects and at the same time to the data subjects themselves. This scenario can also be viewed as the Internet of People (IoP) because of the connection among people. This consciousness is the real engine that has pressed politicians and regulators to intervene in the IoT realm. In fact, there is a growing desire to create a general, comprehensive, and structured legal framework for the Internet of Things to protect users and consumers.

In October 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a resolution on Privacy by Design (PbD) [6] 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 primary 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 adequate 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. That 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 [7]:

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 [8] 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 [9] and indeed establishing this concept in the law is a welcome development. Nevertheless, it is kind of interesting to notice that the EU legislator used a different expression (i.e., data protection by design and by default) from the one adopted in the international context (i.e., Privacy by Design). These two expressions represent two different methodological approaches. Privacy by Design is structured in a trilogy of applications (information technology, accountable business practices, physical design) and the seven principles quoted above. 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. According to the text of Article 25 of the Regulation 679/2016, it is clear that the EU legislator considers by design and by default as different concepts, even though the words by design comprehend the concept by default, making the latter phrase redundant. 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

[2] A. Cavoukian - Privacy by Design and the Emerging Personal Data Ecosystem - https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-pde.pdf

[3] A. Cavoukian, cit.

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.

IV. 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 leading 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 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 assessment it is necessary during the design phase of the project, just for the nature of the approach "by design", applying the PbD principles correctly.

Several IoT applications have been developed in the field named "smart", such as smart grid, smart city, smart home, smart car, etc. This indeed represents what is the IoT evolution that it will continue to grow and develop creating a lot of fields of action. In the "smart context," we cannot dismiss from the privacy and security risks related to the communication among objects especially in the case of processing personal data.

The main questions are:

- "Where are the users' personal data stored?"
- "Who manage the users' personal data?"
- "What kind of security measures has been adopted?"
- "Can it be considered a smart system compliance with the privacy law?"

The answers depend on the design model used during the developing preliminary phase. In fact, the "design" is a fundamental topic as we illustrate in the following considerations.

However, in the IoT echo-system are emerging two relevant and complex aspects in part closely related between them: **Big Data** and **Blockchain**. In the last few years, these have been items of interest in the IoT phenomenon, intensifying the interest by whom deals with it, especially because of the implications both from the side of the developers and from the users. Hence, Big Data and Blockchain represent the new challenge and the new applications of the IoT phenomenon.

This scenario entails the need to deepen these aspects, especially regarding the privacy and data protection issues.

A. Big Data: privacy issues and risks in the Internet of Things

Despite its many potential benefits, the Internet of Things poses important privacy and security risks because of the technologies involved.

According to the Gartner Newsroom [11], 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 [12], 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*"[4]. 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 important 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

[4]See also "Review of Cyber Hygiene practices" - ENISA - https://www.enisa.europa.eu/publications/cyber-hygiene

the acceleration of the technological evolution in the last few years and the IoT phenomenon it is not exempt[5]. 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. In the last few years IoT has evolved from being simply a concept built around communication protocols and devices to a multidisciplinary domain. 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[6]. Big data implies data analysis and data mining procedures but working on big data values[7]. Nowadays it is very simple to develop apps that, by accessing to data, can execute data mining activities with every possible consequence. In this context, the primary goal is to protect data because of their highest value. Among the main risks we can indeed present the following:

- ***Identification of Personal Information***

The IoT system allows you to transfer data on the Internet, including personal data. Personal information may be transmitted only when the object in which the microchip installed is linked to a person. This connection may be direct or indirect.

We could have a direct link when the user is aware of the possible transmission of his or her personal data and gives consent. Alternatively, let us suppose that a person buys something. Alternatively, the connection may be indirect when the object is not linked directly to a person but only indirectly through the use of information that belongs to that person. For example, if we have x objects linked together by the Internet, I might know information about object nr. 1, but I cannot know to whom this information belongs. I can know, however, that objects nr. 2, 3, and so on are connected among themselves and to a person named Jane. In this way, it is possible to link every piece of information provided by the objects (2, 3, etc.) to Jane. Furthermore, if I know that it is possible to link object nr. 1 to the others (2, 3, etc.), I can also indirectly know that the information provided by object nr. 1 likewise belongs to Jane.

- ***Profiling***

There are several risks and threats in the Internet of Things, but the main one is probably profiling [13], [14]. 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. Furthermore, these transmitted data may be stored in one or more servers. When a person can be identified through the use of credit or loyalty cards, its very simple to know the types of products purchased and so on to profile the person, learning about his or her habits and lifestyle. The person may have previously provided consent for the dissemination of data related to his or her purchases for advertising purposes. Regarding privacy, is it possible to protect a person? Who manages the personal data? Where will this data be stored?

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. For some years now, there has been an interest in modernising the existing electrical grid by introducing smart meters, which can communicate a consumers energy consumption data to the relevant utilities for monitoring and billing purposes. 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. Inside each picture file there are some fields among them EXIF and GPS that contain the technical information about the photo and also the location where the picture was taken. If the user has not previously deactivated the geolocation service in the camera or smartphone, and the pictures have been published on a website or social network, anyone who views the photo can know exactly where the picture was taken and see who was there.

In this way, privacy could be compromised. When smartphones and other mobile devices are connected to the Internet, as they typically are, they contribute every day to the Internet of things, sending data ready to be used by other people.

- ***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. For example, Directive 2002/58/EC [15] states that: *In case of a particular risk of*

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

[6]Big data is a term for datasets that are so large or complex that traditional data processing applications are inadequate to deal with them. Challenges include analysis, capture, data curation, search, sharing, storage, transfer, visualisation, querying, updating and information privacy. The term "big data" often refers only to the use of predictive analytics, user behaviour analytics, or certain other advanced data analytics methods that extract value from data, and seldom to a particular size of data set. "*There is little doubt that the quantities of data now available are indeed large, but thats not the most relevant characteristic of this new data ecosystem.*" (Wikipedia)

[7]Is well-known the Four Vs 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).

a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Another risk is the loss of data during processing. The consequences entail, of course, liability for the data controller and data processor related to each particular situation. In fact, because the processing of personal data involves risks to the data in question (such as the loss of it), the EU Regulation n. 679/2016 on data protection contains an article requiring data controllers to conduct a data protection impact assessment (DPIA)[8] an evaluation of data processing operations that pose particular risks to data subjects.

According to the Article 35, paragraph 1, of the EU Regulation n. 976/2016 (GDPR) *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks"*.
This is the law prescription on the need to conduct a data protection impact assessment (DPIA) in some cases. This preventive action could avoid or reduce risks for the fundamental rights such as data protection and privacy. This demonstrates as is crucial to pay attention to security and privacy in any project development.

B. Blockchain: what about privacy?

The blockchain "*is a shared, immutable ledger for recording the history of transactions*" [16]; it is a ledger of records. The blockchain was imagined by Satoshi Nakamoto [17]. Blockchain works as a distributed database, and its structure guarantees any modification or alteration due to the strong link and timestamp among each block.

Regarding privacy, Satoshi Nakamoto [17] 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 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.

Axon [18] 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 [19] 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 [20] say "*Despite the benets 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. Peoples privacy is particularly at risk when such sensitive data are managed by centralised companies, which can make an illegitimate use of them ...*". It is very appreciable these authors' approach [20] because they propose a technical solution presenting it in terms of "private-by-design IoT" [9]. Despite the fact that 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 high technical solution, hence, we cannot dismiss the law obligations, where they are applicable, like in Europe, according to the GDPR mentioned above. 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).

This is an obligation for the controller. 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 EU GDPR. From this scenario arise many consequences for the "owner" regarding law obligations.

In fact, according to the GDPR, it is mandatory to "implement appropriate technical and organisational measures"

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

[9] You read "With the purpose of preventing this situation, the goal of our research is to encourage a decentralized 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."

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.

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 users trust. This solution 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 industries 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 consumers quality of life (and industrys 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.

As I hope I have shown, it is crucial to set up a privacy standard to facilitate a methodological approach to privacy and data protection. With the Internet of Things reaching ever more deeply into peoples lives, it would be beneficial to have an international privacy standard for processing personal data in the same way throughout the world using the forward-looking PbD (or DPbDabD) approach.

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, adapting it to national legislation while keeping the central 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. At the moment we have no record of international privacy standard model.

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 feasible 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.

[10] Article 25, par. 1, says "*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*".

References

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

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

[3] 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

[4] European Convention on human rights - http://www.echr.coe.int/Documents/Convention_ENG.pdf

[5] 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

[6] 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

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

[8] 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

[9] 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

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

[11] 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

[12] Cyberhigiene project - https://www.petrashub.org/portfolio-item/cyberhygiene/

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

[14] Mireille Hildebrandt: FIDIS. Behavioural Biometric Pro ling and Transparency Enhancing Tools, 2009

[15] 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

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

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

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

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

[20] 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

[21] 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

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

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

[24] 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.