Internet of Things: social and legal issues

Valentina Amenta, Adriana Lazzaroni, Laura Abba
National Research Council, Institute for Informatics and Telematics, Italy

Introduction

The advent of internet represents a revolution for the contemporary era, it having brought about a striking series of changes in social, institutional, political and economic life. This ongoing revolution has spread and absorbed within itself all the problems related to its own development. Objects become recognizable and acquire intelligence in that they are able to communicate data regarding themselves and also access other information aggregated by other devices. They are able to participate in a dialogue and interact among themselves within electronic communication networks, without human intervention. For example, alarm clocks ring early if there is traffic congestion, gym shoes transmit times, speed and distance in order to compete with persons located on the other side of the globe. Medicine bottles let us know if we forget to take our drugs. All objects can acquire an active role thanks to connection with the Web.

The associated problems, which can no longer be ignored, draw attention above all to the lack of data control, that is to the vast extent of the data collected and more generally to the security of these data.

This article has the aim of analyzing the ways in which European legislators, and consequently also Italian representatives, have intervened in order to stem the tide of emerging issues.

The “Internet of Things” model

We begin to speak of the “Internet of Things (known as IoT)” in 1999, during a presentation at Procter & Gamble by Kevin Ashton, British technological pioneer. In its first accepted meaning IoT referred to those objects which, by means of banal tags, were identified unequivocally and then represented within the Web.

The first clear definition of IoT dates to 2009, when Ashton wrote: “*We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data*[1]”.

[1] Kevin Ashton, *That 'Internet of Things' Thing*, RFID Journal, 2009, in http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf .

A further definition is found in 2012, when a non-profit making research institute, Rand Europe, attempted to give a definition of IoT in a research work for the European Commission. It is defined as: "*The Internet of Things (IoT) builds out from today's Internet by creating a pervasive and self-organizing network of connected, identifiable and addressable physical objects, enabling application development in key vertical sectors through the use of embedded chips, sensors, actuators and low-cost miniaturization. The IoT is developing rapidly, challenging assumptions underlying the future Internet business, market, policy, and societal models. Connecting billions of objects to facilitate smarter living, the IoT may help us address global and societal challenges, making Europe a sustainable and inclusive economy. However, IoT-driven "smart meters," grids, homes, cities and transportation systems also raise some important issues that will need to be addressed*[2]*"*.

From these definitions it is possible to extrapolate the first important data, that is we can use the term IoT to refer to "intelligent objects". These include devices or sensors, computers, tablets and smartphones, which have the privilege of connecting, communicating and transmitting information with or by means of each other through the Internet.

The paradigm which includes the intelligence of objects can be broken down into three directions[3]:

1. **Functionality of self-awareness**: identification, that is the possession of an unequivocal digital identification number (this is a basic functionality, present in all Internet of Things applications); localization, that is the capacity of objects to be aware of their own position (this may occur in real time, or through elaboration of tracing information collected during the productive or logistic process); diagnosis of state, that is the capacity to monitor the object's internal parameters so as to control its correct working state and possible need for assistance.
2. **Functionality of interaction with the surrounding environment**, that is data acquisition, conventionally divided into 'Sensing' (the measurement of variables of state that describe the physical system and/or surrounding environment) and 'Metering' (measurement of flow variables, such as consumption of electric energy, gas, water, heat, etc.) and implementation, that is the capacity to carry out commands remotely, by means of the distance control of actuators, or deriving from data elaboration *in loco*.
3. **Functionality of data elaboration**, that is, specifically, basic elaboration. This means the treatment of the primitive data collected, for example through filtering, correction, algebraic

[2] Rand Europe, *Examining Europe's Policy Options to Foster Development of the 'Internet of Things'*, 2012, in http://www.rand.org/randeurope/research/projects/internet-of-things.html

[3] Naturally the intelligent object must possess a capacity for connection in order to move the information collected at a local level towards remote applications, creating in this way a network of things.

aggregation, conversion, cryptography, etc., and advanced elaboration, that is the extraction of information from the primitive data, for example by means of statistical analyses, inferences and forecasts.

IoT is not yet a totally accomplished and mature model. It is rather a pathway of development which, starting from discrete-time identification based on RFID tags, has developed to the point of including sensor networks which connect the physical world to the digital world in real time.

IoT framework within Regulation (EU) 2016/679

The enormous amount of data which connected devices generate, often in an autonomous way, arouse concerns in terms of privacy and security.

The Global Privacy Enforcement Network (GPEN), the international network founded in order to reinforce cooperation between the privacy authorities of various countries, launched an investigation[4] in 2016 at an international level dedicated to verifying the respect of privacy within IoT. Besides that of Italy, another 28 national privacy authorities participated in the investigation. From the data it emerges that out of more than three hundred electronic devices connected to the Internet – such as watches and intelligent bracelets, electronic counters and new generation thermostats – more than 60% did not pass the exam of the privacy authorities.

The confirmations obtained by the experts of the Authorities[5], out of more than three hundred devices of the main companies of the sector, brought to light, at a global level, severe deficiencies in the protection of the privacy of users:

- 59% of devices offer no adequate information regarding how users' personal data are collected, utilized and communicated to third parties;
- 68% do not supply appropriate information regarding the way in which data are stored;
- 72% do not explain to users how to delete the data from the device;
- 38% do not guarantee simple ways of contacting those clients who require clarification regarding respect of their privacy.

[4] The investigation is "Privacy Sweep 2016". The "Sweep" on IoT follows similar investigations of recent years which looked into online services for minors, website privacy notices and mobile telephone apps. Antonello Soro, President of the Garante (Italian Data Protection Authority) states that: "the Internet of Things is full of promises, which range from a better healthcare service to an increasing efficiency of our homes. But these objectives must be reached with complete transparency, clearly informing persons of the use that is made of their personal data, safeguarding these data from violation and misuse with adequate security measures and respecting the freedom of individuals. It is vital to adopt an international approach to the Iot issue: a company not operating correctly with regard to users may violate, wherever it might be, the regulations regarding data protection and undermine the trust of the new intelligent objects that communicate and interact among one another". Cfr. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4877134.

[5] Cfr. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5443681

Some devices analyzed also presented problems regarding data security, for example sending "unencoded" (that is unencrypted) transmissions to the local medical practitioner containing information relative to users' health and therefore involving the sensitive data of users.

Despite the topical nature of the subject, above all in juridical terms, a clear and unequivocal picture regarding IoT does not exist. The directions to follow, in an attempt at least to make an effort to regulate the new context, are those offered by already existing directives and regulations. In addition, further complicating the legislative panorama there is the moment of transition due to the issue of the new EU regulation regarding the protection of personal data which repealed the previous directive. In fact, on 4 May 2016 there was publication in the Official Journal of the European Union of "Regulation (EU) 2016/679 of the European Parliament and 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".

The Regulation came into effect on 25 May 2016, but will in practice be operative in EU countries as from 25 May 2018. This leaves a two-year period for all interested parties to carry out the necessary adjustments to their data treatment policies.

In order to apply the new EU Regulation 2016/679, the treatment of personal data must be carried out within the context of activities in the location of the data controller in the EU[6] (irrespective of whether the treatment occurs within the EU). Furthermore, it is clear that this regulation applies to entirely or partially automated treatment of personal data and to the non-automated treatment of personal data contained in an archive or due to be inserted in one[7].

For the purposes of our research, it follows that all the objects used to collect and process individual data within the supply of IoT services (pace counter, thermostats, refrigerators, but also smartphones and tablets) qualify as tools.

A first problem is raised with regard to the identification of the Data Controller[8]. Such a heterogeneous area as IoT involves a combination of actions by various stakeholders such as device producers and social platforms, the providers or leasers of data brokers[9] or data platforms.

The complex network of stakeholders involved implies the need for a precise attribution of responsibility as regards the treatment of personal data, based on the specific nature of their relative tasks. The producers of devices, besides selling objects to their clients or products to other organizations, develop or modify also the operating systems of intelligent objects or they install

[6] Art. 3, parag .1, Regulation (EU) 2016/679

[7] Art. 2, parag. 1, Reg. com. 2016/679

[8] Cfr. Art. 4, comma 1, punto 7, Reg. com. 2016/679, *"Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".*

[9] Data brokers acquire data from firms so as to create lists of individuals belonging to the same category or group.

software which determines their operation, including the gathering of data and their successive transmission. Who are these data transmitted to? The sharing of the gathered and aggregated data belongs to the standard settings predefined by the producers and therefore the legislation would seem to identify the Data Controller as the figure or entity that has had an active role in the management of data collection, such as, for example, an application developer or software programmer.

Shifting attention to the figure of the user, that is the natural person who uses the technologically sensitive devices and to whom the personal data refer, we immediately face the problem of exclusion from application of Regulation 679/2016. In fact, the new Regulation retraces the old directive in the section in which at Art. 2 it is explicitly sanctioned that it cannot be applied to the treatment of personal data carried out by a natural person for the purpose of activities that are exclusively of a personal or domestic nature. What occurs in practice is a transfer of one's own personal data to the producers of devices, application developers and other third parties at the moment at which the various devices are utilized. This generalized lack of awareness on the part of the user is at the center of the debate concerning IoT, bringing to light critical situations and risks for the total effective loss of control over one's own data. The user, indeed, for the most part, is unaware that the technological interaction involving IoT is founded on a massive and ongoing process of collection and manipulation of their personal data. This situation is particularly suited to allowing an intrusion, more or less penetrating, into the individual's sphere of privacy[10].

If it is true, in fact, that the emergence of new technologies based on dialogue between devices involves risk profiles as yet unknown to users, it is absolutely essential to provide users with suitable information in order to make them effectively aware of the single activities of elaboration and transmission of data involved in the services being used, with particular attention paid to the purposes of this treatment.

The need for appropriate information was advanced by WP29[11] which expressly specifies that for the treatment to be lawful the *users must remain in complete control of their personal data throughout the product lifecycle*[12].

[10] Cfr. Opinion 8/2014 on the Recent Developments on the Internet of Things, 16 September 2014, p. 4: "*In the light of the above, the development of IoT clearly raises new and significant personal data protection and privacy challenges". In fact, if uncontrolled, some developments of the IoT could go as far as develop a form of surveillance of individuals that might be considered as unlawful under EU law. The IoT also raises important security concerns, as security breaches can entail significant privacy risks for the individuals whose data are processed in such contexts".*http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[11] The Article 29 Working Party (WP29) has published an opinion on the 'Internet of Things' (IoT). In the opinion, the WP29 gives a reminder that the Data Protection Directive applies in full to IoT. The WP29 highlights the specific privacy and security concerns associated with IoT (such as the need to obtain properly informed consent to the processing of personal data) and sets out the practical measures that must be taken by data controllers in the IoT environment to ensure compliance with data protection laws.

IoT and anonymous personal data

Within the context of IoT, it often occurs that an individual can be identified on the basis of the data originating from devices.

It may be that the subjects interested by the personal data treatment are not themselves IoT users. For example, a wearable device, such as intelligent glasses, can gather data regarding other interested subjects, third parties with regard to the possessor of the device. It follows, therefore, that the possession of a device is not the essential prerequisite for being interested party to the treatment of the data.

Despite various efforts to create techniques of anonymization and pseudonymization, these data remain very much within the category of personal data[13].

As regards the legitimacy of the process of anonymization[14], first of all, this is a technique applied to personal data with the aim of obtaining an irreversible de-identification. Therefore, the initial assumption is that the personal data must be gathered and treated in conformity with the applicable legislation regarding the storage of data in an identifiable format. Within this context, the process of anonymization, understood as treatment of personal data to obtain anonymous data, represents "successive treatment".

In the light of what has been specified above, we can arrive at the conviction that the techniques of re-identification have prevailed and that we have already surpassed the legislative apparatus based so far on the belief that to protect a consumer from aggression to their private sphere it was enough to share information in an anonymous manner.

[12] Option 8/2014 on the Recent Developments on the Internet Things, cit., p.3.

[13] L'Art. 4, Parag. 1, EU Regulation 2016/679 defines personal data as: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[14] Cfr. Option 5/2014 on Anonymisation Techniques adopted on 10 April 2014 (WP 216). Opinion 05/2014 on techniques of anonymisation, highlights four key features:

1. anonymisation can be the result of the treatment of personal data with the aim of irreversibly preventing the identification of the data subject;
2. various techniques of anonymisation may be envisaged. There is no prescriptive standard in EU legislation;
3. contextual elements must be given importance: it is opportune to take into account the combination of means which may reasonably be used for the identification by the Data Controller or third parties, paying particular attention to what at the current state of the technology has become "likely reasonably";
4. anonymisation presents an intrinsic risk factor; this must be taken into account when assessing the validity of any technique of anonymisation (including the possible uses of the data made anonymous by means of this technique). In this opinion the expression "anonymization technique" is used rather than "anonymity" or "anonymous data" to highlight the inherent residual risk of re-identification linked to any technical-organisational measure aimed at making the data anonymous.

An example may clarify. Fitbit, a producer of bracelets and connected scales which monitor respectively physical fitness and weight loss, could introduce a de-identification of the data. This may be done by removing name, address and other information which can identify the user before sharing this information with others. All this will however not be sufficient due to the ease of re-identifying this data set. The reason is very intuitive: each of us has a unique gait. This means that if we know the gait and walking style of a user, it could be possible to identify that individual among the millions of anonymized data belonging to the Fitbit users.

In Italy legislation has dealt with anonymous data, identifying it as that data which in its original form, or following treatment, cannot be associated with an identified or identifiable interested party[15].

Furthermore, Italian legislation puts anonymization within one of the fundamental principles of the Italian Privacy Code, that is the "principle of necessity[16]". According to the regulation, information systems and the software used within them must be configured in such a way as to minimize the recourse to personal and identifying data, substituting the treatment with the use of anonymous data or pseudonyms when there is no significant impact on the purpose for which the data is required. This foresees identification of the interested party only in the case of absolute necessity. This represents a veritable revolution in the approach to the protection of data processed with automated systems, above all as regards electronic commerce and telecommunications services. It is worth noting that this principle appears neither in Directive n. 95/46 nor in Law n. 675/96 and imposes a rather onerous obligation. How is it possible, in fact, to establish if the purposes of a program can be satisfied using anonymous data? This is even the more so given that the breadth of definition of personal data makes it problematic to consider a treatment that does not use personal data. Each time data treatment is carried out relative to a subject, even if the processing occurs regarding data that are apparently anonymous, these must inevitably be defined as personal given that, directly or indirectly, they are relative to a certain subject .

To be precise, the anonymization techniques of particular importance are those which can be termed "issue and forget". After having released a piece of information, publically or privately, to third parties or internally with the same organization, this is forgotten, in the sense that there is no attempt to monitor what occurs to the data after they have been issued. Rather than putting at risk the interested party, the information regarding the data subject is modified before being issued.

These techniques are very widespread because they enable diffusion of the data while at the same time safeguarding privacy. In practice, therefore, before issuing the data, the following steps should be taken:

[15] Art.4 Data Protection Code

[16] Art.3 Data Protection Code

- Locate identifying information: any field which may be used to identify individuals should be ascertained. Often there can be identification of combinations of fields which analyzed together could create a link between the record in a table and the identity of a patient.
- Repression: following this the identifying fields are modified, for example by removing the fields from the table. In doing this, concerns regarding the protection of personal data are reduced. However, if someone knows the birthday, sex, ZIP code and race of an individual their identity could be deduced. This method, however, could make these data useless for research within a medical field (Fig. 10).
- Generalization: there is an attempt to reach the best balance between usefulness and privacy with respect to the repression of the data. This means altering rather than completely cancelling the identifying values. Whoever decides to use this method could, for example, choose the name in the field and generalize the date of birth (leaving only the year, and not also day and month) and ZIP code (leaving only the first three figures).
- Aggregation: in this case we are taking into account more a statistical synthesis rather than raw data. Therefore we can put together, for example, sex, illness and a single figure of the ZIP code. If someone knows no further information regarding the individual, it is much more difficult to identify them.

Comparison of the anonymization process of USA- Europe

In the US the issue of anonymization was taken into account to balance out problems of privacy which regarded the field of healthcare. In 1996 the HIPAA (Health Insurance Portability and Accountability Act) was established. This law, besides having the aim of improving healthcare assistance and insurance, is intended to solve the problems of privacy and security concerning healthcare information. More precisely, as regards the latter, there is the "HIPAA Privacy Rule" which establishes national standards to safeguard information regarding personal health, and is applied to personal healthcare plans, and more in general, to the suppliers of healthcare services that carry out certain operations of personal healthcare assistance through electronic means (these are defines as "covered entities"). The rule specifies adequate guarantees in order to protect the privacy of healthcare information and establish limits and conditions regarding the uses that can be made of this information without authorization of the patient[17].

[17] HIPAA Privacy Rule, Title 45 (Public Welfare, Department of Health and Human Services) C.F.R.(Code of Federal Regulations) §§ 160 (General Administrative Requirements),164 (Security and Privacy) (2009).

In Europe, the situation is different. The Data Protection Directive claims to cover each "piece of personal data", of which we have already analyzed the definition[18]. Reiterating the concept, Europe does not intend to apply the directive to all data, excluding those which do not identify an individual "directly or indirectly", such as anonymized data.

The European legislators, just as occurs in the U.S., are convinced of being able to reach a balance using the power of technology. If they are in an anonymous form, the data could be freely shared, implementing innovation and free expression, it being understood that the interested parties are not identifiable " directly or indirectly ".

For many years debates have developed, above all with companies such as Google, Microsoft, and Yahoo, on the way in which these should protect the databases which trace the online movements of their users. Many of these discussions have focused on IP addresses. In the same way that a social security number identifies a person, an IP address identifies a computer, which may then link online movements to the position and identity of an individual.

Remembering that an IP address is generally made up of 32 bits, sub-divided into 4 equal groups of 8 bits, each one referred to as an octet, the intention of Google was that to safeguard the privacy of its users by memorizing only the first three octets and cancelling the final one. Microsoft and Yahoo wanted to be even more drastic, by cancelling the entire IP address. This was also a debate on the search for an equilibrium between the innovations provided by Google which studies individuals' behavior, and possible harm caused to the users, whose IP addresses are revealed and known[19].

Technology poses new challenges in the field of so-called "non-PII (Non-Personally identifiable information)". Information scientists, in fact, are constantly seeking creative methods in order to combine various pieces of non-PII and make them PII, enabling the de-identified information to be re-personalized. As proof of this, in 2006, America Online (AOL), released 20 million "search queries[20] " for the benefit of researchers. These "queries" were considered to be totally anonymized. However, journalists of the *New York Times* showed that at least some of this information was easily re-personalized. They were able to identify a person on the basis of their search queries (Thelma Arnold, a 62-year-old widow living in Lilburn, in Georgia). All this was possible thanks to the aggregation of apparently disassociated information such as "'landscape painters in Lilburn', 'persons with the surname Arnold' and 'houses sold near the lake in the county of Gwinnett'". AOL apologized for the diffusion of information, recognizing that it had violated the privacy of its users despite attempts to anonymize the data.

[18] Cfr. Art. 4 Reg. Com. 679/2016, punto 1.

[19] On the myth of anonymization and IP addresses, see also P.M.Schwartz, D.J.Solove, "The PII problem: privacy and a new concept of personally identifiable information", NYU LAW REVIEW (2011).

[20] "Research queries" can be defined as questions that the user poses to a database.

In order to demonstrate yet again the ease of re-identifying data, Latanya Sweenwy, professor of computer science at Carnegie Mellon University, by means of a study, reached the conclusion that by combining Zip Code[21], date of birth, and sex, it is possible to identify 87% of the individuals in the United States. This was quite a shocking result given that these pieces of data are generally considered to be non-PII[22].

A further problem with "non-PII" is that much of this information that regards persons is easily available and this increases the possibility of reconstructing PII through non-PII.

This aspect of the problem of re-personalization stems from an aspect of the privacy issue known as "aggregation", which involves the combination of various pieces of data. An individual who thinks that they are anonymous when using certain websites can supply information that can identify the person explicitly, such as when one is making a purchase. IP addresses can be used to connect de-identified data to names and addresses.

A further example involves a studio of Netflix, a popular online film rental service. After some research, two information scientists (A.Narayanan and V.Shmatikov) demonstrated that some persons could be identified by means of a set of apparently anonymous data, on the basis of evaluation regarding the films within a website. Netflix made a de-identified database of film rating available to the public, in order to improve the predictive capacity of its software so as to recommend certain films for rental. This study essentially demonstrates that a single piece of non-PII does not exist in isolation, but there are other data sources which enable the re-identification of a piece of data that has been made anonymous.

"Data miners" and market operators currently use these techniques. Let us suppose we have data on age (13 years), name (single alphanumerical identifier), favorite toy (Lego), favorite film (Batman), favorite candy (Snickers), favorite restaurant (McDonald's), Zip code (20052). In a world without other sources of data this information would remain anonymous, but in current society crisscrossed by a plethora of data originating from a wide range of different sources, this is impossible. This apparently anonymous child, could, for example, have a Facebook profile where, with a precise name, they can share their interests and preferences which can coincide with those mentioned above. Besides a social network, there could also be other databases that can specify, name, date of birth and addresses. All these pieces of apparently anonymous data can be gathered and linked together in order to give a certain identity to a precise individual.

[21] ZIP (Zoning Improvement Plan) code is the postal code for USA addresses.

[22] L.Sweeney, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy Working Paper, LIDAP-WP4 (2000)

The Health Insurance Portability and Accountability Act[23] (hereinafter HIPAA) deals with 18 categories of information as being identifying, excluding from this list such data as those on patients such as hospital name, diagnosis, year of medical exam, patient's age and the first three figures of the ZIP code, which an individual possessing other external information can use to defeat the state of anonymity.

The same approach, in following a categorization of data, is faced by the "Driver's Privacy Protection Act", which requires special treatment for "personal information", which includes among other items: social security number, driver identification number, name, address and telephone number. On the other hand, less protection is required for a Zip code and any information on accidents, driving violations drivers' conditions.

In the same way, the Federal Education Rights and Privacy Act[24] (FERPA) refers to the safeguarding of "directory information", including among other things: name, address, telephone number, date and place of birth and main fields of education.

In the light of this easy re-identification, such regulations appear to be somewhat arbitrary and not protective. In this case there is however the need to take into account recital 26, which beyond what has already ben mentioned, adds that, in order to determine whether a natural person is identifiable account should be taken of all the means reasonably likely to be used by the data controller or other persons to identify the individual. Given that the directive deals with all the information that is directly or indirectly connected with a person, each re-identification of an apparently anonymous database extends the coverage of the directive to that database. As a consequence, the regulation which has the aim of having limits becomes unlimited. The easy re-identification has an opposite impact on the HIPAA, whose safeguards are revealed to be illusory and incomplete, in that it does not take into account the treatment of types of data that can be used in order to re-identify and cause harm. In one way or another, both do not reach the balance established at the outset and the

[23] The Health Insurance Portability and Accountability Act of 1996 was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum–Kennedy Act after two of its leading sponsors.
Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. Cfr. Atchinson, Brian K.; Fox, Daniel M. (May–June 1997). "The Politics Of The Health Insurance Portability And Accountability Act" (PDF). Health Affairs. 16 (3): 146–150. doi:10.1377/hlthaff.16.3.146.

[24] The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) is a United States federal law that governs the access of educational information and records. FERPA gives parents access to their child's education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records. With several exceptions, schools must have a student's consent prior to the disclosure of education records after that student is 18 years old. The law applies only to educational agencies and institutions that receive funding under a program administered by the U.S. Department of Education. Other regulations under this act, effective starting January 3, 2012, allow for greater disclosures of personal and directory student identifying information and regulate student IDs and e-mail addresses. Cfr. Mendelsohn, Stephen A. (2 January 2012). "U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures". The National Law Review. Retrieved 9 March 2014.

vagueness of the regulations inevitably cannot avoid fueling controversy and may very well bring about irrational distinctions between jurisdiction and law.

Towards PII 2.0

There is a need to abandon the idea that the protection of interested parties can be accomplished simply by removing PII. It is not important how the regulating authorities follow the developments of re-identification, because the researchers constantly seek out other types of data fields that are still uncovered by the regulations. The list of potential PII will never cease to grow until it includes literally everything. Legislators and regulating authorities should reevaluate laws and regulations that make distinctions based only on the fact that particular types of data can be associated with identity and should avoid the drawing up of new laws and regulations founded on this distinction. The transformation into an anonymous form, in this way, should no long be taken into account when supplying guarantees of privacy.

The best solution would seem to be that of re-orienting privacy according to a concept different from that of PII (in this case there would not be limits to the scope of the law on privacy), and following the proposal whereby regulators should attempt to safeguard interested parties by restricting and reducing the flow of information within the society, although this could obviously sacrifice values such as innovation, freedom of expression and security.

It seems appropriate, therefore, to carry out a cost-benefit analysis for all the data treated and gathered. However, this is very difficult to undertake, above all because costs and benefits are often not known in advance.

The European expansionist approach, as previously mentioned, appears open to criticism given that privacy rules concerning an identified natural person are equivalent to that of the data concerning an identifiable person.

In this way we come to the definition of the so-called "PII 2.0", as sustained by Solove and Scwartz[25] . The benefit of having two categories of PII, data that regard identified or identifiable persons, paves the way to more correct legal protection. This approach enables the safeguarding of both categories of information.

In this model the information refers to a person:

1. Identified: the information identifies a specific person with respect to others, and therefore verifies their identity. On the content of this category there is international agreement[26].

[25] Paul M. Schwartz, Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, in Berkeley Law Scholarship Repository, 2011.

[26] In the U.S.: General Accounting Office, Office of Management and Budget and National Institute of Standards and Technology. In Europa Art. 29 Data Protection Working Party, Opinion 4/2007 on The Concept of Personal Data 12 (June, 20, 2007).

2. Identifiable: a specific identification, albeit possible, does not represent a very probable event. In other words, an individual is identifiable when there is some possibility of future identification, albeit not too far into the future. The level of risk for the law is moderate. This information should be treated differently from the category of nominally identifiable information, where a connection to a specific person has not yet been established, but it is much more probable that this can occur.
3. non-identifiable: these data are not easily associated with a person, taking into account the means that can be reasonably used for the identification. This is the classic case in which we have enormous amounts of data (e.g. the population of a state).

A clear way of demonstrating the working of this new approach is that of considering the applicability of FIPs[27]. This is with the aim of limiting the use of information, limiting data collection, limiting the diffusion of personal information, gathering and using the information only if it is accurate, pertinent and updated (principle of data quality), creating treatment systems that the interested party is familiar with and understands (systems of transparent treatment) and guaranteeing security for personal data.

When the information refers to identified persons, all these practices should be applied. It must be specified, however, that the precise content of the ensuing obligations will often be different depending on the context in which the data are treated, on the nature of the information gathered, and on the specific legislative, normative and organizational context in which the rules are formulated. In the opinion of the authors, it is not opportune to treat the category of identifiable information in the same way as the information that enables direct identification.

Within the context of identifiable information, it is necessary that companies pay attention to the treatment of identifiable information by third parties. If a piece of information is not identifiable, a company can publically release it and allow access to third parties.

One of the advantages of this approach is that of adapting practices to the nature of the identified or identifiable information. A further advantage is that it is an incentive for companies to maintain information in the least identifiable form possible. If the concept of PII is abandoned, or if the treatment of identified data is considered like that of identifiable data, firms will be less prepared to use resources to maintain the data in an anonymous form.

[27] I FIPs (Federal Information Processing Standards) are a set of rules that describe the elaboration of documents, algorithms of cryptography and other standards of information technology.

Regarding this theme, Federal Trade Commission[28] has expressed the opinion that as long as a certain data set is not reasonably identifiable, the company makes a public commitment not to re-identify it[29].

In brief, FTC has attempted to distinguish between data that are "reasonably identifiable" and data that are not, and also between those firms that are taking the necessary measures to prevent re-identification.

Although both approaches (PII 2.0 and that of FTC) are attempting to use this new third category of identifiable information to avoid the complete collapse of all the data in the category of PII, this may be inevitable within the context of IoT.

More precisely, within the context of IoT there is often confusion in judging data originating from sensors or biometric data as personal information. Some privacy policies of companies define "personal information" (or "PII") traditionally, including names, postal addresses, telephone number, e-mail addresses, etc. For these policies the data originating from sensors should not have the highest protection guaranteed for PII. Other policies are less clear and may mislead to the point of appearing to be contrary to what has been stated above.

The privacy policy of "Breathometer[30]" for example, defines "personal information" as "information that directly identifies you, like your name, address of delivery and/or invoicing, e-mail address, telephone number, and/or data regarding your credit card". Although there is no trace of "sensor data", an information scientist or regulator who understands the problem of re-identification could very well include the test results in the category of personal data.

In the same way, the privacy policy of "Nest Thermostat[31]" defines "PII" as data that can reasonably be associated with a specific individual or family.

Given the threat of re-identification of data in IoT, it is difficult to understand whether the abovementioned policy considers the data originating from the thermostat as personal data or not.

Many other examples could be given, but the point remains the same. Regulators and legislators have not yet faced the reality of these "new" data that can all be identifiable.

The European approach is different where some regulations before the directive and now in the new regulation leave a different margin of flexibility. They attempt to reach a correct balance between

[28] The Federal Trade Commission (FTC) is an agency independent of the government of the United States, founded in 1914 by the Federal Trade Commission Act . Its main mission is the promotion of consumer protection and the elimination and prevention of anticompetitive commercial practices, such as coercive monopoly.

[29] FTC REPORT , Protecting consumer privacy in an era of rapid change: recommendations for business and policymakers, March 2012 .

[30] Breathometer is an application that connects to Breeze, an ethilometer which enables users to evaluate their state of drunkenness.

[31] Nest Thermostat is an intelligent thermostat which can reprogram itself on the basis of an individual's habits.

the rights of the interested person and the legitimate interests of the parties involved which appears somewhat fragile.

Some examples of these regulations, to cite only a few, which appear in the new Regulation n. 679/2016 follow:

- Art. 5, lett. e): kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- Art. 6, lettera f): processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
- Art. 9, lettera c): processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Art.10: Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

According to a European approach, therefore, data protection is aimed at protecting the forms of treatment which typically present a higher risk of "easy access to personal data". Furthermore, the new Data Protection, being configured as a Regulation and not as a Directive, deprives the single states of the possibility of approving national laws in this regard which would be in conflict with each other. The objective to be reached is harmonization of the discipline in the European environment.

This did not occur with Directive 95/46 where, as the Court of Justice of the European Union[32] stated, nothing impeded a member state from extending the scope of its national law with regard to the enactment of Directive 95/46 to sectors not included in the area of interest of application of the directive, as long as they did not infringe any other regulation of EU legislation.

[32] Sentence of the Court of Justice of the European Union C-101/2001 of 6.11.2003 (Lindqvist), point 98.

“Notice and consent” model in safeguarding the consumer

Continuing in our analysis, it is necessary to go into greater depth regarding the principles relative to the quality of data. It is clear that personal data must be fairly and lawfully[33] treated with the effective awareness of the individual. This is a very important requisite in relation to the new technological context, where sensors should be designed so as not to be excessively intrusive. For example, a device that uses a small light to monitor blood flow in the veins is also able to detect information regarding heartbeat. The device can include, moreover, other sensors which measure the oxygen level of the blood, but no information is available on the collection of these data either from the device in general or from the user interface. Even if this sensor is working, it should not be enabled without having first informed the user. It follows that explicit consent is required in order to enable the sensor.

In this context, at least three important principles deserve attention:

1. “principle of purpose limitation[34] ”: that of «purpose limitation», according to which the treatment is lawful as long as it is not incompatible with the original purpose for which the processing was carried out (this principle is very close to the idea of pertinence as opposed to excess in data collection);
2. “principle of data minimization[35]”: the data collected on the interested parties must be strictly necessary for the specific purpose pre-emptively determined by the data controller
3. “principle of storage limitation”, for which the personal data can be stored for the time required to reach the original aim and only exceptionally can they be stored for longer periods on condition that they are processed exclusively for the purpose of archiving in the public interest, for scientific or historical research or for statistical purposes. These public interests balance the personal interest in privacy with the public interest in data collection. This final principle is what can limit the potential opportunities of IoT, becoming a veritable barrier to innovation.

An example may clarify better the final concept expressed. Let us suppose we have a wearable device, such as a sticking plaster, which can assess the skin conditions of an individual. The device does not need to gather precise geolocational information to work efficiently. However, the device

[33] Art. 5, lett. a), Principles relating to the processing of personal data of EU Regulation n.679/2016.

[34] Art. 5, lett. b). Principles applicable to the treatment of personal data.

[35] Among the many references on "principle of data minimization", FTC Staff Report: "Internet of things, Privacy Security in a Connected World", January 2015, with reference to the risks of gathering and maintaining great quantities of data, among all: the possibility of violating data and the possibility of using data in such a way which moves away from the reasonable expectations of the consumer.

producer could believe that such information can be useful for implementing future features of the product, which may enable the user to choose further treatment options regarding their particular medical condition. As part of the exercise of minimizing the data, the producing company should wait before gathering geolocational data until beginning to offer the new features of the product. There may also be the possibility, for the company, of gathering less detailed information, such as a ZIP code, rather than more precise information of geolocation. If the company decides that the collection of the latter is necessary, it must supply clear information regarding the gathering and use of the information, and obtain clear consent from the consumer. Finally the company must establish the limits of reasonable maintenance of the data gathered. Once this necessity is established in order to satisfy business requirements, this can also be the possibility of conserving the data in a de-identified form. This could be a solution, as already discussed, in order to establish a balance between consumer protection and benefits for the company in terms of using the information collected.

Here we arrive at a much debated area of the Internet of Things, that is the so-called "notice and consent" model, which we should contextualize in order to highlight its limits.

Consent[36] is whatsoever display of free, specific and informed will with which the interested party accepts, by means of declaration or unequivocal positive action, that the personal data regarding them are an object of treatment[37]. This offers a way to reconcile, on the one hand, the problem of damage to the consumer with regard to the data deriving from connected devices, and on the other hand, the desire to possess the device which inevitably implies benefits, already previously analyzed. Therefore, if the consumer were aware of and consented to the flow of data generated by the various devices, there would be no cause for concern.

The point is that within the current context, where the “transformative” use of Big Data makes it impossible to describe all the possible uses of information at the moment of initial data collection, this type of approach is inadequate. Furthermore, the digital world is characterized by an asymmetric distribution of control over information, in terms of access to quality data and in terms of ability to use them. In this sense, control over information deriving from predictive analyses is not accessible to everyone, because it is based on the availability of great quantities of data, costly

[36] Art. 7, Conditions for consent, EU Regulation n. 679/2016 and Art. 29 Data Protection Working Party, "Opinion 15/2011 on definition of consent", adopted on 13 July 2011,7
Article 29 Data Protection Working Party ,"Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 or Directive 95/46/EC" adopted on 9 April 2014, 11, 23-32

[37] Art. 4, n. 11, Definitions, EU Regulation 679/2016 and Art. 4 (8) Proposed General Data Protection Regulation (pGDPR). Differently in the U.S., the traditional approach, built on various sector-based regulations, has underestimated the role of the user’s choice, adopted a more market-oriented strategy. However, it seems that the recent guidelines, adopted by American administrations, suggest a different approach, reinforcing “self-determination". In this regard, see The White House "A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" pp.47-48.

technology and specific human skills able to develop sophisticated systems of analysis and interpretation. A final restraining aspect is that in the current digital economy, consumers often seem to accept that there have no negotiating power regarding their personal information, essentially due to the concentration of the market and relative social and technological lock-in effects, which are a further limitation to "self-determination" and to the user's choices[38].

For these and other reasons we need to reconsider the "notice and consent" paradigm within existing regulations that regard data protection, and define new rules able to face the various problems of the current and future digital environment[39].

At this point all the legislative apparatus seems to be in difficulty. Analyses of Big Data are designed to remain hidden, therefore it appears that the description of purposes, as we have seen, at the center of the regulations on data protection, is becoming increasingly tenuous.

It follows that the difficulty in defining the expected result of data treatment prompts the production of generic and vague declarations for the consumer regarding the purpose of the data collection. Furthermore, in the hypothetical adoption of long and detailed information, the complexity of data processing within the new context does not offer users a real opportunity to understand it, interpret it and therefore make informed choices.

This all prompts reconsideration of the role of user self-determination, in the situation in which the consumer is no longer able to fully understand the data processing and its purposes, or is not in a position to make decisions. In this regard, initially, the proposal of the EU Regulation was that "consent does not constitute a juridical basis for the treatment when there is a notable imbalance between the position of the interested party and the data controller[40]" .

To further complicate the situation there are various technical issues regarding IoT devices. The devices are often small, without a screen, have meager input-output capacities, such as keybord or touch screen. From here there arises the need to channel elsewhere the user's privacy information: in the device's box, on the producer's website or within a cell phone application.

Currently, the preferred solution on the part of producers is to supply information on data treatment within a privacy policy published on a website. However, this system does not take into account

[38] " Social lock-in effect" is one of the consequences of the dominating position maintained by the big players, evident in the market of social networks. It represents the incentive to remain on a network, given the number of connections and social relations created and managed by the user of a platform of a social network. This implicitly limits the possibility of users recreating the same network elsewhere.

"Technological lock-in effect" refers to technological standards and data formats that are adopted by the various service providers. This effect limits data portability and the migration from one service to another even though the same functions are offered.

[39] A. Mantelero, "The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics", Computer Law & Security Report, November 2014

[40] Art. 7 (4) PGDPR, subsequently cancelled and replaced with Art.7(4) PGDPR (COM(2012)0011 – C7 0025/2012 – 2012/0011 (COD)), hereafter PGDPR-LIBE.

that a consumer's purchasing experience may very well be different from their Internet navigation skills. In addition, there is an unjustified belief in the association between devices and a smartphone app or Internet account[41].

Confusion also reigns when it is decided to apply two privacy policies: one for the website and one regarding use of the device. This kind of solution simply doubles the cognitive and attention load of the consumer.

Essentially, as asserted by S. Peppet[42], the issues regarding privacy policy focus on the ambiguity of the language of the policies – this has already been discussed regarding the "PII" issue – and on the evident omissions in the policies. It often occurs that the privacy policy does not mention the owner of the data of the device (consumer or producer?), which type of data the device gathers and which type of sensors are used by the device. These policies are often contradictory when one speaks of rights of access, modification and cancellation by the consumer, and the policies frequently confer these rights only for personal data, for which there remains the problem of exact categorization.

To conclude regarding policy omissions, we cannot help but mention the lack of a precise and clear explanation of how these data are processed in the device itself and on the companies' remote servers to which the data are transmitted.

Possible developments: towards an opt-out scheme

In the light of what has already been said, the user's role must inevitably be restricted and the importance of the independent authorities must increase. The latter, with respect to the consumer, have the technological know-how to assess the risks associated with the various data treatments and can adopt legal remedies to tackle them. Moreover, the authorities are those in the best position to balance all the different interests of the various stakeholders regarding the vast collection of data and their extraction.

This does not mean cancelling the old model, but simply reinforcing it, increasing transparency, the responsibility of service providers, and architectures oriented towards the protection of data.

Transparency

[41] This is an example examined in the article of S.R. Peppet (see note 11). It regards "iHealth" producers of various devices that monitor health and fitness, and which function together with smartphone-installed apps. The conclusion reached is that the consumer is guided into a vicious circle permeated by total confusion.

[42] Peppet Scott R., "Regulating the Internet of Things: first steps toward Managing Discrimination, Privacy, Security, and Consent", Texas Law Review, Vol 93:85. (2014)

Transparency[43] is an instrument which aims to improve the user's understanding and control of personal data. This can occur only if the user's notice is provided and is clear as regards various aspects. These include the purposes of data collection, the memorization and/or treatment of the data, an overview of the type of data made known, information regarding the data controller exactly which policy is being used and if there is online access for personal data . In addition, it must be made clear the way in which the data are processed, and if a sort of counter of profiling capacity has been put into effect to help users to prepare a group filing by means of their data[44].

The notice can be provided on the device, using wireless connectivity, or using the location through privacy-preserving proximity testing, done by a central server. This information must be supplied in a clear and understandable way in accordance with the principle of correctness in data treatment. For example, the producer of devices could insert in the "things" equipped with sensors, a QR code or an instantaneous code able to describe the types of sensors and the information they capture together with the purposes of the data collection.

As also stated in a report of FTC97, the privacy notice should be clear as clear, brief and standardized as possible so as to be easily understood and also enable the user to compare privacy practices.

One of the first attempts to develop a standardized privacy notice for the user was the "multilayer privacy notice", which included a standardized page, sub-divided into sections, in which aspects of privacy were explained. The upper part parte included titles of standardized sections and a brief summary of the content of each section.

Others supported the so-called "nutrition label" approach for the standardization of privacy policies[45]. This approach enabled consumers to search for information more rapidly and precisely compared with a traditionally written privacy policy. It is certainly shorter, easier to read and its standardized table enabled the user to understand the search modes (what and where to search) and facilitated comparison with other policies.

Although privacy policies are not exactly a good tool for communicating with most users, they do play an important role in promoting transparency, accountability and competition between companies as regards issues of privacy. This is all made possible only if the policies are clear, concise and easy to read, as in the case of the "nutrition label". There is often to need for small

[43] This theme is also recognized as an important element of privacy in the "Mauritian Declaration on the Internet of Things", approved on 14 October 2014: "transparency is the key: whoever offers IoT devices should be clear on what data is being gathered, for which purpose and for how long they are stored". Furthermore, cfr. Art. 13a PGDPR-LIBE

[44] R.H. Weber, "Internet of Things: Privacy issues revisited", Computer Law & Security Review 31 (2015) 618-627. There are regulations on transparency also in the Recommendation n. 7 of the Commission: "on the application of principles of protection of private life and personal data in applications based on radiofrequency identification", May 2009.

[45] Lorrie F. Cranor, "Necessary but not sufficient: standardized mechanisms for privacy and choice", (2012) 10 J. on Telecom & High Tech L. 273.

icons that can be integrated in web pages or in a browser to allow users to obtain a rapid understanding of the policy without having to go through the "nutritional label privacy". In the studies carried out by Lorrie F. Cranor[46] on the users of the "Privacy Finder", it was discovered that creating points in terms of privacy, in this case by using green and white boxes, helped users to rapidly search sites with the best privacy policies, thereby influencing consumers' decisions as to where they could make purchases.

To conclude on this theme of maximum transparency regarding privacy policies, one must also take into account the "machine-readable privacy policy", which is none other than a declaration regarding the privacy practices of a website, such as the collection and use of data, written in standard programming language, which software tools like a consumer's browser can read automatically. For example, when the browser reads a "machine-readable policy" it can compare the policy for the preferences regarding privacy of the consumer's browser, and inform the consumer when these preferences do not correspond to the practices of the website being visited. If, for example, the consumer decides not to visit websites that sell information to third parties, they can set a rule that is able to recognize this type of policy, to block these sites and set a warning notice[47].

Accountability

Moving our attention to accountability[48], this should include two main objectives. It should promote a public understanding of the business system and also a certain level of trust in the system, and ensure an adequate level of protection for the consumer.

Today it is increasingly necessary and important that data controllers adopt efficient measures for a real protection of data and there are many reasons for doing this.

Above all, with respect to data we are witnessing a so-called "flood effect", with a constant increase in the amount of personal data existing, being processed and transferred. This phenomenon is favored both by technological progress, that is ongoing development of information and communication systems, and by the growing capacity of users to exploit technologies and interact with them.

With the growth in the quantity of data being transferred worldwide, also the risks of abuse increase. This further highlights the need for data controllers, in both public and private sectors, to put into effect real and efficient internal mechanisms to safeguard personal information.

[46] V. nota 45

[47] Cfr. FTC Staff Report, "Internet of Things, Privacy & Security in a Connected World", Jan.2015, pp 41-42.

[48] Cfr. Art. 32a, 33, 33a, 34, 35, 39 PGDPR-LIBE e Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability" (2010)

Secondly, the increasing amount of personal data is accompanied by an increase in their value in social, political and economic terms. In some sectors, particularly in the online environment, personal data have become de facto the currency of exchange for online contents. At the same time, from a social point of view, there is growing recognition of data protection as a social value. In brief, as personal data gradually become increasingly precious for data controllers in all sectors, also citizens, consumers and society in general are increasingly aware of their relevance. This fact in turn reinforces the need for applying rigorous measures to safeguard these data.

Finally, it follows from what has been said that violation of privacy may have notable negative repercussions for data controllers in the public and private sectors, with further repercussions in both economic terms and, above all, as regards reputation. Therefore, reducing as much as possible risks, building and maintaining a good reputation and guaranteeing the trust of citizens and consumers are becoming fundamental tasks of data controllers across all sectors. From this it emerges that there is an absolute necessity for data controllers to apply real and effective measures for data protection aimed at the correct management of their protection, but also reducing to a minimum juridical, economic and reputational risks which may stem from inadequate practices in this regard.

In brief, the data controller or processor must carry out an analysis of the risks of the potential impact of the treatment on the rights and freedom of persons[49] and appoint, when necessary[50], a data protection officer . In cases in which there are specific risks[51], the data controller must perform a "data protection impact assessment[52]", which must include the entire management of personal data from initial collection to cancellation. The assessment must be documented and a plan drawn up for periodical conformity checks regarding data protection. The assessment must be updated without delay on discovering any lack of conformity. Furthermore, on request, the data controller and processor must make this assessment available for inspection by surveillance authorities.

Therefore, the data controller must consult the data protection officer, or, in the absence of this position, a supervision authority, before beginning data treatment. The purpose is that of ensuring conformity of the data treatment foreseen by this regulation and a reduction in the risks for the interested party. This consultation must take place every time that an impact assessment indicates that, by virtue of their nature, content or purposes, the data treatments may represent a high degree of specific risk or whenever data protection officer or surveillance authority considers it necessary[53].

[49] Art 32 (a) (1) (2) PGDPR-LIBE

[50] Art 32 (a) (3b) PGDPR-LIBE

[51] Art. 32 (a) (3c) PGDPR-LIBE

[52] Art. 33 PGDPR-LIBE

[53] Art. 34 (2) PGDPR-LIBE

Finally, it may also occur that in order to reinforce the mechanism of transparency, a data controller may apply to any authority of the European Union, on payment of a limited fee, for a certification of the treatment of personal data, which attests conformity with the regulation on data protection, considering the obligations of who deals with the data and rights of the interested parties[54].

Final considerations: an "opt-out" scheme

Returning to the notice and consent model, we should add the consideration of the FTC121, which foresees those cases in which companies have no obligation to provide a choice for the consumer before the collection and use of their personal data.

These cases refer to transactions or consumer-company relations. In fact, as the uses of the data are generally coherent with the reasonable expectations of the consumer, the cost for consumer and companies in providing notices and choices exceed the benefits. This is a principle that also applies to IoT. Consider an example where a consumer purchases an intelligent oven from company X. The oven is connected with an app to the company which enables the consumer to switch on the oven remotely. If the company decides to use the consumer's usage information to improve the sensitivity of the temperature regulation, there is no need to offer the consumer a choice regarding this use. In this sense, the staff have incorporated certain elements of the so-called "use-based model" in the new approach to the notice and consent. The idea of associating the choices with the context takes into account how the data will be used. If the use is not coherent with the context of interaction (unforeseen use), the company does not need to offer the consumer a choice and vice versa. It being understood that the companies should not gather data without express consent. Furthermore, is a company allows the data collection of consumers and it de-identifies the data immediately and efficiently, a choice does not need to be offered to the consumer[55].

However, adopting only a used-based model for IoT is not the best solution. This is for a series of reasons. Use-based limitations have not been fully incorporated into legislation or into any other code of conduct and it is not clear who decides whether or not a data use is harmful. The limitations of use themselves do not address the risks regarding privacy and security created by the collection and expansive maintenance of data, since, as mentioned before, maintaining a great amount of data may increase the attractiveness of the company to the point of being a target for data violation. Finally, this model does not take into consideration the gathering of sensitive data originating from inferences among various pieces of data.

[54] Art. 39 PGDPR-LIBE

[55] For example the FCRA (Fair Credit Reporting Act) establishes a number of statutory protections applicable to information regarding " consumer relationship ", including restrictions on uses for which this information may be shared.

In conclusion, the new pillars on which the new model should be based refer to a rigorous multiple assessment of the impacts of data treatment. This must be ongoing throughout the life cycle of the product-services[56] and the adoption of di an "opt-out scheme".

In the presence of complex data processing systems or data gathering affected by lock-in effects, the assessment of risks and benefits should not be carried out by consumers or companies, but by third parties, under the supervision of the data protection authorities. Consumers must only decide whether to exercise their right to opt out or not.

Once the assessment has been approved by the data protection authority, the process is considered to be secure in terms of protection of personal information and of the potential social consequences. This is the reason for companies involving users in certain treatments, without prior consent, although they must be given a notice regarding the results of the assessment and they must be offered the opt-out option[57].

Therefore, from the user's point of view, on the one hand, there is a guarantee of assessment of the risks relative to data treatment thanks to the analysis carried out by the data protection authorities, and on the other hand, the opt-out enables users to receive information regarding treatment and to decide whether or not to consent to data collection.

It follows that this kind of model is more appropriate and gives more guarantees compared with the "notice and consent" model, which within this context is unreliable. It being understood that a solution to cover all fields within the new context as yet does not exist, the themes dealt with here are attempting to find the most well-balanced solution for facing the issue of privacy.

Conclusions

The subject matter has enabled us to reflect on the change in approach with which legislators are facing new technological challenges. This is particularly as regards privacy understood in its new interpretation as opposed to the classic "right to be alone". After briefly examining definitions and advantages originating from this new phenomenon, we moved on to deal with the aspect which technically distinguishes this new technology and consequently the associated problems.

However, the firm belief exists that there still remains a certain lag between the evolution of the Internet of things and the development of its legislative regulation.

We have underlined how the issue of privacy includes not only the concealment of personal information but also the capacity to control what is happening to that information. The attribution of tags to objects may not be known to users, and there may very well not be any kind of acoustic or

[56] Cfr. Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection frameworks", adopted on 30 May 2014.

[57] Article 29 Data Protection Working Party, "Opinion 06/2014" pp.45; art.19 PGDPR.

visual signal that draws the user's attention to the device. In this way, individuals can be followed unbeknown to them.

In order to limit this, a certain number of technologies have been developed, the so-called Privacy Enhancing Technologies (PETs). Briefly, these include:

- Virtual Private Networks (VPNs): extranets established by closed groups of commercial partners. This is a private telecommunications network, set up by subjects who use a public transmission system (e.g.: internet) as a transport infrastructure. Only partners have access to this network.
- Transport Layer Security (TLS): refers to cryptographic protocols which enable secure communication from source to destination (end-to-end), providing, among other things, the integrity and confidentiality of IoT data.
- DNS Security Extension (DNSSEC): uses cryptographic public keys to sign "resource records", in order to ensure the authentication and integrity of the information provided.
- Onion Routing: encrypts and mixes internet traffic from many different sources. The data are enveloped in various encrypted layers, using the public keys of the onion routers on the transmission route. This process impedes the correspondence of a particular source with an IP packet. The sender remains anonymous because any one intermediate subject only knows the position of the directly preceding nodes. On the other hand, there is an increase in waiting times which affect performance.
- Private Information Retrieval (PIR) systems: which enable a user to recover an element from a server possessing a database, without indicating which element is recovered, once EPCIS have been located. However, there are problems of scalability and key management, and also of performance in a globally accessible system such as ONS, which makes this method impracticable.

Another way of increasing security and privacy is peer-to-peer (P2P), which generally has good scalability and performance in applications. These systems could be based on Distributed Hash Tables (DHT). Access control, however, must be carried out on its EPCIS, not on the data memorized in the DHT. It is reasonable that the encryption of the connection and user authentication could be carried out without great difficulty, using a commonplace internet connection and web security services. In particular, client authentication may be done by means of the emission of "shared secrets" (data items known only to the parties involved) or by using cryptography of public keys. It is important that an Rfid tag, it being associated with an object, can be deactivated in a later phase, so as to enable the clients to decide if they wish to make use of the tag. Rfid tags can be deactivated or put into a protective " Faraday cage", impenetrable by radio signals of certain frequencies. The information on ONS is eliminated to protect the privacy of the owner of the tagged object, whereas the tag can be read, and therefore reveal further information. Furthermore, also transparency is necessary for identifiable non-personal information recovered by Rfid. An active Rfid may, for example, trace movements without identifying a person, who remains anonymous. However, it still remains to be seen whether or not this information not covered by privacy laws can be collected without further restriction.

Therefore, IoT is extremely vulnerable to attacks for various reasons. Firstly, because it may happen that its components spend most of the time unprotected, and are therefore easily open to physical attack. Secondly, most communications occur via wireless systems, and this makes interception very simple. Finally, most of the components of the Internet of things are characterized by low capacities both in terms of energy resources and ICT resources (an argument that is particularly valid for passive components). This means that they are unable to implement complex security schemes.

The solutions for data integrity should ensure that they are not modified during a transaction without the system detecting the change. The data can be modified while they are memorized in the node or while moving through the network. To protect the data after the first attack, the memory is protected in many tag technologies. For example, both EPCglobal Class-1 Generation-2 and ISO/IEC 18000-3[58] tags protect both reading and writing operations on their memory with a password. The first solution has five areas of memory, each of which can be protected in reading or writing with a totally independent password. The second solution defines a pointer (a type of data, a variable that contains the address in its memory of another variable) to a "memory address" and safeguards with a password all the areas of memory with a lower "memory address". To protect he data from the second kind of attack, the messages could be protected according to authentication of the HMAC (Keyed-Hash Message Authentication Code[59]) scheme. This is based on a common secret key shared between the tag and destination of the message, which is used in combination with a hash function to provide the authentication. It can be observed, however, that the above-mentioned solutions have problems when we consider Rfid systems. The password length, in fact, supported by most tag technologies, is too short to guarantee reliable levels of protection. If the length problem can be solved, there still remains the problem of management when entities belonging to different organizations are involved, as in the case of IoT.

[58] P.Talone, G. Russo, Standard e protocolli di comunicazione, Fondazione Ugo Bordoni, in http://www.rfid.fub.it/edizione_2/Parte_VI.pdf

[59] For technical considerations, H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997

Finally, it must be recalled that all the solutions proposed to support security take into account techniques of cryptography. Also in this case we must face the problem of the use of great quantities of resources in terms of energy and bandwidth, both at source and destination. In fact, in IoT, elements such as Rfid tags and sensor nodes are limited as regards energy, communications and calculating capacity. Consequently, a great research effort is required in this field. Privacy is exposed to a greater number of attacks because it is impossible to personally control the distribution of personal information, together with the reduction in the cost of information memorization. To this we can add that, compared to the traditional Internet, the issues of privacy arise also for those who never use IoT services. As a consequence, individuals must be safeguarded, guaranteeing a control over the data collected, and when this is done. Furthermore, the personal data gathered must be used only for the designated purpose authorized by the service provider and the data must be stored only for the time necessary for that purpose.

To manage the process of data collection, appropriate solutions are necessary in all the various subsystems that interact with individuals in IoT. For example, within the traditional context of internet services, the W3C group has defined the so-called "Platform for Privacy Preference" (P3P). This is a protocol that enables websites to declare the end use destination of the information gathered. A language is established for the definition of personal data management policies which is interpreted automatically and compared with the user's preferences, taking into account the management of the individual's data during the rest of their browsing activity.

For sensor networks the situation is more complex. A possible solution in this regard could be that of limiting the capacity of the Web to gather data at such a detailed level as to jeopardize the individual's privacy (for example in the case of CCTV, surveillance images can be blurred).

In the case of Rfid systems, the problem is twofold. On the one hand, the Rfid tags that are usually passive respond to query readers, irrespective of the owner's own volition. On the other hand, an ill-intentioned user can intercept the response from a tag for another authorized reader. Solutions for the first kind of problem, as we have already seen, are based on the authentication of authorized readers. However, these solutions require tags that are able to carry out authentication procedures, which, due to their nature, would bring about an increase in costs and the need to set up an authentication infrastructure, impossible to distribute in complex systems like IoT. Solutions proposed use a new system based on personal choices configured by the user. The decisions on privacy adopted by this system can be made by creating collisions in the wireless channel with the responses transmitted by the Rfid tags, which should not be read.

The interceptions by attackers in Rfid systems can be avoided through the protection of communications by means of cryptography, although this does not completely solve the problem.

So there is new family of solutions in which the signal transmitted by the reader has the form of a pseudo-noise. This signal is modulated by the Rfid tags and therefore, its transmission cannot be detected by ill-intentioned readers.

With the aim of guaranteeing that the personal data gathered are used only to support services authorized by the same providers, solutions have been proposed which are based on a system referred to as "privacy brokering". The proxy (a server which is placed between a client and a server with the role of intermediary or interface between the two hosts) interacts with the user on the one hand and with the services on the other. Consequently, it ensures that the provider obtains only the information strictly necessary from the user. The user can set the options of the proxy. When sensor networks and Rfid systems are included within the network, then the proxy operates between them and the services. However, in this case the individual can neither configure nor monitor the policies used by the privacy brokers. Furthermore, these solutions do have a problem of scalability.

It is worth noting, finally, that in order to face problems associated with an increase in the amount of data, also due to a lowering of memorization costs, there arises the need for new software tools which can delete the information that is no longer useful for the prearranged objective (e.g. "drop.io" and "Guest Pass" on Flickr).

The Internet of things has begun to revolutionize both the life of every single individual and also the classic social-juridical schemes of companies and public institutions. However, there is still a long way to go before reaching a legislative and regulatory framework which fully satisfies the effective needs of the society.