Privacy Risk in the IoT Environment: the Need for a Multiple Approach According to the GDPR Principles

Giovanni De Marco

Freelance Engineer - Data Protection Consultant
UNIDPO associate
Napoli, Italy
Email: gdemarco@demarcoconsulting.it

***Abstract*—The Internet of Things environment poses many problems of technological, socio-technical and legal nature. Many efforts have been made to solve the several technical challenges and issues arising from the peculiar characteristics of IoT devices, but none of them seems to be decisive at present. Moreover, the user's behaviour is almost always excluded from the premises of these approaches, causing them to be systematically weak towards non-proactive attitudes of end users. In particular, the relationship between risk awareness and the attitude towards privacy preserving behaviours seems to be undervalued. Outside of that, the centralized system on which common Internet devices work is not suitable in the IoT environment, asking for decentralized methods. Referring to the principles of the General Data Protection Regulation UE/679/2016 may be the key to a global approach to both the technical and non-technical challenges that the IoT environment presents. The objective of the paper is to delimit the problem's contours, as they emerge from the analysed technical, legal and sociological contributions, and therefore to propose an optimization of the management strategies for the protection of personal data in the Internet of Things ecosystem.**

Keywords–IoT; GDPR; Privacy by Design; Data Protection by Design and by Default; Privacy Risk Awareness

I. INTRODUCTION

Under the acronym IoT -standing for *Internet of Things*- are grouped several technologies from a vast variety of contexts and an ultimate definition of the ecosystem going under this term is not easy. An effective logical synthesis is given in [1]: *"an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfil a common goal."*. These devices are smart in the sense that they have (at least) one sensor and are capable of interacting with other devices, IoT or not IoT, connected to them via a network. IoT technologies have already started flooding our daily life, but their endemic diffusion is yet to come; should there be as much as 20 billions or 47 billions [2] connected devices in 2020, it will make no difference: the set of problems to be faced will be the same. This new kind of technology has distinct peculiarities translating into completely new sets of problems, related to their huge multiplicity, their pervasiveness and ubiquity and their primary function, i.e., gathering (personal) data from the physical environment. Consequently, the potential harm that the spreading of IoT devices can cause in terms of privacy and data protection is really high. Many efforts have been made to solve the several technical challenges and issues arising from the peculiar characteristics of IoT devices, but none of them seems to be decisive at present (see, for instance, [1]). Moreover, approaching these issues only from a technical point of view may be not effective, both because these problems are not only technical problems, and because the intrinsic dynamism of these technologies requires a structured strategy covering socio-technical and legal aspects alongside the technical ones. In particular, the relationship between risk awareness and the attitude towards privacy preserving behaviours should be taken into account. The paper is structured as follows: in section II the technical issues proper of the IoT environment are enumerated and legal requirements for data protection are analysed. In section III the focus is on the interaction between these new technologies and user's behaviour. In section IV a synthesis of the various aspects of the problem is presented and a proposal of management strategy compliant to the principles of the European Union *General Data Protection Regulation EU/679/2016* (GDPR) is suggested, as the key to a global approach to both the technical and non-technical challenges that the IoT environment poses. Finally, in section V, the critical points of the suggested strategy are underlined and the path to the future needed work is indicated.

II. TECHNICAL AND LEGAL ASPECTS

The peculiarities of IoT devices result in specific arguments to be addressed in order to keep this technological blossoming under control, in terms of practical usability, security and privacy protection; even if an exhaustive catalogue cannot be determined, due to the intrinsic dynamical and very varied nature of devices falling under the IoT category, the following can reasonably be the list of principal topics (see [3]-[5] for detailed analysis):

A. Physical and resource restraints

Particular types of IoT technologies, such as wearable devices or equipment designed to carry out tasks in contexts of high mobility and lack of sources of supply, are characterized by very limited physical resources [3][4]; reduced form factors implying small or no user interface and limited processing and/or supply power are very common features to many IoT products [6][7]. These limitations have immediate repercussions on the security aspects, since many consolidated strategies and techniques prove to be inapplicable due to lack of resources.

B. Heterogeneity and scale

IoT products are extremely various, in terms of field of application, conditions of use, physical and technical properties

 ISBN: 978-1-61208-721-4

[3], and their number will be unprecedented [6]. These peculiarities mean big challenges to be faced, such as an adequate network infrastructure able to manage an enormous number of connections and a robust frame to permit the correct interaction between very different IoT devices and between these devices and the infrastructure itself [4][5][8].

C. Authentication and confidentiality

The IoT ecosystem will be an overpopulated world blurring physical and virtual reality. In such a context the usual techniques of authentication lose any effectiveness and, in relation to the heterogeneity aspect, multiple solutions have been and will be implemented; thus, authentication and consequently confidentiality become a much bigger problem to manage compared to the usual Internet context [3][4][9].

D. Updating and accountability

Even though these two points can appear as fringe issues, their impact can be devastating, considering the huge number of devices and, hence, of manufacturers [10]. In the daily usage of the "common" connected devices, like desktop and laptop computers, tablets and smartphones, we take for granted the surveying of basic and application software and the consequent releases of patches and updates [11]. This is going to be even more true in the IoT environment, exactly because of the big heterogeneity of manufacturers and of products. In this scenario, accountability conflicts are an obvious side effect [3][12].

In various percentages, all these aspects contribute to give rise to threats for the personal data processed in the IoT environment; hence, one of the main goals to be achieved in the IoT ecosystem is to provide adequate *trust* strategies and practical solutions. As everything else in the IoT world, this question is very complex, too. For sake of simplicity, we will detect two macro-areas of relationships occurring in the IoT world: the trust of the end user towards the IoT system itself and the trust between different devices collaborating and exchanging data in the network. Both areas have been thoroughly examined in several researches, and many solutions have been proposed (see surveys [1][3]-[5][13]); the central point is that many of these works start from existing technologies and try their best to adapt them to the context of IoT.

The negative side effect of this approach is dual: first, many solutions developed for the "traditional" Internet security scenario, such as encryption protocols [3][4] or IP (Internet Protocol) standard addressing [8] are literally not suitable in the IoT context; second, and even more important, adapting some existing technique or paradigm in an effort to manage unprecedented challenges, as those posed by the IoT environment are, is in conflict with the principles of *Data Protection by Design and by Default*, prescribed in the *General Data Protection Regulation EU/679/2016* (GDPR, [14]) – Article 25.

As explained in [15], these principles are slightly different from the *Privacy by Design* (PbD) principle [16], since the approach adopted in the GDPR focuses on the data protection rather than on privacy. Nevertheless, without any prejudice towards this important distinction, the two concepts are strictly related; so to say, the prescriptions in Article 25 of the GDPR are in a child-parent relationship with the PbD, and, in this context, it's much more useful to focus on the common idea that connects them. In other words, any technical or organisational measure to be undertaken must have as a cornerstone the privacy protection itself. To be even more clear, and referring to the last of the 7 foundational principles of PbD [16], the *mantra* is ***keep it user-centric***.

GDPR compliant solutions should consequently consider, for instance, data preprocessing, i.e., data minimisation, data anonymisation and data pseudonymisation, as told in Recital n. 26, 28 and in Articles 25 and 32 of the Regulation, to reduce the risks *at source*. In any case, the cited countermeasures are not the only possible ones, since the Regulation describes them simply as some amongst many remedies. An important suggestion about further countermeasures to be undertaken comes from the *European Data Protection Supervisor* (EDPS) opinion on online manipulation [17], in which one of the biggest current problems in the context of cybersecurity is identified in the centralisation of personal data in few private hands: *"[...] Big data analytics and artificial intelligence systems have made it possible to gather, combine, analyse and indefinitely store massive volumes of data. Over the past two decades, a dominant business model for most web-based services has emerged which relies on tracking people online and gathering data on their character, health, relationships and thoughts and opinions with a view to generating digital advertising revenue. These digital markets have become concentrated around a few companies that act as effective gatekeepers to the internet and command higher inflation-adjusted market capitalisation values than any companies in recorded history."*. The endemic diffusion of IoT products is an obvious aggravating circumstance to these worries; hence, in a *proactive* approach [16], the decentralisation of databases is a fundamental criterion for data protection, in addition to the aforementioned countermeasures. Moreover, strictly related to the issues emerging from this EDPS opinion, there is another very important and challenging novelty introduced with the GDPR, i.e., the *right to be forgotten*, as per article 17 of the Regulation. The practical implementation of this new right of the data subject, i.e., the right to ask for (and to obtain) a complete and definitive cancellation of her/his data held by a specific data controller, would be largely facilitated and better granted by the use of decentralised databases in addition with anonymisation techniques, since a large part of personal data would be, in this scheme, stored locally rather than in a remote server managed by the data controller.

Nevertheless, it is very important to underline that the *ex ante* approach required by the PbD and embedded in the GDPR, is of crucial importance also when the trust problem in IoT is addressed in innovative ways, and thus the proposed solution is the effect of a fresh start. Starting from scratch does not lead, by itself, to achieve the goal: for instance an authentication system relying on the blockchain is *per se* compliant with the decentralization idea, being the blockchain an intrinsically decentralized technology; furthermore the example of the blockchain sounds particularly striking to address the trust management, given the capability of blockchains to ensure trust between participants without relying on a supervising authority. Nevertheless, a blockchain solution could reveal itself to be non-compliant with the PbD principles. For instance, in [18] a very interesting trust system for IoT is developed exploiting the blockchain technology; the

 ISBN: 978-1-61208-721-4

system hinges on "promises to be honored" between a *service provider* and a *service consumer*, and the "reputation" of each participant to the chain is brilliantly built up not only from the previous history already stored in the chain, but it is also linked to other trust indicators coming from external environment, so that a new participant to the chain is not obliged to start from "zero trust", but can inherit his (good) reputation from other contexts. All the transactions are encrypted *"[...] to provide confidentiality between the parties [...]"*, but the side effect of this *ex post* privacy countermeasure is that the encryption could also be exploited by malicious consumers to keep their bad reputation hidden; the problem is solved *"[...] publishing the obligations that were not fulfilled in an unencrypted form [...] and linking them to the previous encrypted ones."*. The result is that *"[...] all the non-fulfilled obligations are public."*, and this solution, since the non-fulfilled obligations have immediate negative impact on the reputation of the participant, is hardly acceptable, being the blockchain records immutable and not subject to any impartial trust agency, making it impossible to erase a potential *perp walk* effect caused by the disclosure of non-fulfilled obligations to all other participants.

Moreover, as explained again in [15], not all blockchain systems are compatible with the GDPR (only *private*, i.e. *permissioned*, blockchains and *combined* blockchains can be GDPR compatible) and this means that any measure developed without accounting these legal constraints will be almost useless in a global interconnected virtual market in which the GDPR becomes day by day the main normative reference. This one is far from being a secondary detail: there have been several works addressing the trust issue in IoT through the blockchain technology [19] but, unfortunately, those adopting *public*, i.e., *permissionless* blockchains are intrinsically non-compliant with the GDPR. The risk can be that some technically effective solutions may be implemented and spread, and possibly become established as reference solutions, while they cause in the approach itself a compliance problem.

III. Socio-Technical aspects

As we have seen, the security and trust challenges presented by the growing IoT ecosystem are really arduous; but there are even more problems to be taken into account. Let us refer to another concept expressed in [15], i.e., the fundamental relation:

$$security \neq privacy.$$

This inequality summarizes the real possibility of scenarios in which, despite the computer security countermeasures, no effective privacy protection has been achieved. From this point of view, the aforementioned examples are perfectly suitable.

Another remarkable and extremely concrete example of this kind is the so called *privacy paradox*; this expression refers to a recurring finding of several researchers: very often individuals who claim to be really concerned about their privacy, actually behave in strong contradiction with their statements [3][6][20][21].

As it is clearly understandable, such a phenomenon cannot be easily limited by standard security countermeasures of any kind, being it a disrupting attitude, capable of undermining the system from the inside. An end user who would correctly fulfil all the established security and trust criteria though behaving according to the privacy paradox, could however put her/his personal data under threat, considering that she/he acts with full privileges and authorizations: a perfect example of security without privacy. Furthermore, as stated in [6], the limited resources typical of many IoT devices, in combination with the huge scale of data exchange that we expect with the further diffusion of these technologies, can only worsen this gap between intentions and actual behaviour [22].

These socio-technical aspects seem to be at least as important as the strictly technical ones; in any case, it must be pointed out once more that the consideration of the behaviour of individuals when facing these new technologies is far from being totally clear. In [20], the complexity of these problems is well documented, and the intrinsic difficulty to identify the cause of the phenomenon is underlined. Some studies even question the actual existence of the privacy paradox [23], however, further and more recent evidence, and more strongly related to the IoT blossoming, suggests the contrary [22].

In any case, notwithstanding the fact that the privacy paradox phenomenon must always be estimated while taking into account all the biasing parameters, such as age [22], digital literacy and skills [6], convenience and context [20][24][25], a robust privacy protection strategy cannot afford to ignore it.

Moreover, these behavioural issues interact and intertwine themselves with other aspects of individual's behaviour in articulated technological environments, such as the *herding effect* [26][27], where, in a nutshell, individual's decisions are strongly biased by decisions previously taken by other subjects in a closed social group or category. As underlined in [6], the interaction between these two attitudes of the end users represents a serious threat to any security frame, being these weaknesses *outside* the security system.

As already said, in order to understand the nature of these phenomena, several works have addressed the problem; amongst various interesting aspects emerging from these works, three of them seem particularly relevant in the IoT context: the correlation between individual's digital skills and risk awareness [6][28], the correlation between individual's risk awareness and how coherent are her/his attitude and behaviour in terms of privacy [28] and the "privacy for convenience" mechanism [20][25]. In short, in the sociological literature a direct proportionality relation is detected between digital skills and privacy risks awareness [6]; furthermore, in [29]-[31] the relation between risk awareness and choices in terms of privacy is outlined. Even if no definitive results come out of these researches, the aforementioned aspects are very interesting clues to try to understand which the parameters favouring proactive user's behaviours are.

In addition, in [28], a further interesting assumption is made, i.e., that the incoherence of some behaviours can be explained with the concept of *privacy cynicism*: *"[...] an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile."*. The results of the study seem to confirm the hypothesis, and this sheds even more worries in view of the definitive diffusion of the IoT technologies. This research is also directly linked to other works, like [32][33], in which the tendency to ignore terms and condition of online services is underlined, and it results to be the standard behaviour; moreover the common experience of

the average user do aims to a substantial feeling of impotence, being the so called EULA (*End User License Agreement*) perceived as pretty mocking for their length and complexity [34]-[37]. On the Internet, it is even possible to listen for hours and hours to a guy reading some appliance's terms and conditions [38].

Last but not least, the trading of privacy for convenience must be considered in relation to the two previously remarked aspects. This mechanism, analysed in [39], is summarized by the authors stating: *"[...] small incentives, costs or misdirection can lead people to safeguard their data less [...]. Moreover, whenever privacy requires additional effort or comes at the cost of a less smooth user experience, participants are quick to abandon technology that would offer them greater protection. This suggests that privacy policy and regulation has to be careful about regulations that inadvertently lead consumers to be faced with additional effort or a less smooth experience in order to make a privacy-protective choice."*.

IV. Discussion

The scenario described in the previous sections is really complex and challenging, as well as worrying. The unprecedented number of devices that will more and more permeate our daily experience, their multiplicity and the consequent variety of ways of interaction pose very big issues to be solved, in order to have concrete benefits from the IoT ecosystem, rather than achieving an ungovernable myriad of devices collecting, transmitting, comparing and processing personal data without control.

In many cases, the problems are mostly technical [40], and it comes out that much better could have been done by simply applying basic security countermeasures, such as, for instance, data encryption. Nevertheless, the complex relations between new hyper-connected technologies and human behaviour pose even bigger problems. Many researches reveal disconcerting attitude towards the possible use and misuse of personal data widespread on the Internet, to the point where individual's behaviours become really difficult to understand and explain [41][42], but these events cannot be regarded as totally conscious and aware behaviours.

Once again, it is appropriate to refer to the GDPR principles and prescriptions in order to correctly address the whole set of problems. Besides the already mentioned principles of Data Protection by Design and by Default, we should consider another fundamental prescription of the GDPR, i.e., the necessity of a risk assessment for any potential harmful data processing in order to support the central concept of accountability of the data controller, on which the whole regulation hinges.

Indeed, the Data Protection Impact Assessment (DPIA) is a legal obligation under Article 35 of the regulation. This obligation, together with the Data Protection by Design and by Default principle, can be taken as a jumping-off point to imagine a solution, which may be seen as a natural application of the GDPR prescriptions.

- *Data management model in relation to privacy risks intrinsic to IoT technologies and compliance criteria to the privacy by design and privacy by default principles*

  Article 35, paragraph 1 of the GDPR prescribes: *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*. It looks pretty clear that this prescription does apply to IoT technologies; this means that any data controller dealing with IoT devices is obliged to undergo a DPIA process and to evaluate its results in order to comply with the EU/679/2016 Regulation. Moreover, in article 35, paragraph 7, is told that: *"The assessment shall contain at least:*

  (a) *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*

  (b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*

  (c) *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*

  (d) *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."*.

  In other words, an evaluation of the risk inherent in personal data processing intrinsic to the usage of an IoT device is necessarily included into any compliance process to the GDPR; the evaluation must detail and specify the techniques adopted in order to ensure personal data protection during the operation of the device. In this sense, amongst the DPIA results, the countermeasures put in place to respond to the basic principles of *privacy by design and by default* must also appear. All these DPIA outcomes can be stored in a database managed by a third party Authority (it could be, for instance, the EDPS, or a further Authority related to the EDPS). In this way, any (new) IoT device would be automatically classified and archived in this public database, and, alongside the device, the database would register the details of the risk level for each processing and of the countermeasures implemented to mitigate those risks; the crucial task of the managing Authority would be the harmonisation of each device's DPIA results, so to have an evaluation scale as homogeneous as possible. Something similar already happens with many privacy-friendly services, such as, for instance, the *DuckDuckGo* browsing service [43]; however, in order to ensure real impartiality, the involvement of a supervisory Authority appears necessary, as was the case, for example, with the *Privacy Flag* project [44]. The harmonization process is for sure a critical point of the whole management strategy; nevertheless, in accordance with Articles 40 et seq. of the GDPR, the diffusion of common *codes*

of conduct could be the shared background on which to build a widely supported reference frame for the comparison of different services and devices in terms of privacy risk. Indeed, respecting determined codes of conduct approved by the EDPS, would mean, by itself, ensuring the compliance to well known, shared and detailed data protection criteria.
For how much it concerns, instead, possible cases of unreliable or untruthful DPIAs, they come under the more general casuistry of infringements of the GDPR, and they must be treated as breaches of the accountability principle; in the same way, here is not considered the extreme case in which the use of a prior consultation is needed (article 36 of the GDPR).

- *Basic risk mitigation criteria*
  Given that a detailed description of each specific situation would be unachievable, precisely because of the already examined extreme heterogeneity of the IoT ecosystem, it is, in any case, possible to identify two macro-categories: indoor devices and outdoor devices. For devices belonging to the first category, they will, in almost all cases, be connected to a trusted Local Area Network (LAN); thus, for these equipments, the basic criterion for risk reduction must include the implementation of strict anonymisation and/or pseudonymisation procedures which, together with the use of a local database for data storage, must lead to a standard for the transmission of data outside the LAN on the basis of which only data rendered appropriately anonymous must be able to reach the central management server of the device. In other words, inside of the trusted LAN the user's personal data are normally processed in order to safeguard the quality of the service provided through the device and its customization by means of the progressive learning of user's tastes and preferences, so that the appeal and the convenience of the specific IoT device are not compromised. On the other hand, only data made anonymous according to the techniques indicated above will be sent to the main external server of the considered equipment, thus safeguarding the possibility, for the manufacturer, to carry out statistical processing on the data processed by his own devices, but in anonymous form. For the second category, namely that of outdoor devices, the problems are greater, as they cannot rely on the support of a trusted LAN. However, there is nothing to prevent from reproducing the previous scheme by sending user's personal data to a private server, that is to say inside of the user's trusted LAN; at this point an application related to the device and operating locally in the trusted LAN, provides for the anonymization and/or pseudonymisation of the data and the subsequent sending of the data made anonymous to the central server of the device. Alternatively, a second personal device could play the role of the trusted LAN and of the local storage space, for instance taking advantage of a smartphone generated Personal Area Network (PAN) or through some other sort of short range connection between the IoT device and the user's smartphone. In addition, for such equipment, the default setting should provide for the deletion of all data whose sharing with the central server of the device is indispensable for the use of the service itself (e.g., geolocation data in the navigation devices) at the end of every single usage. This kind of data processing policy would be of great help also to fulfil the obligations in terms of *right to be forgotten*. These countermeasures obviously have nothing to do with the security issues of data transmission, which must be addressed and resolved beforehand, so that this granular privacy management system can be based on a solid foundation of computer security, avoiding incurring cases like that illustrated in [40]. For instance, symmetric cryptography could be the right choice due to cost and power restraints [7], and an OTP (One Time Password) second security level may be the solution to improve security by pairing the IoT device with the user's smartphone. However, this aspect has no trivial solution, given that, as already mentioned, IoT devices are almost never suitable for the application of standardized security methods due to their limited resources; therefore this aspect must certainly be deepened, although this deepening goes beyond the scope of this contribution.

- *Real time signalling of the risk level based on the settings in terms of protection of personal data of the device*
  As already seen, to obtain adequate levels of protection of personal data it is absolutely essential to take into due account the behavioural aspects of the end user. From what we have seen in section III, it appears necessary to implement a mechanism that, with immediacy and without interfering with the functions of the device, is able to signal in real time to the user the level of risk to which the user is exposed. Furthermore, this indicator must take into account all the possible modifications to the device settings that impact on data protection, so that the signalling changes instantaneously and consistently according to the specific settings chosen, so to allow the user an effective, rapid and conscious balancing between practicality of use and risk for personal data. In consideration of the scheme illustrated in the previous two points, this can be achieved through a chromatic signalling system on board the device, or shown through an application specifically related to the device, by correlating to each different setting of the personal data management parameters (which is normally a possibility already included in almost all network devices or applications) a different colour signal. For example, imagining a scale on five levels, you would have:
  (1) Bright green: high personal data protection level and privacy safeguarding.
  (2) Yellow-green: medium-high personal data protection level. Good privacy safeguarding.
  (3) Yellow: medium personal data protection level. Privacy safeguarding acceptable: some risks.
  (4) Orange: medium-low personal data protection level. Privacy safeguarding weak: significant risk.
  (5) Red: low personal data protection level. Bad privacy safeguarding: high risk.

 ISBN: 978-1-61208-721-4

The scale can obviously be deepened by adding more levels and the corresponding colour nuances beyond these five sample levels. This dynamic signalling system would allow the user to choose the balance point between practicality of use and data protection that best suits her/his needs. In other words, with reference to the previous point, the level of protection chosen may or may not include anonymisation as well as automatic deletion of navigation data, but these choices, accompanied by the corresponding signal indicating the level of risk, would certainly be more aware, even in the case of "unscrupulous" users who, knowingly, choose the most dangerous settings for the protection of their personal data.

In this way, associating in real time with each change in the settings a signal of the corresponding level of protection of personal data, it is possible to actively oppose the tendency of users to yield to the dynamics of *privacy for convenience*, which, as the literature on this topic shows, are often not very conscious dynamics because of the lack of perception of the risks to which the users are exposing themselves. Such a privacy risk management frame, explicitly thought to maximize the protection of user's data, could nevertheless be of great convenience for the manufacturers too, since any choice made in a context of maximum understandability of the privacy risk could hardly leave room for litigations seizing on the lack of awareness. In other words, an increase in user's privacy risk awareness can be the most effective strategy not only to let individuals make their choices in the most conscious way, but also to build up a proactive environment involving users and manufacturers, in order to reduce the sense of impotence in front of personal data violations and misuses that, in the long term, could ultimately bring to a "lose-lose" situation, into which, obviously, no one would be glad to get.

Nevertheless, the obvious premise to all these considerations is the compliance to the GDPR and the fair play of all manufacturers and players in the cyber-market.

V. Conclusion and future work

The IoT technologies are expected to become a pervasive aspect of the life of us all in the very near future. Its special characteristics, such as the unprecedented number of devices, their ubiquitous nature and the capability of making virtual and physical world blur together, outline an intrinsic duplicity in this incoming revolution: it promises to drastically transform our way of living, but it also poses threats to the privacy of us all end users as never before. The profound interaction, almost a symbiosis, between IoT devices and the surrounding world, including human beings, forces a multiple approach in order to frame the problem and then have chances of solving it; in this regard, the principles stated in the GDPR appear even more as the correct guidance to lead the way. Waiting for ambitious, visionary and fascinating projects of self-protecting personal data to come true [45], we need to develop right now an effective strategy to manage this paradigm shift.

This contribution proposes a general strategy of approach to these problems which puts the respect of norms on the protection of personal data, first of all the GDPR, above the identification of technical solutions. Moreover, the strict interaction between IoT technologies and human beings also means a strict interaction between user's behaviour and personal data protection, this reflecting itself in the need of integrating, into the technical solution, practical and effective signalling of the risks to which the user is exposed when using a specific IoT device or equipment. The proposed strategy tries to solve these problems by means of rearrangement and optimisation of already existing technologies and solutions. The legal obligation to undergo a DPIA is a very important starting point, since, at least in markets in which the data protection regulation is the GDPR or a *GDPR like* regulation, it can be the starting point on which to build the crucial component of the strategy proposed, i.e., the existence of a common standard for the evaluation of risk levels between different IoT devices. As already underlined, this task should include the involvement of a supervisory Authority to ensure the necessary level of impartiality for all parties involved; nevertheless, the current panorama already offers systems that compare various services in terms of privacy protection, and these examples can act as a reference point for a comparison platform as broad and shared as possible. Hence, amongst many possible and needed next steps to be made, two appear more urgent: the development of a prototype application which implements the signalling system taking into account any possible configuration of the data parameters of a significant selection of IoT device, and the testing of this prototype application in therms of usability and risk awareness increase on a sample of users.

Acknowledgment

The author would like to sincerely thank the reviewers for the great help given. Their ability in highlighting critical points and in indicating all necessary modifications has been decisive to improve this contribution.

References

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porosini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, 2015, pp. 146–164.

[2] "IoT numbers vary drastically: devices and spending in 2020," 2017, URL: https://www.wespeakiot.com/iot-numbers-devices-spendings-2020/ [retrieved: may, 2019].

[3] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, no. 2, 2017, pp. 155–184.

[4] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of network and computer applications, vol. 42, 2015, pp. 120–134.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, 2015, pp. 2347–2376.

[6] M. Williams, J. R. C. Nurse, and S. Creese, "The Perfect Storm: The Privacy Paradox and the Internet-of-Things," in 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 644–652.

[7] K. A. RafidhaRehiman and S. Veni, "Security, Privacy and Trust for Smart Mobile devices in Internet of Things – A Literature Study," IJARCET, vol. 4, no. 5, 2015, pp. 1775–1779.

[8] H. Ma, "Internet of Things: Objectives and Scientific Challenges," Journal of Computer Science and Technology, vol. 26, no. 6, 2011, pp. 919–924.

[9] "Internet of Things Security and Privacy Challenges," 2018, URL: https://reolink.com/internet-of-things-security-privacy-challenges/ [retrieved: may, 2019].

[10] "The Internet of Things will be vulnerable for years, and no one is incentivized to fix it," 2014, URL: https://venturebeat.com/2014/08/23/the-internet-of-things-will-be-vulnerable-for-years-and-no-one-is-incentivized-to-fix-it/ [retrieved: may, 2019].

 ISBN: 978-1-61208-721-4

[11] "IoT Security Upgradability and Patching," 2016, URL: https://www.ntia.doc.gov/files/ntia/publications/ota_ntia.pdf [retrieved: may, 2019].

[12] "IoT and Blockchain Convergence: Benefits and Challenges - IEEE Internet of Things," 2017, URL: https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html retrieved: may, 2019].

[13] A. S. Neeraj and A. Singh, "Internet of Things and Trust Management in IoT - Review," IRJET, vol. 03, no. 6, 2016, pp. 761–767.

[14] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ," 2016, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [retrieved: may, 2019].

[15] N. Fabiano, "Internet of things and blockchain: Legal issues and privacy. the challenge for a privacy standard," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, Jun. 2017, pp. 727–734.

[16] A. Cavoukian, "Privacy by Design The 7 Foundational Principles," 2016, URL: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf [retrieved: may, 2019].

[17] "Opinion3/2018EDPS Opinion on online manipulation and personal data," 2018, URL: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf [retrieved: may, 2019].

[18] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the internet of things," in Proceedings of the 23Nd ACM on Symposium on Access Control Models and Technologies. ACM, Jun. 2018, pp. 77–83. [Online]. Available: http://doi.acm.org/10.1145/3205977.3205993

[19] X. Zhu and Y. Badr, "Identity Management Systems fot the Internet of Things: A Survey Towards Blockchain Solutions," Sensors, vol. 18, no. 12, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/12/4215

[20] S. Barth and M. D. T. de Jong, "The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review," Telematics and Informatics, vol. 34, no. 7, 2017, pp. 1038–1058.

[21] "The EMC Privacy Index," 2014, URL: https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf [retrieved: may, 2019].

[22] M. Williams, J. R. C. Nurse, and S. Creese, " *"Privacy is the boring bit"*: User Perceptions and Behaviour in the Internet-of-Things," in Proceedings of the 15^{th} Annual Conference on Privacy, Security and Trust (PST) Aug. 28–30, 2017, Calgary, AB, Canada. IEEE Computer Society, Aug. 2017, pp. 181–190, ISBN: 978-1-5386-2487-6.

[23] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors," European Journal of Social Psychology, vol. 45, no. 3, 2015, pp. 285–297.

[24] A. Gambino, J. Kim, S. S. Sundar, J. Ge, and M. B. Rosson, "User disbelief in privacy paradox: Heuristics that determine disclosure," in Proceeding of the 2016 CHI Conference Extended Abstracts. ACM, May 2016, pp. 2837–2843.

[25] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," Computers & Security, vol. 34, Jan. 2015, pp. 122–134.

[26] H. Sun, "A longitudinal study of herd behavior in the adoption and continued use of technology," MIS Quarterly: Management Information Systems, vol. 37, 12 2013, pp. 1013–1041.

[27] Y. E. Huh, J. Vosgerau, and C. K. Morewedge, "Social defaults: Observed choices become choice defaults," Journal of Consumer Research, vol. 41, Oct. 2014, pp. 746–760.

[28] C. P. Hoffmann, C. Lutz, and G. Ranzini, "Privacy cynicism: A new approach to the privacy paradox," Cyberpsychology: Journal of Psychosocial Research on Cyberspace, vol. 10, no. 4, 2016.

[29] L. M. Coventry, D. Jeske, and P. Briggs., "Perceptions and actions : Combining privacy and risk perceptions to better understand user behaviour," in Symposium on Usable Privacy and Security (SOUPS) 2014. USENIX Association, Jul. 2014, pp. 443–457.

[30] I. Oomen and R. Leenes, Privacy Risk Perceptions and Privacy Protection Strategies. Springer, 05 2008, vol. 261, pp. 121–138.

[31] L. Shepherd, J. Archibald, and I. Ferguson, "Perception of risky security behaviour by users: Survey of current approaches," in Human Aspects of Information Security, Privacy, and Trust: First International Conference, HAS 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings, vol. 8030. 0302-9743, 07 2013, pp. 176–185.

[32] Y. Bakos, F. Marotta-Wurgler, and D. R. Trossen, "Does anyone read the fine print? consumer attention to standard-form contracts," The Journal of Legal Studies, vol. 43, no. 1, 2014, pp. 1–35.

[33] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services," Information, Communication & Society, vol. 0, no. 0, 2018, pp. 1–20.

[34] "How Silicon Valley Puts the 'Con' in Consent," 2019, URL: https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html [retrieved: may, 2019].

[35] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," A Journal of Law and Policy for the Information Society, vol. 4, no. 3, 2008, pp. 543–568.

[36] "You're not alone, no one reads terms of service agreements," 2017, URL: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [retrieved: may, 2019].

[37] "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," 2012, URL: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [accessed: 2019-03-04].

[38] "Here's nine hours of a guy reading the entire terms and conditions for the Amazon Kindle," 2017, URL: https://news.avclub.com/here-s-nine-hours-of-a-guy-reading-the-entire-terms-and-1798259191 [retrieved: may, 2019].

[39] S. Athey, C. Catalini, and C. Tucker, "The digital privacy paradox: Small money, small costs, small talk," National Bureau of Economic Research, Working Paper w23488, Jun. 2017.

[40] "European Commission orders mass recall of creepy, leaky child-tracking smartwatch," 2019, URL: https://cyware.com/news/european-commission-orders-mass-recall-of-creepy-leaky-child-tracking-smartwatch-e61468b3 [retrieved: may, 2019].

[41] J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini, and R. de Oliveira, "Your browsing behavior for a big mac: Economics of personal information online," in Proceedings of the 22Nd International Conference on World Wide Web. ACM, May 2013, pp. 189–200. [Online]. Available: http://doi.acm.org/10.1145/2488388.2488406

[42] "Amazon Key asks users to trade privacy for convenience," 2017, URL: https://money.cnn.com/2017/10/26/technology/business/amazon-key-privacy-issue/index.html [retrieved: may, 2019].

[43] "DuckDuckGo," 2019, URL: https://duckduckgo.com/ [retrieved: may, 2019].

[44] "The Privacy Flag Project," 2019, URL: https://privacyflag.eu/ [retrieved: may, 2019].

[45] G. J. Tomko, D. S. Borrett, H. C. Kwan, and G. Steffan, "Smartdata: Make the data "think" for itself," Identity in the Information Society, vol. 3, no. 2, 2010, pp. 343–362.