Athens Journal of Law - Volume 3, Issue 3 – Pages 201-214

Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation

By Nicola Fabiano[*]

The Internet of Things (IoT) phenomenon needs to consider the legal issues related to the dataprotection law. The IoT is not exempted from privacy and security risks because of the use of technologies that often cannot guarantee an acceptable security level. In the IoT, the main risk for privacy is the profiling that allows identifying natural persons through their personal information. However, regarding the privacy and security risks, there are some issues with potential consequences for data security and liability. The IoT system allows transferring data, including personal data, on the Internet. The IoT ecosystem is evolving and companies are developing applications to provide services based on the blockchain. It is important to evaluate the technical structure of the blockchain to analyse the law impact and the legal issues on data protection and privacy. In this context, it is necessary to consider the new European General Data Protection Regulation (GDPR) that will apply from 25 May 2018. The GDPR introduces Data Protection Impact Assessment (DPIA), data breach notification and very high administrative fines in respect of infringements of the Regulation. A correct law analysis allows to evaluate the risks and to prevent a wrong use of personal data and information.

Keywords: *Internet of Things; Security; Privacy; Data protection; GDPR*

Introduction

Defining the Internet of Things (IoT) can be a challenge because of its technical and conceptual complexity[1]. Basically, the IoT is a phenomenon founded on a network of objects, linked by a tag or a microchip, that send data to a receiving system.

The IoT includes every connection among objects; therefore we have machine-to-machine (M2M) systems communicating real-time data and information.[2]

The Internet is one of the main resources of this century and it is certainly very valuable for people.

The IoT is a virtual reality that can reproduce what happens in the real world. There are many advantages due to the connection among objects

[*] Independent researcher and partner at Studio Legale Fabiano, Rome, Italy.

[1] Cavoukian (2011).

[2]Wikipedia describes IoT as "*the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society."*

https://doi.org/10.30958/ajl.3-3-2 doi=10.30958/ajl.3-3-2

especially in sectors in which the technology can help or support people. As for supporting people with special needs, it may be important, for instance, to know how it happens to evaluate specific interventions. Authors say that "*IoT is a paradigm with different visions, and involving multidisciplinary activities*"[3]

However, we cannot dismiss that the information provided by each object can be aggregated, thereby creating a personal profile that may contain sensitive information which raises the possibility for the subject of being monitored. This is a crucial issue for privacy.

This scenario could present a number of legal issues related to privacy and data protection law. The main goal of each project is to evaluate the impact of the IoT phenomenon on fundamental rights such as the right to respect private and family life according to the European Convention on human rights. Nevertheless, there are others legal aspects to take into account developing a project on IoT.

Developing Applications for IoT

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, applications are developed to allow the interaction among objects themselves, transferring real time information.

For instance, to control household appliances in a smart home, industries have been developing sensors and applications, deciding autonomously the time to turn on or off, and communicating also any operation to the owner. This phenomenon is known as domotics. Thinking to the smart grid, it is interesting to transfer information from the meter installed in the house to the electric central system, bringing benefits both to the provider and users. Another application is the development of the city automation by systems that allow increasing the quality of life for people.

From a technical point of view, these applications need to be developed guaranteeing a high security level to avoid any kind of alteration. As technology develops, the attacks on the systems increase. However, we cannot ignore the threats to these systems. For example, the communication from a fridge to the owner about the food stored in it was intercepted allowing people to understand that the owner was away from home because the communication by the fridge was reduced or, instead, increased requiring some intervention for the presence of rotten food. However, it might happen that the fridge's owner has a pathology by which they are obliged to use special food and beverages. In case of communication interception, the health data could be discovered and spread: no personal data protection. The distorted use of this kind of information might facilitate criminal activities.

From another side, Israeli engineers raised an alarm for possible attacks to the public lighting with imaginable consequences. The effort to develop a

[3] Vermesan&Freiss (2016).

smart system based – as in this particular case – on the public lighting has its advantages but, at the same time, it is necessary to implement strong security measures to prevent any criminal activity. Let's image the devastating consequences of an attack to the smart grid!

The IoT concept is wide and involves critical infrastructure. The technological evolution is a value, but at the same time it is important to prevent any fraudulent attempt using strong security measures and privacy solutions.

Recently, a lot of news are spread over 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*"[4]. 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?

Privacy: Issues and Risks in the IoT

Despite its many potential benefits, the IoT poses significant privacy and security risks due to the technologies involved. There are several privacy risks for the users, as the following:

- *Identification of Personal Information*

Personal information can be transmitted only when the object is linked to a person, with a direct or indirect connection. A direct link occurs when the user is aware and gives consent to a possible transmission of his/her personal data. Or, when a person buys something and there is a RFID or other tag on the object, this could be a risk for privacy — especially if the person is automatically linked to the object during the purchasing process, such as through the use of a credit or loyalty card.

Alternatively, the connection is indirect when the object is linked to a person indirectly through the use of information that belongs to that person. For example, a number of objects are linked together by the Internet; I get information about object no. 1, but I don't know to whom this information belongs. I know, however, that objects nos. 2, 3, and so on, are connected among themselves and to a person named "Jane", therefore every piece of information provided by objects 2, 3, etc. are linked to that Jane. Furthermore, if I know that it is possible to link object no. 1 to objects nos. 2, 3, etc., I indirectly know that also the information provided by object 1 belongs to Jane.

- *Profiling*

The main risk for data protection and privacy probably, is profiling[5]. If

[4] The Economist (2015)

[5] Cavoukian (2010); Cavoukian, Polonetsky& Wolf (2010); Conoscenti, Vetr& De Martin (2017); Hilderbrandt (2009); Direcctive 2002/58/EC and Directive95/46/EC.

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 object. Furthermore, the transmitted data may be stored in one or more servers. Once people buy goods or services using electronic payment methods, it is simple to link the types of products purchased to his/her habit and lifestyle. The person may have previously provided consent for the dissemination of data related to his/her purchases for advertising purposes. Who manages the personal data and where these data will be stored? Data is a value, and it is mandatory to protect it. If data are stored on servers without high-security measures, it might grow the risks related to the data compromising with several consequences for the users' rights. It might happen also a system break down because who manage it does not use high-security measure or underestimate potential risks. The access by unauthorised subjects to the data is dangerous to the user.

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 modernizing the existing electrical grid by introducing smart meters, which communicate the 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 devices (first of all the smartphones) it is simple to find precise details on the location. If the user has not previously deactivated the geolocation service in the smartphone, his location will be known. In this way, privacy is definitely compromised. Smartphones and other mobile devices connected to the Internet contribute every day to the Internet of Things, spreading around data that can be used illicitly by other people.

- *Liability for Data Breaches and Loss of Data*

In Europe, there are numerous domestic and European Community (EC) laws relating to personal data breaches. Hence, also the Internet of Things has effects on liability when the data collected and transmitted lacks the appropriate security measures. Since the Directive 2002/58/EC, data breach is governed by law:

> "*In case of a particular risk of 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*".

The EU Regulation on the protection of natural persons[6], that will apply from 25 May 2018, revised the legislation on data protection[7] and, according to the Article 33, "*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent …*". In addition, data controllers and processors – in certain cases – must conduct a Data Protection Impact Assessment (DPIA – better known in the rest of the world as Privacy Impact Assessment - PIA) before undertaking risky data processing operations. The GDPR introduces several novelties such as Data Protection Officer, data protection by design and by default, and so on. The GDPR harmonises the domestic legislations of the EU member States adding value to privacy and data protection.

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

Blockchain, Privacy and Legal Issues: The New Challenge

The blockchain is a distributed database and this technology underlies bitcoin. The blockchain has been the object of technical analysis in the IT sector attracted attention for its potential applications. From a technical point of view, would emerge a structure very secure of the blockchain. Due to its technical configuration, it is founded on a powerful algorithm that should avoid any kind of alteration. In the last few years, different technical solutions to increase security have been provided. The blockchain technical structure seems very strong and exempt from compromising; however, its weak point is that if the owner of one of the nodes makes a mistake, the whole chain is compromised.

Academics and scientists[8] have developed theories about the blockchain to demonstrate the safety of its technical structure and someone says "*blockchains cannot handle privacy at all*"[9]. One of the main issues is the need of a 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, the IBM along with Samsung Electronics have developed the ADEPT (Autonomous Decentralised Peer-to-Peer Telemetry)

[6] Regulation (EU) 679/2016.
[7] Direcrtive 95/46/EC.
[8] Axon (2015);Conoscenti, Vetre& De Martin (2017); Kosba, Miller, Shi, Wen &Papamanthou (2016).
[9] Zyskind, Nathan &Pentland (2015).

project where, according to the document[10] [10] titled "Empowering the edge - Practical insights on a decentralised 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 decentralised IoT. Though many commercial systems in the future will exist as hybrid centralised-decentralised models, ADEPT demonstrates a fully distributed proof*".

Hence, it is evident the IoT evolution from a network of the object to a blockchain-based IoT.

In that IBM document[11] 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 makes the technical structure of the blockchain a very strong system. However, the blockchain, still now, is designed for the financial services and/or transaction. We cannot forget that the blockchain is sustained by the bitcoin and that in the successive phases it has been implemented thinking to a currency system. Now the blockchain implementation (such as Ethereum[12]) is being developed about contracts. However, the term "contracts" is related to one (or more) financial transaction(s) because it is a legal agreement where essentially the payment of an amount is completely automated. In fact, for example, in case of insurance obligation, on the date set the systems automatically make the payment. This kind of "contract" basically realises the financial transaction but any control is planned on the other agreement obligations. This confirms how developing is much closer to the technology than to 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 trains, the first one being much faster than the second one. A system development requires some technical intervention and rarely the legal support. People dealing with 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

[10] IBM (2015).
[11] Ibid.
[12] https://ethereum.org

always, after its complete development. It is appropriate – in certain cases – to involve a legal to evaluate previously the compliance with the law.

Blockchain, Privacy and Data Protection

Returning to the blockchain, one of the legal issues is the data protection and privacy law.

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 in terms of nature and approach.

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

The compliance process cannot ignore the EU Regulation of 2016[13] that – already in force – will be applied from 25 May 2018. It is necessary to highlight that a correct analysis approach in terms of Privacy by Design (PbD) or Data Protection by Design and by Default (DPbDbD) excludes any compliance with the law because this evaluation has to be made during the design phase. Privacy, hence, has to be considered 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 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.

The blockchain represents a computational operation apparently without natural person involved in it. There are several automatic operations executed by the software, but the blockchain cannot work without input from a natural person. More deeply, the node's owner – a natural person – decides what kind of transaction he/she wants to execute. This excludes, therefore, that the blockchain can be considered as a totally automated process in the creation nodes phase.

It is, therefore clear that:

1. the blockchain works by a software platform;
2. the blockchain adopts encryption and other high security measures;
3. the blockchain contains personal information or data;
4. the blockchain is a distributed database;

[13] Regulation (EU) 679/2016.

5. because of the distributed database, people do not know where data are stored;
6. people do not know who manages their data.

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

The Article 1, paragraphs 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 one hand, there is no doubt that the blockchain realises a fully automatic processing of personal data. On the other hand, the analysis has to evaluate if, in the blockchain, the processing of personal data by a natural person does not in the course of a purely personal or household activity. If both these conditions are realised, the GDPR is applicable. Instead, it might happen that the processing of personal data is in the course of a purely personal or household activity. In this case, even though the processing of personal data is fully automatic, the GDPR is not applicable.

If the case is under the GDPR, it requires the data subject's consent.In fact, according to the Article 6 (*Lawfulness of processing*), par. 1, lett. (a), of the GDPR "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 the data subject be considered informed by him/her?

This hypothesis rises a number of legal consequences; among them, the node owners can be considered as "controllers" and consequently they would have obligations and liabilities according to the GDPR.

As to privacy, due to the structure of the blockchain, the owner of each node should be considered as a "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 […]*".

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, has to consider also the organisational aspect. On the other side, among the measures indicated in the aforementioned Article 25, the pseudonymisation and the minimisation techniques can be used in the blockchain. These measures should be considered samples and not mandatories. The pseudonymisation seems in fact to be in contrast with the purpose of the blockchain in certain cases. For the same reason, also the minimisation could be not compliant with the blockchain nature and structure. This panorama demonstrates that 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 a distributed database, this could pose issues on the location where the data are stored since data could be stored everywhere in the world. This implies important consequences on the localisation and the application of the law. The data subject's rights could be compromised in case – for example –data are stored in a non-European country considered a "third country"[14].

In my opinion, it is clear that the GDPR has to be applied in particular cases regarding the blockchain.

Blockchain and Electronic Identification (eID)

There are other legal issues related to the blockchain, as contracts and electronic identity (eID).

One of the main important issues is the electronic identification of the user.

The EU Regulation 910/2014[15] 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 EU Regulation (910/2014), it is possible to suppose the development of the blockchain for any application that guarantees the electronic identification of each node's owner.

Very often people have to be identified themselves several times in the same process. An example is a financial service in which different operators and stakeholders are involved. Each person has to be identified step by step

[14] The European Commission has the power to determine, on the basis of Article 25(6) of Directive 95/46/EC, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

[15] Regulation (EU) 910/2014.

from different stakeholders. In fact, if a person asks moneys to a bank there might be the needing to identify the subject several times. Despite the certainty that a person is identified, this is a waste of time and resources. A identification system inside the blockchain could be a benefit both for the bank and for the person.

Due to the secure structure of the blockchain, it is possible to realise an identification system based on the same blockchain structure that guarantees the person identity once for all steps.

In this way, it is sufficient that the person has been identified once in the process to guarantee his/her identity to all the stakeholders and operators. It is possible to realise a secure electronic identity database – better, a secure electronic identity distributed database – that will be based on the high security measures of the blockchain.

According to the EU 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, data protection and privacy, and, at the same time, realising a secure database, guaranteeing the access to the authorised subjects for the authorised uses.

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 consciousness is the real engine that has pressed politicians and regulators to intervene in the IoT "realm". What about a legal approach to privacy?

In October 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a resolution on Privacy by Design (PbD)[16] 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.

Regarding privacy, we have always thought in term of compliance with laws, failing to evaluate the real role of the user (and his/her personal data). It is fundamental to start any process putting the user at the centre. This means that during the design process, an organization always has to think how to protect the user's privacy. By making the user the starting point in developing any project (or process), we realise a PbD approach.

The methodological approach is based on the following seven foundational principles[17]

[16] Resolution on Privay by Design (2010).
[17] Cavoukian (2011).

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.

The European Data Protection Supervisor (EDPS) has promoted PbD, touting the concept in the March 2010 Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy[18] as "*a key tool for generating individual trust in ICT*". Not long after this endorsement, the 32nd International Conference of Data Protection and Privacy Commissioners as well adopted the PbD concept.

In Europe, this approach became "Data Protection by Design and by Default" (DPbDabD) according to 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 that it's necessary 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 give a lot of attention to the technical and security aspects instead of the legal concerns, as seen in highlighting of the term "security".

The Article 25, paragraph 1, (Data protection by design and by default) of the GDPR 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*".

Applying the Privacy by Design or Data Protection by Design and by Default principles it is possible to take on any project, such as the complex blockchain in the IoT ecosystem. Each IoT application has to be designed

[18] Opinion of he European Dara Protection Supervisor (2010).

considering privacy (or data protection) by default. In this way, it is possible to guarantee both the users' privacy and data protection.

Conclusions

Industry may be wary of efforts to regulate the Internet of Things, since the IoT phenomenon is a potential source of huge business opportunities. For example, changes in the lifestyle — such as the use of more technological services like domotics — can definitely increase the consumer's quality of life (and industry's profits). It will be a decision of 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. With the Internet of Things reaching even more deeply into people's lives, it would be beneficial to have an international privacy standard to process 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 is related to existing laws, which are different in every nation (and even in different states and provinces within those nations). It is possible to develop a standard privacy framework that the organizations could use for the data protection activities. A 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 Data Protection Management System (DPMS) could be a reference model or a software system working on the PbD principles. At the moment, there is not an international privacy standard model, although several attempts were made.

In conclusion, in addition to the technological aspects, every future research on the Internet of Things phenomenon has to consider the legal issues, in particular privacy and security.

References

Axon L. (2015). "Privacy-awareness in Blockchain-based PKI" in *Oxford Reaserach Archives*, at: https://ora.ox.ac.uk/objects/uuid: f8377b69-599b-4cae-8df0-f0cded53e63b

Castelluccia, C., Druschel P., Fischer Hübner, S., Gorniak, S., Ikonomou, D., Pasic, A., Prenee, B., Tschofenig, H. & R. Tirtea(2011). "Privacy, Accountability, and Trust — Challenges and Opportunities*." European Network and Information Security Agency (ENISA),* at https://www.enisa.europa.eu/publications/pat-study

Cavoukian, A. (2010). "Privacy by Design; The Nsxt Genertation in the Evolution of Privacy:, in *Identity in the Information Society*, Vol. 3(2).

Cavoukian, A. (2011). "Privacy by Design - 7 Foundational Principles, at https:// www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Cavoukian, A.J., Polonetsky, J. & C. Wolf. (2010). "Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation." *Identity in the Information Society*, Vol. 3(2): 275-294.

Conoscenti, M., Vetr, A. & J.C. De Martin. (2017). "Peer to Peer for Privacy and Decentralization in the Internet of Things", in *39th International Conference on Software Engineering, Buenos Aires (AR)*, pp. 1-3, at http://porto.polito.it/26657 23/1/peer_to_peer_for_privacy_and_decentralization_in_the_internet_of_things.p df

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

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/LexUri Serv/LexUriServ.do?uri= CELEX:32009L0136:EN:NOT

Hildebrandt, M. (ed.). (2009). "D 7.12: Behavioural Biometric Pro ling and Transparency Enhancing Tools". FIDIS, *Future of Identity in the Information Society*.

IBM (2015). *Empowering the edge - Practical insights on a decentralized Internet of Things at* https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

Kosba, A., Miller, A., Shi, E., Wen, Z.& C. Papamanthou(2016). "The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", IEEE Symposium, at https://eprint.iacr.org/2015/675.pdf

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),19 March 2010, at: https://secure.edps.europa.eu/ EDPSWEB/webdav/shared/Documents/Consultaion/Opinions/2010/10-03-19 _Trust_Information_Socierty_EN.pdf

Regulation(EU) 910/2014 of the European Parliamnet 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, at: http://eur-lex.Euro pa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

Regulation (EU) 679/2016 of the European Parliamnet 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 repeal- ing Directive 95/46/EC (General Data Protection Regulation). At: http://eur-lex.europa.eu/ legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Resolution on Privacy by Design (2010). 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-29 October 2010. At: https://edps.europa.eu/sites/ edp/files/publication/10-10-27_jerusalem_re solutionon_privacybydesign_ en.pdf

The Economist, 31 October 2015 - **"**The great chain of being sure about things" at http:// www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

Vermesan, O. & P. Freiss (eds.) (2016). *Digitising the Industry Internet of ings Connecting the Physical, Digital and Virtual Worlds*. River Publishers Series in Commnication. Athttp://www.internet-of-things-research.eu/pdf/Digitising_the_ Industry_IoT_IERC_2016_Cluster_eBook_978-87-93379-82-4_P_Web.pdf

Zyskind, G., Nathan, O.& A.S. Pentland(2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy", at https://arxiv.org/pdf/1506.03471.pdf or http://www.enigma.co/enigma_full.pdf