ENHR 2021
Conference Proceedings

European Network for Housing Research

Sustainability and The Smart Home: The Challenges of an Interconnected Environment

Francesca Gennari, PhD student
Mykolas Romeris University, Last JD RIoE, Ateites st, 2008303, Vilnius, Lithuania
e-mail: frgennari@stud.mruni.eu

Abstract

This paper would like to be a bridge between technical and legal knowledge as far as the construction of environmentally sustainable and privacy compliant homes is concerned. Uniting data protection law as the leading legal subject guiding us through the Digital Revolution with the SDG30 objectives is already the preferable option for housing in unsettled times like the ones we are living. This paper will analyse the actual weakness of the current smart home from a data protection point of view and will argue that the principle of privacy by design and by default is already influencing new techniques that could fix the Internet of Things (IoT) paradigm from within. It is wished that the interdisciplinary collaboration between legal scholars and technical experts becomes stronger as regulation will never be able to keep up with the pace of technology.

Keywords: smart home, sustainability, IoT, environment, housing

Introduction

Summer 2021 showed us once more that climate change is real and unsettling: fires and floods all over Europe and the world are just the tip of the iceberg. How the smart/connected/ IoT home can help stopping Nature’s deterioration while ensuring comfort and the respect of human rights, especially data protection and privacy, is the question that this paper aims to answer or, at least, to provide useful insights to any relevant stakeholder.

In order to do that, it is necessary to have a brief and succinct outline of the structure of the argumentation. Firstly, I will deal with the methodological issues: my aim is to try to find a balance between the observation of technological feeble points of the smart home and the relevant legal background. Secondly, I will restrict my analysis to the European Union (EU) because of the first-hand knowledge of its legislative acts and, because, as I intend to deal with data protection law, the General Data Protection Regulation is an inspiring legal model recognised worldwide.

After pinpointing the main data protection problems of the current smart home, the constructing part of this paper will develop from a quite simple idea: law and technology need to be combined in order to make the smart house a sustainable and empowering reality for people. On the one hand there will be the analysis of some technological developments of the home IoT, such as Edge Computing and Distributed Ledger Technologies (DLT) protocols for the connected home and how these innovations can accommodate data protection concerns. On the other hand, studies in the new Green IoT are having a momentum and could be an important connection between environmental sustainability and data protection in the smart home.

In conclusion, it will be argued that building a sustainable smart home is indeed possible, but there must be a close cooperation between legal and technical disciplines, otherwise a smart home could do more harm than good.

The Actual Smart-Home. A Dream Becoming Reality?

In this first part, the technical state of the art will describe what the Internet of Things (IoT) paradigm implies and its connection to the smart house. Subsequently, there will be an explanation about why the smart house is still not a widespread reality today. In the second part of this section there will be a brief outline of the two main legal instruments that I will use throughout my analysis. On the one hand the Sustainable Development Goals 2030 (hereinafter SDG30) and, on the other hand, the General Data Protection Regulation in the EU (hereinafter GDPR).

Technical Issues and State of the Art: How an Interconnected Environment Works

When referring to the smart/connected/ubiquitous home (I will use these terms almost interchangeably as for law scholars the differences among these terms are not substantial) it is important to refer to the IoT paradigm as a general way to explain the functioning of an interconnected environment, such as a smart home.

Since its first concretisation in 1999 by K. Ashton, the IoT has been one of the most adaptable technologies. There are still several definitions of IoT but more and more authors, although with some personal differences, are transitioning to a concept of seeing the IoT paradigm as an enabling set of technologies for more complex ones such as Artificial Intelligence (AI). The IoT thus relies on many ‘supporting technologies’ such as sensing, software, communication, networking, and information technologies, but it will become more and more an infrastructure connecting the digital to the physical world and vice versa. It is true that the IoT paradigm was derived from studies in the RIFID technology, but, maybe, the union between the words Internet and Things will never lose its ‘fuzziness’ entirely.

In short, we could say that the IoT is an ensemble of sensors, actuators, gateways, antennas, electromagnetic waves, cloud and networks that is able to create a connected environment, such as a smart home. A connected environment is a smart environment in the sense that its parts can learn from each other and interact not only among themselves but with users. Moreover, these connected objects can learn from users too and adapt their functions accordingly.

From a technical point of view, however, most literature agrees on dividing the layers of the IoT in three parts: *i)* perception (physical) layer, which is the one of the object that the user; *ii)* network layer which is responsible for the connection with other things and *iii)* the application layer, through which the user interacts. However, there exists even four, five and seven layer models. They are less used as they are quite complicated to use. It is interesting to notice that legal informatics scholars tend to rely on a three layers’ model as well but taking the perspective of the network that the IoT creates, thus labelling the layers in the following way: ‘level of basic connectivity; level of network interoperability and level of syntactic interoperability’, which correspond more or less to the three technological layers mentioned before.

Nevertheless, the IoT is a ‘general’ technology that can be adapted to many different fields (from healthcare to transportation, from housing to industrial manufacturing). What is generally specific to the smart home is that there are sensors (standalone or in devices) that should allow the gathering of data. Then, data is sent through a gateway (which can be both a physical but also a digital device), and then is sent to the cloud (or proprietary network) where data analytics techniques known as processing (e.g. Machine Learning) analyse it. Subsequently, a new input is sent back through the same route in the opposite direction and the IoT object might respond and interact thanks to the use of actuators. At the moment, however, there is not such a thing as a completely connected home: there exist different smart objects which can more or less connect to the same network but that do not always cooperate with each other. So ‘the ubiquitous home’ days as derivation of ubiquitous computing have not come yet.

It is interesting to know that the concept of smart house was indeed foreseen before the development of IoT technology. The first ideation of the smart home as the *non plus ultra* of luxury housing dates back to the 1930s. However, the first prototypes of interconnected home environments (mainly for experiments in assisted living) started to be built in the 1990s in Japan and in the US. The reasons for which the connected house is not yet a widespread reality are several. In the past, it was because of the high costs of any kind of connected/automated object and, more generally, because of the lack of a sufficient quantity and quality of computational power. Nowadays, the lack of common protocols among the different objects, sensors and applications (even though things are evolving under this aspect) and of a homogeneous 5G infrastructure are among the most important reasons because of which there is not a widespread presence of smart homes.

Legal Methodology

The possibilities to make the smart home a powerful driver in the implementation of equality for housing and for ensuring human rights seem to be quite apparent: if we take objective SDG30 n. 2 (good health and well-being) quite a lot of wearables IoT can already connect inside the house and there are several rehabilitation pilot programs to conduct from an environment (their home) that the users consider safer than a general hospital, especially during a pandemic.

Moreover, in recent years there have been several ‘assisted living’ pilot projects with the function to provide help for elderly or disabled people. This would foster the way to reach objective 11 (sustainable cities and communities). Moreover, if the connected environment can ‘learn’ from its inhabitant’s habits, it can make objective 13 (climate action) reachable through the management of clean energy, if these smart objects are coupled with renewable energy sources for the house (objective 7). Overall, smart homes can inspire people to have a more responsible approach to consumption and daily habits (objective 12).

The SDG30 objectives are important policy instruments but they are general and they are considered as part of ‘soft law’. Even though states decided to respect them, there is a lack of coordination and binding nature of these objectives. With the Next Generation EU (hereinafter NG EU) plan in the EU, each Member State (MS) has rules to follow in order to implement the Green Deal objectives, which are inspired from the SDG30 ones. For housing, great expectations were born from the presentation of the New Consumer Agenda and from the launch of the Bauhaus initiative to rebuild more energetically sustainable buildings and infrastructures.

However, at the moment of writing, the MS are still in the process to see each of their NG EU plans approved and there is no guarantee about a common and efficient approach to follow sustainability and technological rules for housing.

Despite that, I argue that the General Data Protection Regulation EU 676/2016 (GDPR) can become a truly effective vehicle in making access to housing more environmentally sustainable and fairer while waiting that all the aforementioned policy and legislative instruments become effective in the EU.

Methodologically, I decided to restrict the field of investigation to the EU regulation not only because of the first-hand experience I have of it, but also because it addresses a human right that the SDG30 do not single out explicitly but that is of fundamental importance when talking about technology: I refer to data protection. Data protection law is the field of legal studies that is absorbing part of what was considered as consumer law as more and more objects and tools we use are somehow connected. It is assumed that along with an attention to environmental issues, the near future will also investigate how technology can help to attain environmental sustainability.

Furthermore, the selection of the European approach to regulating data protection is motivated by the diffusion and influence the GDPR has had all around the world. In fact, the State of California, Brasil, Japan, South Korea and Switzerland (among many others) got inspired by this regulation which can therefore provide a *fil rouge* when discussing about data protection all over the world. A reason for its success is that it tries to balance fundamental rights protection with a risk assessment *rationale*.

Legal Issues in The Smart Home

The functioning of the smart house described previously and how the IoT and cloud technology operate put into focus two technical phenomena *i)* the first one is described as data deluge. It means that the quantity of inputs that are created and received even in a closed connected environment such as the smart home are way too many. This has consequences on the differences between the personal and non-personal data distinction and how to ensure the respect of the GDPR data minimisation principle; *ii)* the IoT and smart-house model just appears to be close to the user. On the contrary, the smart house paradigm as it is built today is founded on the reliance on the cloud, where the most important processing and data analysis phases are carried out. This is a weak point not only under a cybersecurity perspective but also under a legal one, especially when we are thinking about liability issues in a very complex chain of stakeholders

What Is Personal in an IoT Environment?

The GDPR is the EU regulation that deals with personal data. Despite the definition of personal and non-personal given at Article 4.1 GDPR seems to be straightforward, the legal scholarship has pointed out some relevant issues. The first thing is that the definition of what is personal according to the regulation is not just limited to what is proper of a certain individual. It expands and considers personal also what is just a means to make a certain person identifiable. The reason of this drafting lies in the respect of previous judgements of the Court of Justice of the EU (hereinafter CJEU). The CJEU adopted this view in order to protect fundamental rights of individuals and, for example, in one occasion it even considered IP addresses as personal data. However, it has been pointed out that this large definition of 'personality' is also given because what is personal is time and context dependant. For example, at the beginning of the 2000s, the ZIP code was not primarily considered as something personal, whereas in recent years it was used in combination with other data (personal and indirectly personal) to infer personal information about people (such as their income and if they were part of minorities or not). In the house there are several kinds of data that will be interested and that belong also to more sensitive, hence more protected, groups of personal data, such as data concerning health and biometric data (see Article 9.1 GDPR). These kinds of data can be processed only under specific exceptions, which can be found at Article 9.2 GDPR. These protected groups of personal data are also among the mostly used in our IoT home. Let us think about our face image used as a security key to unlock doors and smartphones, or our smart-watch, taking our heartbeat and syncing it with other smart gym furniture that we might have in the house. The hypotheses are already many right now and they will not stop growing in the near future.

Consequently, if data is personal, the producer of the device will have to respect several obligations and will have to carry out specific duties to ensure their protection (see Section 2 of Chapter 4 GDPR). This is understandable, but, if we consider that the majority of data is personal there can be some unwanted consequences for businesses: a very broad definition of personal data does not encourage innovators to invest in a field such as the IoT one, as the costs and risks in case of data breach (data leakage in technical parlance) could outweigh the profits.

Data Collection v. Minimisation Principle and Who is Who In The Data Processing Phase

In the last subsection we mentioned briefly the duties that the producer of the IoT device has according to the GDPR. In GDPR parlance, the producer or main manufacturer is the data controller as it needs to collect data for its activity (see Articles 4.7 and 27 GDPR). The data controller has not only several compliance duties to ensure (such as the safety and security of the data processing and the drafting of a data protection impact assessment), but does also have to ensure the respect of fundamental rights principles while processing personal data (and within an interconnected environment it can be challenging).

In the GDPR, processing basically encompass any operation on personal data both in digital and in a non-digital way (Article 4.2 GDPR). Article 5.1 GDPR lists the principle concerning processing and one of the most important ones is the principle of minimisation of data collection and processing

(Article 5.1c GDPR). Commentators have advocated for a contextual approach when applying this principle, meaning that the quantity of personal data gathered needs to be the least possible. This is done by taking into account the specific circumstances of the case. However, ascertaining this ‘permissible level of data collection’ in an interconnected environment such as the IoT smart house is not that simple even now when smart houses are not so diffused.

As a matter of fact, the IoT paradigm on which the modern concept of smart house is built is based on collecting as much data as possible. This is because the more data is obtained, the more can be sent through the gateway in the cloud, analysed and used for ‘feeding’ Machine Learning (ML) models, and then sent back to IoT home objects to perform better, to adapt to new situations and requests from their users.

Moreover, quite often, it is not the data controller which performs these operations, but the data processor. In theory, the data processor (Articles 4.8 and 28 GDPR) has a more instrumental and operative function than the controller (this is also reflected from a reduced responsibility at Article 24 GDPR but not from liability which is regulated at Article 82 GDPR). Concretely, the data processor can be a contracting software agency that handles the whole or a huge part of the processing phase and thus might be the first stakeholder responsible for a personal data breach in the sense of Article 4.12 GDPR. However, the stakeholder which will respond concretely (meaning, paying compensation) is the controller, because it has delegated part of its functions to the processor. However, if it is the processor which acted with a level of negligence that could not have been expected, it is unfair that the controller has to pay for everything.

Another problem might arise and it is partly connected to the difficulty in establishing who is who in a smart home. In the near future, with the progression in sharing interoperability and internet protocols among several IoT domestic objects, it could happen that different objects start communicating among themselves sharing inputs and maybe personal data. At that point, it will be complicated to also ascertain responsibility/liability whenever a substantial damage arises: if two IoT producers (who are respectively controllers for the data gathered by their products) find themselves as joint controllers for a damage caused by two interoperable IoT objects, what should they do? The GDPR does allow joint controllership for personal data processing, but in order to do that it is indispensable that there is a written agreement (Article 26 GDPR). It is argued that in the future, with the possibility of IoT objects connecting spontaneously without the data controllers knowing about it, the lack of this written joint-controllership document can establish a further title of liability for IoT producers and discourage investment from this area overall.

The Processing: Still Too Far from The User

The last important element in this synthetic overview of the clashes of modern domestic IoT technology with GDPR is that the cloud system on which the home IoT objects rely on is not transparent and it is also far from to the users. Knowing the full width of consequences after giving an IoT object consent to operate with our data (personal or non-personal) can be problematic even for people who know more than average about these matters.

Moreover, recent scandals and data breaches (from Cambridge Analytica onwards) have made EU citizens warier of what they do on the Internet. Furthermore, the relatively low price for which one person can buy these new domestic objects is not always accompanied by a sufficient level of cybersecurity of the object itself.

What I argue is that this IoT cloud centred paradigm has to change as soon as possible for several reasons. Firstly, if users are granted to have control and they can rely on relative proximity (e.g. within a possible EU cloud or in a MS server) to the place where their data is being stored and processed, the market could flourish more. This would happen because people would trust IoT technology more. Secondly, enhancing data proximity and data control would produce a lesser quantity of energy. It could allow the future entirely connected smart house to be more self-sufficient from an energy point of view. Lastly, having data proximity and data control as new paradigms for building a better interconnected house can help fulfil the GDPR requirements, most of which are in opposition to the rules according to which the IoT objects are built today.

Technical and Legal Insights for A Sustainable Smart Home

What I argue in this part of the essay is that solutions to the aforementioned issues cannot just rely on regulation and legal enforcement. Of course, there will be the need, of rules but IoT technology is proceeding at a faster pace than any known democratic political process. In this case, any regulation will always be late and will not satisfy completely the needs of users and innovators. What I suggest is to combine the overarching principle of privacy by design and by default set in the GDPR with the most promising technologies to change the centralised IoT paradigm from within (through the help of techniques such as Edge Computing, DLT and Blockchain protocols for the house). To sum up, it is essential to promote an interdisciplinary dialogue between legal and technical experts. This could effectively help not only in building more privacy and data protection compliant smart homes, but also more environmentally sustainable consumer habits and buildings.

Privacy by Design and By Default As An Overarching Principle

There is an important principle at Article 25 of the GDPR. It is called the principle of privacy by design and by default. The principle of privacy by design was formulated in the 1990's by Ann Cavoukian (former privacy officer of Ontario, Canada) and the privacy by default was just one of the consequences of it.

Instead, in the GDPR the two principles are separated and coexist in the same article. On the one hand, privacy by design means that privacy must be the core value since the design and first ideas about the development of a new technology. On the other hand privacy enhancing options must be the default options and not left to the choice of the consumer.

The GDPR entered into force in 2018, and already the scientific and the legal worlds have started collaborating both in the creation of new technology (which is data protection compliant from the beginning) and in the assessment of the privacy compliance level of already existing technologies.

Surely commentators have questioned also the generality of this ultra-broad data principle and some rightly worry about the economic interests that building technology in this new way might compromise. These doubts are founded but at least this principle is hardwired in the EU legislation that has been source of inspiration for many other countries. It is true that things are not made easier by the fact of thinking ahead a 'practically more difficult to obtain and maybe less economically rewarding' solution, but the advantages that could spread among society and consumers could be much more rewarding and lasting in the long term. Users would trust privacy technology and green compliant IoT for the house as they acknowledge privacy and environment protection as urgent issues to solve. Moreover, if a consumer is satisfied with the purchase of an IoT product that respects the user's privacy and the environment, they will be more likely to buy other IoT objects of the same brand.

The Promise of Edge Computing

To understand Edge Computing, one has to know a bit more in detail how the data cycle in the IoT concerning the house work. I will recall briefly what stated *supra*. After the sensorial inputs are collected at the physical/device layer through sensors on the objects, data are transformed into and are sent to a gateway which has the function of selecting the data and sending them to the cloud or proprietary network. However, the traffic on the web has increased in an astonishing way during the last ten years. Even before privacy, structural concerns interested the technical experts: it was apparent to many that the Internet infrastructure based on the cloud model could not last forever. Because of these infrastructure concerns, Edge Computing was developed. The idea is actually quite simple and some commentators actually consider it as a derivation of Moore's law. If computational power cannot exceed a certain threshold, nothing actually prevents objects or parts at the edge of the entire cloud system to become more powerful computationally, thus maintain an overall balance. This will mean that small computational units will be hosted by more devices that will able to process and analyse data but also to keep a log of all the operations done at the edge by the IoT object. The problem of sending all data to the cloud (which maybe it is outside the EU) would not exist anymore.

Even if the reason why Edge Computing exists is entirely technical and structural, it can have good effects on the application of Art. 25 GDPR: keeping the data closer to the user is indeed something that responds to the privacy by default and by design principle.

It is true that some commentators say that the IoT model is quite centralised and that better optimization could reside in a better use of the fog layer, a sort of a transparent layer before the cloud invented by CISCO. Honestly, I think that Edge Computing responds better to the challenges set by data analysis in an era where data protection is more and more felt as a value and something to care for even by non-experts. To make this technique more GDPR compliant, there would be the need to ensure that the logs and data entries are explained in a comprehensible and transparent manner but also that can be retrieved safely and that can be also translated in a machine readable format according to Art. 20 GDPR, which ensures data portability (which is more or less the legal equivalent of interoperability).

DLT and Blockchain Protocols for The House

The IoT has been the paradigm for object 'intelligent' communications since the beginning of the '00s. Despite that, it has been known for a while that the security level and integrity of IoT (especially domestic ones) can be easily breached. One of the main liabilities is that, overall, the IoT is quite a centralized system. At both ends, at the edge of it and in the immateriality of the cloud, there are basically no techniques in order to protect the data from being stolen by hackers. It goes without saying that the problems are tougher if third party data is involved in a data breach. But centralisation is not the only structural problems with IoT in general, and home IoT in particular. Also, the low battery and traditionally low computational power (including memory) made security and data protection challenges more apparent in the IoT objects which are also called constrained devices. It is true that Edge Computing can be quite a game changer in augmenting the computational strength of even home IoT objects but also some efforts have been made in order to apply some low-weight cryptography (cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process) which can adapt better to the specificities of the IoT.

That is why technical scholarship but also legal scholars are wondering whether Distributed Ledger Technologies (DLTs) and Blockchain can serve as corrective of traditional structural IoT deficiencies. Distributed ledgers are *ipso facto* de-centralised structures, which fix in an unmodifiable way transactions of users that work in a collaborative way

However, the kind of cryptographic techniques used by DLT (symmetric and asymmetric functions together with hash functions) require quite a lot of power to perform the communication between simple IoT objects, therefore some questions persist about whether a full implementation of DLT and Blockchain protocols in IoT objects would give problems in terms of scalability. Most technical experts are convinced that there must be specific DLT/Blockchain protocols to make the IoT more secure. That is why there are already experimentations of protocols such as IOTA, Chain of Things, Riddle &Code; Modum.io.

The advantages could be quite sensible not only under the cyber security and privacy angles but also on the liability one. Transparency in transactions can explain better what happened and who caused a damage. At the moment there is no way to know it easily through the cloud system. Furthermore, in the event of a damage, the IoT could register all that happened and ascertain almost exactly who or what was at fault for causing the damage.

The Green IoT

The Green IoT (hereinafter GIoT) is a promising new field of automation engineering combined also with material research whose objectives is to decentralise the IoT cloud based structure and make it ecologically more sustainable. The structure of the GIoT is practically the same described before, but what changes is the effort in reducing network wastes of energy. This is obtained with also new techniques of routing data and making them closer to the user and by using new materials that are known for their non-toxicity and that could in principle be recycled. This promising field is at its dawn (the first publications are of 2020) and it is definitely promising.

Conclusions

This paper hopes to be like a bridge. Hopefully, it would be a bridge between the law and the best technological developments that are taking place in the field of the smart home automation. The fact that the smart home is still not realised (or, at least, not generalised as a means of living) can become an asset under a double point of view.

On the one hand, the development of privacy and data protection policy and legislative instruments (GDPR included) is already influencing the IoT domestic technology in making it more transparent, more decentralised and more understandable to the common user. On the other hand, climate change and policy endeavours to make housing fairer and greener are taking place and are influencing how technology is built and conceived. Furthermore, it appears that a more decentralised IoT model can ensure at the same time good results both in terms of data protection and environmental sustainability.

It is wished that home IoT producers and manufacturers see this combination of both environmental sustainability and data protection not as just an economic hurdle, but as a chance to make the best product on the market and to increase the trust users have towards new technologies for the house. These two aspects (environment and data protection) cannot be dealt with separately as they will become soon not just an option but the only option. What the legal scholars could start doing is to begin a shared discussion with innovators about the advantages and the limits of the concept of personal data and be open to learn about the specificities of the production process of domestic IoT in order to create a liability system that is fairer and boosts innovation while maintaining a satisfactory level of user protection.

This article is cautiously optimistic as both the GDPR or GDPR inspired legislation and environmental policy objectives seem to stir businesses and states in the right direction.

In this historical conjuncture, if privacy and environment issues are not taken as a necessary challenge, we all have to lose, users and businesses alike. The alternatives such as systemic personal data breaches and impossibility to limit the impact of climate change from our houses are far worse than continuing to create cheaper, less secure and more polluting technology. That is why furthering cooperation among data protection and technical experts is the only way forward to meet the challenges of environment sustainability and a more trustful relationship with new technologies.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177.

References

Albreem M., Sheik A., Alsharif M. et al. (2021) ‘’ Green Internet of Things (GIoT): Applications, Practices, Awareness, and Challenges, *IEEE Access*, 9, pp: 38833-38858.

Alfa A., Alhassan J., Olaniyi O. et al (2021) ‘’ Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions, *Journal of Reliable Intelligent Environments*, 7, pp: 1153-143.

Ali B., Awad A. (2018) ‘’Cyber and physical security vulnerability assessment for IoT-based smart homes, *Sensors (Switzerland)*, 2018, 18(3), pp: 817.

Bandyopadhay D., Sen J. (2011) ‘’ Internet of things: Applications and challenges in technology and standardization, *Wireless Personal Communications*, 2011, 58(1), pp: 49-69.

Bygrave L. (2017a) “Hardwiring Privacy”, in R. Brownsord, E.Scotford and K. Yeung (eds.) *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press, Oxford, pp: 754-772.

Bygrave L. (2017b) ‘’ Data Protection by Design and by Default : Deciphering the EU’s Legislative Requirements, *Oslo Law Review*, 2017, 1(2), pp: 105-120.

Cavoukian A. (2009) ‘’ Privacy by design. The 7 Foundational Principles. www.ipc.on.ca. (06/08/2021).

Chevru S., Kumar A., Smith N. et al (2020) *Demystifying Internet of Things Security. Successful IoT Device/Edge and Platform Security Deployment*, Apress Open: New York.

De Conca S. (2020) ‘’ Between a rock and a hard place: owners of smart speakers and joint control, *SCRIPT-ed*, 17(2), pp: 238-268

Edwards W.K., Grinter R. E (2001) “At Home with Ubiquitous Computing: Seven Challenges”, in G. Abwod, B. Brumitt, S. Schafer (eds.) *Proceedings of the International Conference on Ubiquitous Computing (Ubicomp 2001)*, LNCS 2201-Springer, Berlin, pp: 256-272.

EU Commission (2021) Next Generation EU, https://europa.eu/next-generation-eu/index_en (06/08/2021).

EU Comission (2020 a) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL New Consumer Agenda Strengthening consumer resilience for sustainable recovery COM/2020/696 final.
EU Commission (2020b) New European Bauhaus: Shaping more beautiful, sustainable and inclusive forms of living https://europa.eu/new-european-bauhaus/index_en (06/08/2021).

EU Commission (2019) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal, COM/2019/640 final.

EU Fundamental Rights Agency, Council of Europe (2018), *Handbook on European Data Protection Law*, EU publishing: Luxembourg.

EU Parliament and Council, 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), OJ L 119,4.5.2016.

Floridi L. (2014) *The Fourth Revolution. How the Infoshpere is Reshaping Human Reality*, Oxford University Press: Oxford.

Floridi L. (2020) *Il Verde e il Blu. Idee ingenue per migliorare la politica*, Raffaello Cortina Editore:

Rome.

Gonçalves M. E. (2020) ‘’ The risk-based approach under the new EU data protection regulation: a critical perspective, *Journal of Risk Research*, 23(2), pp:139-152.

Huh J., Seo Y. (2019) ‘’ Understanding Edge Computing: Engineering Evolution with Artificial Intelligence, *IEEE Access*, 7, pp. 164229-16245.

Jain S. (2019) ‘’ Can Blockchain accelerate Internet of Things (IoT) adoption?, https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html (06/08/2021)

Leenes R., De Conca S (2018) “Artificial intelligence and privacy- AI enters the house through the Cloud”, in W. Barfield, U. Pagallo (eds.) *Research Handbook on the Law of Artificial Intelligence*, Edgar Elgar Publishing, Celthenham, pp: 285-306.

Minoli D., Occhiogrosso B. (2018) ‘’ Blockchain mechanisms for IoT Security, *Internet of Things*, 2018, 1(2), pp: 1-13.

Mocrii D., Chen Y., Musilek P. (2018) ‘’ IoT-based smart homes: A review of system architecture, software, communications, privacy and security, 1(2), pp: 81-98.

Nativi S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) A multi-facets analysis*, JCR: Luxembourg.

Ohm P. (2010) ‘’ Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57(6), pp: 1701-1777.

Pagallo U., Durante M., Monteleone S. (2017) “What is New with Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing Control in IoT”, in R. Leenes, R. Van Brakel, S. Gurtwith et al., *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer International, Cham (Switzerland), pp: 59-78.

Pranit Jeba Samuel C., Dharani K.G., Bhavani S. (2020) ‘’Power algorithm to improve the IoT device for lightweight cryptography applications, *Materials Today*, DOI: 10.1016/j.matpr.2020.11.326 (article in press).

Purtova N. (2018), ‘’ The law of everything. Broad concept of personal data and future of EU data protection law, *Law, Innovation and Technology*, 10(1), pp: 40-81.

Sahu M. (2021) ‘’Criptography in Blochain: types and applications, *UpGrad Blog*, https://www.upgrad.com/blog/cryptography-in-blockchain/ (06/08/2021)

Simmons D., (2021) ‘’ 13 Countries with GDPR-like Data Privacy Laws, *Comforte Blog*, https://insights.comforte.com/13-countries-with-gdpr-like-data-privacy-laws .(06/08/2021)

Shabandri B., Maheshwari P. (2019), ‘’ Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle, in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp: 1069-1075.

United Nations, *Sustainable Development Goals (SDG30)*, https://sdgs.un.org/goals (06/08/2021)

Van Alsenoy (2019), *Data Protection Law in the EU: Roles, Responsibilities and Liability.* Intersentia: Cambridge-Antwerp-Chicago.

Varjovi A., Babaie S. (2020) ‘’ Green Internet of Things (GIoT): Vision, applications and research challenges, *Sustainable Computing: Informatics and Systems*, 28, pp: 100448- 1004456.

Voigt P., von den Bussche A. (2017), *The General Data Protection Regulation (GDPR) A Practical Guide*, Springer: Cham (Switzerland).

Wolters P. (2017) ‘’ The security of personal data under the GDPR: A harmonized duty or a shared responsibility? *International Data Privacy Law*, 7(3) pp: 165-178.

Yamazaki Y. (2007) ‘’ The Ubiquitous Home, *International Journal of Smart Home*, 1(1), pp: 17-22.

Zeadally S., Das A.K., Skavlos N (2021), ‘’ Cryptographic technologies and protocol standards for *Internet of Things*, 14, pp: 100075-100065.

Zhang J., Chen B., Zhao Y et al., ‘’ Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues, *IEEE Access*, 6, pp: 18209-18237.