Which future strategy and policies for privacy in 5G and beyond?

Which future strategy and policies for privacy in 5G and beyond?

Enrico DEL RE
University of Florence and CNIT
Firenze, Italy
enrico.delre@unifi.it

***Abstract*—In May 2018 the General Data Protection Regulation (GDPR) entered into force in all Member States of European Union (EU) and its principles received a worldwide interest and acceptance. It represents a fundamental normative step forward for the protection of personal data in the future Internet systems. However, 5G networks, Artificial Intelligence technologies and the Internet of Things raise security and privacy issues that could not be addressed only by GDPR, even assuming its complete compliance by the service providers. In addition and in synergy with GDPR rules, we need innovative scientific and technical solutions to guarantee the complete control to the users to the access and the use of their personal data. Some preliminary results are encouraging for achieving this objective, but advanced international researches must be promoted on this challenging yet fundamental issue in the next future to guarantee the users the protection and the complete control of the use of their personal data and to guarantee all people their unalienable fundamental rights.**

Keywords—5G, AI, IoT, privacy, a priori user control

I. INTRODUCTION

This paper addresses the problem of the protection of personal data in future 5G and Internet systems, coupled with Artificial Intelligence (AI) technologies and suggests a visionary new paradigm for its definitive solution. The combination of 5G, AI and Internet of Things (IoT) arises severe and concrete risks to the security and privacy of personal data without any awareness of their owners. Presently, the protection of personal data is assigned, legally, to normative regulations and, technically, to suitable protocols. However, this paper tries to clarify that both approaches, even at the forefront of their respective fields, cannot guarantee the awareness and the control of personal data by their owner and that new efficient technical solutions are mandatory to safeguard the people fundamental individual rights.

The paper is organized as follows. Section II clarifies the inadequacy of present regulation and technical solutions to guarantee the awareness and control of personal data by the owner and indicates the requirement of a new paradigm of the technical solutions that could solve definitely and efficiently the protection of personal data. Section III gives an overview of some international researches addressing in some way the new paradigm and providing some interesting preliminary results. Section IV clarifies that an intensive and aggressive international research is mandatory to achieve the required technical solutions in reasonable timeframes and that this is the main and indispensable future task of the International Scientific Community to guarantee the fundamental individual rights to all people in the future human digital society.

II. SECURITY AND PRIVACY ISSUES IN FUTURE 5G AND INTERNET SYSTEMS

In the future Internet systems the 5G mobile networks provide high-speed, ultra-reliable, massive, ubiquitous and always available connectivity at the global scale, the AI capabilities can implement innovative and powerful processing of any kind of data and the billions of (more or less) smart objects and sensors always connected in the IoT provide an enormous amount of data (Big Data). The combination of these three technologies will realize the possibility to obtain, to store, to process, to deliver diversified and high volume Big Data. Most of these data will refer to human sensitive information and could be acquired even without the awareness of the interested subjects. For example, this is particularly realistic when automatic profiling (i.e. profiling without any human intervention) of personal data and automatic facial recognition are put in place. It is not visionary to imagine that this scenario looks like an ever present distributed and global computer dealing with personal data without the awareness of their owners and suggests a future world much worse than the one of the famous *Big Brother* described in Orwell's *1984,* with the concrete risk of violation of the fundamental human rights and of people becoming the new future digital slaves of a few big players.

Of course, 5G, AI and IoT can provide breakthroughs and enormous benefits to the society and the persons (e.g. for e-health applications and services to disabled and elderly people, environment control and security, smart energy production and utilization, smart mobility management, industry efficiency, smart cities, smart buildings, media and entertainment, e-government,…) and it is a vital interest of the entire human society to preserve the benefits while reducing to the minimum the associated risks of violation of personal security and privacy.

European Union (EU), as the first political organization, since 2012 tackled this problem and stated, "*Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services, e.g. in more efficient and less resource intensive provisions of services. This is why data protection plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy*" [1], and "*by design new systems must include as initial requirements:*

- *The right of deletion*
- *The right to be forgotten*
- *Data portability*

- *Privacy and data protection principles taking into account two general principles:*
- *The IoT shall not violate human identity, human integrity, human rights, privacy or individual or public liberties*
- *Individuals shall remain in control of their personal data generated or processed within the IoT, except where this would conflict with the previous principle.*" [2]

Following these general and challenging statements, in spite of the many heavy attempts to defeat any rule, EU issued the so-called GDPR (*General Data Protection Regulation*) that entered into force in all Member States on May 25, 2018 [3]. This complex regulatory document deals with all cybersecurity requirements related to personal data and, particularly, to the confidentiality and privacy of data anyhow referred to the user (defined *data subject* in the GDPR terminology).

Basic principles and guidelines of GDPR, when someone or something is collecting, processing and storing personal data, are lawfulness, fairness, transparency, minimization, purpose limitation, security, accuracy and integrity. Another key and distinguishing feature is that the service providers must ask data subject for consent defined as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"* [3,preamble 32]. Consent is not given once and forever, but must be renewed whenever personal data are used for purposes other than those initially authorized. Heavy penalties are imposed to service providers who do not comply with the GDPR rules. GDPR is a significant step forward for user security and privacy protection, as demonstrated by the worldwide acceptance of its principles that have gained consensus outside Europe (California, Japan, Brasil, Singapore, New Zeland, and others) and in recent public events have even suggested the CEO's of major social networks, perhaps reluctantly, to sponsor their adoption on a worldwide basis.

Thus, can we be confident that GDPR directives are sufficient to guarantee the personal data security and privacy in the future Internet systems?

First, the implementation of the cybersecurity requirements, even after GDPR, is in charge of service providers that should guarantee their fulfillment. The heavy penalties in case of noncompliance should convince service provides to conform and to implement all the necessary tools and actions, but we all know that this is not always the case.

Second, present offered services, while too slowly trying to comply with GDPR rules, miss almost completely the fulfillment of the security and privacy requirements 'by initial design', as stated by the EU principles.

Third, does GDPR fully comply with the stated EU principle "*Individuals shall remain in control of their personal data generated or processed within the IoT"* ? Apart the initial request for consent, no *a priori* control by the owner of the authorized or unauthorized subsequent use of her/his data is guaranteed and at most this can be verified only *a posteriori*, e.g. accessing to a database of all data transactions certified by a Distributed Ledger Technology, like Blockchain. The automatic profiling, the facial recognition and possibly in the near future the analysis of individual pheromones [4] are examples of personal data processing that could not be ruled by the GDPR.

The solution of these problems cannot rely upon even much advanced regulatory directives like GDPR even in combination with Blockchain. To avoid, perhaps definitively, the violation of our fundamental rights, we need the new paradigm of *"individual a priori data usage control"*, defined as:

"except in cases of force majeure or emergency, any use in any form and for any purpose of personal data must be authorized in advance and explicitly by its owner, correctly informed of the purpose of use".

To meet this highly challenging objective, we need synergize the innovative and revolutionary GDPR directives and new efficient technological tools specifically dealing with the direct and *a priori* control by the data subject of her/his data.

III. RESEARCHES ON INDIVIDUAL A PRIORI DATA USAGE CONTROL

Currently, some international research projects are ongoing on this subject. In the literature, they appear with different names: "*User-centric security and privacy*" [5], "*Information-centric cybersecurity*" [6] [7] [8], "*Usage control cybersecurity*" [9] [10].

User-centric Security and Privacy

In 2015, EU issued a CHIST-ERA call *User-Centric Security, Privacy and Trust in the Internet of Things* [5]. Six projects have been selected, started in 2017 and ending in 2019. Other projects are ongoing in specific calls of the EU Framework Programme Horizon 2020. Preliminary results of these projects are presented in [11], giving in the *Introduction* a synopsis of the new technologies and the application to specific use cases. The objective of these projects is to support the users to understand how their data are accessed, collected, used, processed, and kept safe. Security and privacy are implemented *by design* since the initial development of an app/service and are under the control of the data subject by as simple as possible efficient technical solutions. By providing the relevant information, the users should be empowered to be aware and to make their own decisions regarding their data, which is essential in gaining informed consent and in ensuring the take-up of IoT technologies. Proactive social involvement of the users is also foreseen from the beginning to ensure education and awareness of their rights and to provide adequate technical solutions to meet shared requirements.

Projects address one or more of the following research challenges:

- Methods for data anonymization
- Technical mechanisms to increase trustworthiness when data is shared between different providers
- Intrusion detection methods
- Authentication using trusted computing
- Dynamic security to allow systems to adapt to users with different requirements and capabilities

- Tools for supporting preferences and priorities of culturally diverse users
- Natural language for expressing data access/usage policy
- Data visualisation for increasing user awareness of privacy issues
- Empowering users with risk evaluation tool for their data and contacts
- Assistive technology/techniques to encourage more secure behaviour and awareness of users.

Examples of application of the new technologies to some use cases are compliance to GDPR regulation, management of informed consent/deny and of privacy in mobile apps, application to food chain, electricity load balancing, mobile gaming, smart meter, humans with special needs, extraction, classification and encryption of the document content, and distributed ledger technologies.

Information-centric cybersecurity

This approach appears to be a revolutionary paradigm. It proposes an internal self-protection of data instead of external protection by systems and/or applications together with a complete architectural and functional new design of microprocessor and operating systems. Intelligence is embodied into the data itself that defines its 'use policy' to implement a self-defense action in any application context. Accessing the data, the new CPU and operating system consult the 'use policy' of the data and uses it (processes) only if the context is reliable and consistent with its use policy.
If technically possible, this combination of the new data structure and hardware/software architecture could solve definitely the problem of the controlled and authorized processing of the user data. However, with this approach even the positive technical solution is not sufficient. We would need the international and cogent regulation agreement (i.e. standardization) in order that the solution be adopted by all the processing systems of new generation. Of course, the latter point is much more difficult to achieve in realistic timeframes.

Usage control cybersecurity

This approach still assumes a 'use policy' embodied into the data. The data and its 'use policy' is incorporated in an encrypted entity and only a specific software authorized to its decryption uses the data according to its 'use policy'. Dynamically the 'use policy' can also be changed over time. Interestingly, this proposal does not require any change to the architecture of microprocessors and operating systems, but only a specifically designed software authorized to access and process the encrypted data. Thus, it could run on all present processing systems.

IV. Final considerations and the role of the international future research

All the described techniques have the revolutionary potential to guarantee the correct use of personal data under the direct control of the interested users:

- "*User-centric security and privacy*" and "*Usage control cybersecurity*", with some relevant differences, require only the implementation, even in current processing systems, of the specific software and of data encryption inclusive of the 'use policy'
- "*Information-centric cybersecurity*" requires a paradigm shift in the design and implementation of microprocessors and operating systems and an international global agreement on a new standard for processing systems of future generation.

The horizon of actual availability and implementation is therefore much closer to the formers, whereas the latter would provide a more definitive solution to security and privacy of user data. However, at the moment all techniques require adequate processing resources, that, whereas compatible with present processing systems, are too computational intensive for the use in the future IoT, where most objects in the network will have reduced or very poor processing capabilities. In IoT future scenarios, much more simple and implementable technical solutions are needed.

Finally, what could and should be the role of the international present and future research on security and privacy for 5G and Internet systems?

EU, the first and unique at international level, has the great merit to have raised the problem of the protection of the user personal data in the future Internet and IoT systems. It resisted to all attempts to stop and frustrate any regulation and finally succeeded to issue the GDPR, cogent regulation for all Member States. The international success and recognition of the rules of GDPR place EU on the forefront of the legal implication and protection of personal data. However, even advanced and revolutionary regulations are not sufficient to *completely and definitely* guarantee people the correct use of their personal data. People need efficient and easy-to-use tools to control *a priori and in itinere* the generation, acquisition, storage, processing and usage of their data. The preliminary interesting results reported in this paper indicate at least some possible pathways towards this objective. They must be followed by an intensive scientific research on the technical solutions and technological implementations to achieve efficient and affordable tools for the future Internet scenarios and sufficiently simple for the use of the common citizens. Moreover, the results must be obtained in reasonable timeframes before our privacy be definitely compromised. The International Scientific Community has the challenging and primary task to strongly sustain worldwide scientific and technical innovative and disruptive researches on the subject of the personal data protection. The international present funding on this subject is not sufficient.

This should be one of the most relevant scientific and technical objectives in the framework of security and privacy in 5G and future Internet systems. It must be pursued in spite of the likely very strong resistances by major players and it is absolutely mandatory to guarantee the fundamental individual rights to all people in the future human digital society.

References

[1] *European Commission, 25.01.2012, SEC(2012)72 final, page 4.*

[2] *European Commission, 2013, IoT Privacy, Data Protection, Information Security.* *http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753*

[3[*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, Official Journal of the European Union (OJ), vol. 59, pp. 1-88, 2016.*

[4] https://iapp.org/resources/article/privacy-2030/

[5] UE CHIST-ERA 2015 call: *User-Centric Security, Privacy and Trust in the Internet of Things*

[6] R. Chow, et al., *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control,* in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 85–90. [Online]. Available: http://doi.acm.org/10.1145/1655008.1655020

[7] R.B Lee*, Rethinking computers for cybersecurity,* IEEE Computer, 2015

[8] *IEEE Communications Mag.,* Jan. 2017

[9] A. Lazouski, F. Martinelli, P. Mori, *Usage control in computer security: A survey*, Computer Science Review, vol. 4, no. 2, pp. 81–99, May 2010. [Online]. Available: http://dx.doi.org/10.1016/j.cosrev.2010.02.002

[10] E. Carniani, D. D'Arenzo, A. Lazouski, F. Martinelli, P. Mori, *Usage Control on Cloud systems,* Future Generation Computer Systems*,* vol. 63, pp. 37 – 55, 2016, Modeling and Management for Big Data Analytics and Visualization. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16300875

[11] J.L. Hernandez Ramos, A. Skarmeta, (Eds), *Security and Privacy in Internet of Things - Challenges and Solutions,* within the series: *Ambient Intelligence and Smart Environments,* (*Introduction* by E. Del Re), IOS Press, 2020