INTRODUCTION TO 5G TECHNOLOGIES AND THEIR RISKS IN TERMS OF PRIVACY

v. May 2020

EXECUTIVE SUMMARY

The use of mobile telephony is present at almost every social activity. Since the third telephony generation, mobile devices have grown exponentially in functionalities, but threats to the privacy of its users have likewise increased. At the moment, the technological leap is occurring from the fourth to the fifth generation of mobile telephony, better known by its acronym 5G.

This technical note aims to review the evolution of mobile telephony since its implementation, and to expose new functionalities in the 5G technology (better accuracy in geolocation services, virtualization, edge computing, …), as well as to identify its risks. A series of recommendations and conclusions are likewise proposed for all implied actors, so that 5G does not pose a threat to the rights and freedoms of natural persons.

Finally, it is proposed to think about the need to adapt the current regulations on the collection and preservation of network traffic data due to the changes in the proportionality of data collected.

Keywords: 5G, Edge Computing, IA, IoT, Mobile, Privacy, Data protection, GDPR, Risk, Technology, Telephony, Virtualization, Slice.

TABLE OF CONTENTS

I. INTRODUCTION

The fifth generation of mobile communications (5G) started to be deployed in Europe in early 2019 and it is envisaged to have a great impact on the digital society.

The main improvements offered by 5G to users are:

- *Enhanced mobile broadband or eMBB*
- *Massive machine communications or mMTC*
- *Ultra-reliable and low latency*[1] *communications or URLLC*

These features will allow for the implementation of products and services where a high speed is requested, such as multimedia applications or augmented reality applications, as well as the definitive launch of the Internet of Things (*IoT*), due to the possibility of having a great volume of devices connected simultaneously. On another note, it will materialise applications requesting real time responses, such as those typical of the connected industry or remotely-assisted surgery, thus enabling the expansion of services based on automated decisions, often through the use of artificial intelligence.

In order to carry out the deploy of the 5G networks, a technological renewal unprecedented in recent mobile technology history is being planned. The network architecture and the network functions will experience great changes with the introduction of technologies such as virtualization [2] (*software-defined networking* and network function virtualization), *edge computing*[3] and *network slicing*[4].

II. PURPOSE AND RECIPIENTS

The purpose of this document is to offer a wide picture of the innovations presented by the 5G technology of mobile communications and to perform a non-exhaustive analysis on the risks for privacy that may be inherent to this technology, as well as other technologies that use it.

It is specially addressed to agents who, as a result of a certain unfamiliarity with the 5G technology, are uncertain about the implications that its generalised implementation may have for privacy.

It is likewise addressed to manufacturers and suppliers, to service operators, telecommunication companies and application developers who will establish 5G business models and who wish to further explore the implications for privacy with regard to the products and services they develop like, for example, any OTT[5] service developers.

III. EVOLUTION OF MOBILE TELEPHONY

Since 1980, each decade has seen a significant advance in mobile telephony, which has been described under the shape of generations. Each generation offers new functionalities that have contributed to the popularisation of mobile devices. However, new threats to privacy for individuals have likewise appeared at the same time.

---

[1] Latency is the response time between the action and the reaction. In communications, it is the time interval between the start of the submittal of a message and the arrival of the first bit to its destination. Transmission time is the time between the arrival of the first bit and the arrival of the last bit. They are independent values. A low latency allows for real time applications.

[2] Technology that allows to execute different operating systems that are independent within the same host equipment.

[3] Technology that allows to have the systems that perform processing activities and the data physically closer from the user, thus minimising the delays produced during long-distance transfers of information.

[4] Technology that allows to use the same physical network infrastructure for multiplex virtual networks within the same physical network infrastructure.

[5] Broadcasting and communication services using services provided by network operators (Over The Top).

- 1G: At the beginning of the 1980's the first analogical mobile telephones appeared with very limited capabilities, only being capable of making calls. Functionality was prioritised those days, with no regard to data protection, for, even if its use was anecdotal, communications among people were less private than what users thought.
- 2G: In 1991 the second generation, this time of digital telephony, provided the functionality of text messages through user terminals, such as the broadly known SMS. For example, this generation introduces encryption techniques in communication that improve confidentiality, although many loose ends are still pending in the authenticity dimension. Users suffer the first SPAM attacks and the interception of communications through rogue base stations.
- 3G: By the year 2000, the first 3G devices appear with multimedia, access-to-the-Internet, and television functionalities These phones also brought along the first malware code vulnerabilities, GPS geolocation and other.
- 4G: In 2010, the 4G telephony started to be deployed, which granted high-speed access to the Internet, and more robust encryption techniques were implemented. Because it was a network that was based on IP technology, all traditional threats present in LAN networks and the Internet were transferred to the world of telephony: APTs[6], DDoS[7], viruses, etc. as well as the risks related to privacy. The massive use of phones entailed an increase in the scale of the threats.
- 5G is the technology of this decade and for which the first terminals and services are already being commercialised.

IV. MAIN INNOVATIONS IN 5G

The fifth generation (5G) of mobile telephony entails a significant change with regard to prior generations. For the first time, specific hardware for telephony is no longer used to give way to general purpose equipment, which does not differ from the equipment we may find at any IT data processing centre, and a use is made of virtualization techniques, containers and orchestration. This is an advantage in terms of costs and flexibility of implementation, and, on the other side, it makes the infrastructure inter-operative and accessible by Internet equipment.

There are three features that allow to speak of 5G as a disruptive technology and a change in the paradigm of conception of mobile communication networks: virtualization, *edge computing*, and geolocation, as well as important changes in security strategies.

Before a description is provided of them, and in order to better understand all concepts used, it is necessary to know the two differentiated parts of the architecture of a mobile telephony network.

- *Access Network*: It is the part of the network that connects final users (mobile devices) with the central network of the operator. It is the part of the infrastructure that enables an aerial connection, through radio, between the mobile devices and the network of the operator.
- *Core Network*: It is the central part of a network of a telecommunications operator. The part that manages all functionalities and services of the operator or, to put it another way, the part containing the functions of the network.

[6] Advanced persistent threat is the set of hidden computer processes aimed at and capable of attacking a specific objective in an advanced and ongoing way through time.
[7] Service denial distributed attacks.

5G has brought about novelties for both sides of the network, but the more disruptive ones apply to the *core network*. In Figure 1 a diagram is included with the basic architecture of a 5G network.

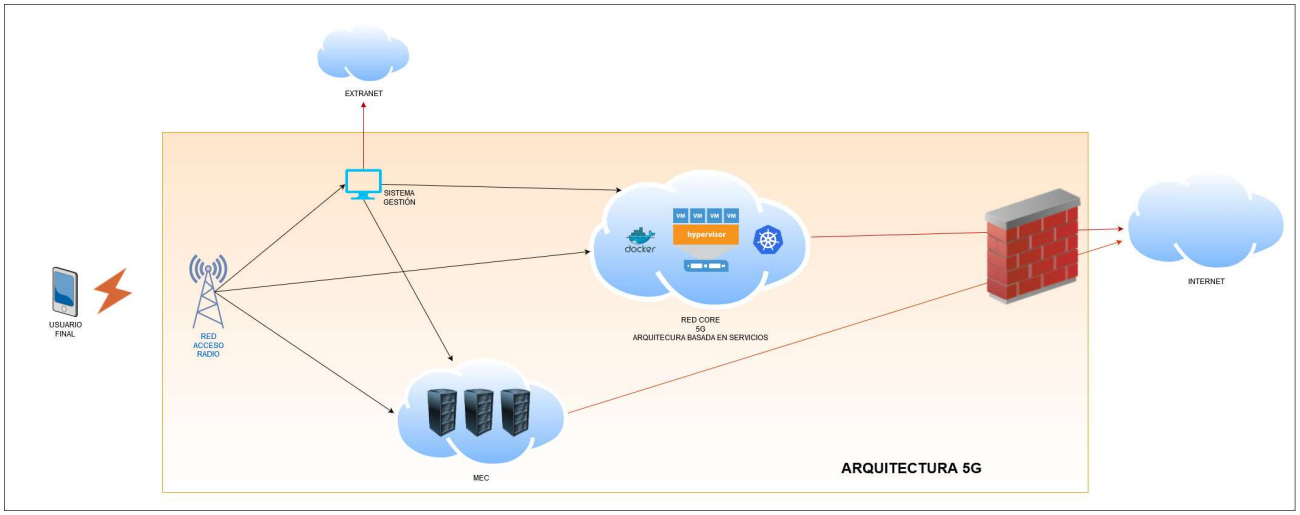

Figure 1. Basic architecture of a 5G network.

A. VIRTUALIZATION

It is doubtlessly the greatest revolution of all, and what may have an important impact on privacy is the use of virtualization technologies, which includes concepts such as:

- *Software Defined Networking* (SDN): current telephony networks are very static, and any change may imply modifications in the hardware, with costly manual procedures. The SDN allows for operators to make changes in the network swiftly and, in some circumstances, also automatically, adapting itself to the needs of demand in the network.
- *Network Function Virtualization* (NFV): entails a new way of creating, deploying and managing network services through the virtualization of each and every function provided by the network.
- *Network Slicing* (NS): implies an improvement and an adaptation of the support to the different types of traffic in 5G networks, through the virtualization of a set of network functions that are part of the *core network*. Conceptually speaking, it would be equivalent to saying that each *core network* may be composed of a set of *slices* or *virtual core networks*.

Virtualization is an already mature technology within the IT background, but 5G enables its début within the background of mobile communications, while transferring along its advantages and disadvantages.

The *core network* will be divided into the so-called *network slices*. *Network slicing* allows for logical networks to be established, with their own network functions, on a sole physical telecommunications infrastructure, and with parameters specifically set to provide an answer to the different requirements of each application. The network functions are a set of virtual components that are parametrizable and subject to creation from a dynamic point of view, each of them with a specific function that is designed without a status and separating the computation functions from the data storage functions. Each *slice* is composed of a set of network functions defined in the 5G standard.

The connection of the devices will be managed by the device manufacturers themselves or by the service suppliers through an integrated SIM (eSIM) and connected to a *slice* of the network also under their control. Thus, the user will not have to manage the connection with an operator or insert a SIM in the device.

The specification of 5G defines three standard *network slices*, each of them defined in order to provide one of the functional requirements of 5G (uLRLLC[8], eMBB[9], mMTC[10]), but it does not establish a limitation in the number of slices that may be established. The *network slices* function as independent virtual networks composed of a full set of network functions, but they are not totally isolated from one another because there is a network function that may be shared among several *slices*.

Thus, the *core network* of each operator will be composed of several *slices*, each *slice* formed by a set of network functions, and the *core networks* of the different operators will be connected with one another through a specific network function that will perform proxy functions.

The sole network function that may be shared among several *slices* of the same *core network,* according to the 5G standard, is the *Access and Mobility Management Function* (AMF). This is a key function, for it manages the registration, access and mobility of the user devices, the geolocation services and the potential legal interception of communications by law enforcement bodies.

The access network knows what *slices* are available as well as the requirements in terms of access capacity that it needs to provide to each user device while managing to what *slice* it needs to be connected. If the requirements of a device are very demanding, and the device is set for it, the same device could be able to connect to several *slices*.

For example, a mobile phone will connect through the access network to the *slice* corresponding to general purpose telephony while an intelligent traffic signal could be connected to a different *slice* specifically aimed at managing the traffic in a city. Both devices would share an *access network*, but they would end up receiving service from different *slices*.

This architecture is based on virtualization and *slices*, and it enables the implementation of management models that allow to offer *slices* as services (NSaaS). That is to say, an operator could commercially offer the management of a *slice* by a third party, such as in the case of virtual operators, but not limited to this specific case.

At the same time, *network slice* technology could allow for a substitution of the traditional dedicated networks and, thus, we would be able to see *slices* with different priorities and qualities subject to the SLA[11] contracted. For example, *slices* could be established to provide service to emergencies, traffic signalling, sports events, national defence, etc., as well as *slices* managed from the city council itself*,* an administration in charge of the services, and private organisations.

This management model for *slices* added to the low latency and massive connectivity features provided by 5G, will in all probability facilitate the definite development of the pairing IoT and Artificial Intelligence, with an exponential increase in the number of devices connected to a 5G network through the *slices* that are needed to meet their operation requirements.

[8] Low latency in communications.
[9] Great increase in the bandwidth.
[10] Massive connectivity of devices.
[11] SLA: service-level agreements.

B. EDGE COMPUTING

Cloud computing is based on the use of big data processing centres at different locations through the world geography aimed at storing and processing enormous amounts of data. The service model in mobile devices, as it is known today, uses mobile applications (Apps) that exchange data with Internet servers whose physical location does not need to be managed, at least a priori, by the user. Although this architecture is useful in many cases, there are certain situations where it cannot be applied due to the presence of a very high or unpredictable latency, which does not allow for real time applications.

The use of general purpose hardware in order to contain virtualized operator services or services from other suppliers allows for the implementation of one of the most disruptive elements of 5G, such as the so-called MEC (*Multi-Access Edge Computing*). The *edge computing* technology will allow for the "gravity centre" of data processing to be displaced from the servers to locations closer to the terminal user device, when necessary. In summary, an information and/or services flow may exist between the different locations agreed upon with the network operators and the service managers at points close to the final user and within the mobile telephony network of a telecommunications operator without being, in principle, on the Internet.

At the time to perform such computation tasks as close as possible from the final user, 5G will allow for a reduction in the latency of communications in such a way that it will allow for capabilities close to real time, which are essential in scenarios such as:

- Self-driving cars
- Industrial automatisation
- Augmented reality
- Connected households and offices
- Videogames
- Remotely assisted surgery

C. GEOLOCATION

The use is envisaged of transmission frequencies higher (within the band of 26GHz) than those currently used in prior mobile telephony networks as part of the deployment of 5G, which will allow for much faster transmissions. However, the range of the signal will be more reduced in and the open field and very sensitive with regard to obstacles such as internal walls.

The way to overcome these disadvantages will be the installation of a denser network at external access points and the deployment of unprecedented mobile telephony access points indoors, especially at highly-attended large public surfaces.

In summary, a more compacted *access network* is required with many access points and a lesser distance from one another. This greater density will provide the capacity to localise the user terminal for operators and other agents related to the exploitation of network data, with a much greater precision than nowadays, reaching accuracies lower than one meter and, opposite to telephony generations previous to 5G, even three-dimensional geolocation. Therefore, a development is expected regarding novelty localisation-based services (LBS).

D. SECURITY

From the point of view of security, the specification of the 5G technology adds important improvements in the security measures with regard to prior generations, both in the access network and the *core network*.

Some of them are:

- A new permanent user identifier structure and, moreover, encryptions to avoid an unencrypted transmission via radio as was the case in certain circumstances with other generations prior to 5G.
- Improvements in the **authentication** mechanisms with the introduction of 5G-AKA[12], whose main improvements are that it is the network of the operator with whom the service is (*home network*) that authenticates both the user terminal and the network where the mobile phone seeks to connect (*service network*). The *service network* does not have keys to decrypt the communications until it has been authenticated by the *home network*, in addition, it has several control mechanisms against fraud.
- User data protected in **integrity** in the radio interface, additional to the protection of confidentiality already provided by 4G.
- Enabled access from non-3GPP networks [13] creating an encrypted tunnel through a key provided by the operator.
- TLS **encryption** of communications among network functions within the *core network*.
- Incorporation of **traceability** options that facilitate the registration of the operations in order to audit the security of the network.

The virtualization capacities, the implementation of a Service Based Architecture (SBA), and the separation between the user plane and the control plane (*Control and User Plane Separation* CUPS) will allow for 5G networks to be deployed respecting the principle of security by default.

These improvements made at security level entail a great advance both within the reliability of aerial communications of the *access network* (user device-antennae) and within the *core network*. Notwithstanding, the specification leaves the implementation of some of these mechanisms to the operator's criteria, and therefore, the increase in security of 5G networks may vary significantly from one telephony operator to another subject to the deployment of technology, with decisions by a sole actor affecting the global security of 5G network communications .

In addition, circumstances could potentially arise where security is degraded by an access to the service through a network with implementation deficiencies in itinerancy situations. The need to preserve compatibility with protocols of generations prior to 5G causes for vulnerabilities present in such protocols to extend over time.

V. RISKS FOR PRIVACY

5G is expected to be the great communication channel of the decade. All public or private network data may end up using the 5G communication structures and, all this linked to the increase in connected devices makes us think that virtually all individuals will be users of this network and all devices will be connected to it.

Without limitation, and pursuant to the above, at least the following risks for data privacy may be identified. Many of these risks are interrelated and are not new but rather, they were present in prior mobile telephony generations. However, they may experience an exponential increase if the implementation of 5G reaches the envisaged expectations of success.

[12] *Authentication and Key Agreement*

[13] 3GPP: *3rd Generation Partnership* Project Association of telecommunications groups participating in the standardisation of mobile networks since the 3G.

- Precise user geolocation: The fact that 5G uses much more base stations and a lesser distance from one another makes geographical location based on the network much more precise.
- Profiling and automated decisions: the increase in the amount and the data categories that circulate through the network multiplied by the amount of devices that each citizen will connect through 5G (IoT) will allow for the arrival of a precise individualisation of persons and the development of services that allow for automated decision-making on the persons (IA and real time services).
- Distribution of responsibility among manufactures, network operators and service providers: a significant increase in the number of agents that may be involved in personal data processing activities is envisaged through the deployment of 5G networks and through the explosion of new services. This could lead to ambiguity problems with regard to responsibility for the data processing, that is to say, the risk that the responsibility for each of the parties be diluted.
- Different privacy goals and interests among involved parties: in relation to the above, agents intervening in telephony networks will have different privacy interests, commercial interests, national security interests, etc., with manufacturers, telecommunications operators and services suppliers subject to different regulations, inter alia, the obligation to provide legal access to communications to law enforcement bodies from different states.
- Absence of a homogeneous security model: as 5G allows for the existence of multiple agents in the chain of communication, even within the *core network* of the operators, through services deployed by different service providers within the MECs. Each agent may comply with different security standards and may include segments corresponding to protocols of the first generations. Therefore, the global security will equal that of the weakest element.
- Exponential increase in the cyber-attacks surface: increase in the services, the connectivity, the interoperability, the input points and the management points to the network will increase the opportunities for threats to privacy to materialise.
- Inheritance of the privacy problems arising out of interoperable standard infrastructures: through the implementation of 5G with general purpose equipment, an infrastructure that was technologically differentiated in the past will be permeable vis-à-vis the same attacks suffered by conventional information technologies.
- Vulnerabilities arising out of virtual backgrounds and shared functions; in the same sense as the paragraph above, the privacy problems of virtualization technologies will be inherited, as well as the risk of data leak among functions shared among different slices, such as the referred *Access and Mobility Management Function* (AMF).
- Dynamism in the management functions of communications: if the management functions of the network in prior generations were de facto wired, the possibility of an update thereof through software introduces stability problems, version traceability, updates by several intervening parties, back doors, factory malware, and hacking.
- Possible loss of control by the user: this may occur on data flow, with possible cross-border implications, as well as the exercise of rights. 5G uses a distributed and dynamic processing model, where it is envisaged for data and processing activities to move in real time to the physical location where they are most needed or where their processing is more efficient.

Despite being a non-comprehensive risk list, such risks should be taken into account from the first design stages of the processing activities for the implementation of technical and organisational mitigating measures integrated in the nature of products and services that use

,or are based on, 5G technology to comply with required by GDPR article 25. The necessary efforts must likewise be made for the identification and the mitigation of new risks through risk management procedures and impact assessments on the protection of relevant data both at service suppliers and, most of all, at manufacturers.

VI. CONCLUSIONS AND RECOMMENDATIONS

When 5G technology reaches a suitable grade of maturity, the necessary conditions will be achieved for the pairing 5G-IoT-AI to provide new and disruptive services. This situation will probably have a high and unpredictable impact on the privacy of individuals.

The decisions by the operators in the implementation of the network, the management of the setting and the procedure thereof will have a decisive impact on the level of privacy reached. Thus, they are encouraged to define 5G infrastructures subject to the privacy by design and privacy by default frame. The developers and providers of equipment of network base technology for 5G must supply products with an adequate level of fulfilment of the GDPR that allows for the deployment of networks. At the same time, other agents providing a service within those communication networks through the creation and the management of new products and services will likewise have a level of responsibility in the implementation of measures and guarantees.

It will be necessary for all intervening parties in the implementation, management, and exploitation of the 5G network to take into consideration the following recommendations:

- In the new 5G-based applications and services, the information that needs to be provided to data subjects according to the regulations on data protection must be particularly clear and understandable, especially with regard to data controllers, the purposes, the adoption of automated decisions, and profiling, as well as on the access and the use of control measures by users. This last one being particularly highlighted.
- At the same time, transparency and traceability mechanisms need to be implemented both in cases of connection of devices to the 5G service and in cases where a distributed processing is performed.
- Careful definition of the roles and corresponding responsibility scopes (from the point of view of data protection) and clear delimitation of the obligations by developers, providers, operators and agents. This delimitation of responsibilities must provide an answer to the decisions effectively adopted on the means and the purposes of the processing in order to avoid the transfer of responsibilities via a contract.
- Implementation of control measures for the users themselves on data protection, both on data collected from the users and data inferred from their activity or the activity of other devices connected to the network within the frame of the IoT.
- Implementation of data minimisation measures, more precisely, with regard to geolocation, taking into account the privacy by default principle from the very early stages in the design process of 5G products and services.
- Establishment of measures that guarantee the compartmentalization of the data and avoid the leak of information between one procedure and another in cases of distributed processing and in the compartmentalization of network functions.
- Application of homogeneous security criteria on the different agents and network segments that are based on a risk analysis for rights and liberties, as established by the GDPR. The risk analysis must be oriented towards the management of threats in the 5G networks as a whole, not only in the particular operation of every agent.
- Guaranteed encrypted communications from one end to another and, furthermore, development of encryption models protecting the procedure and the transfer of

information in the *edge computing* model (such as homomorphic encryption, *network coding* techniques, or otherwise).
- Adaptation of the use of automated decisions to the provisions in the GDPR.
- Establishment of the necessary guarantees in the event of international transfers of data.
- Independent infrastructure and service audit, including the adherence to certification mechanisms with regard to data protection referred to in the GDPR.
- Collection of learned lessons in the world of the Internet and absence of direct imports of models that have proved to be vulnerable.

In all probability, infrastructure models will arise together with use cases and new services that will imply personal data processing that could be framed within those for which the GDPR requires an privacy impact assessment (PIA). Moreover, if the residual risk is still high, a prior consultation to the supervisory authority will be requested at the start of the processing activities pursuant to the lists drafted by the supervisory authorities to comply with Article 35.4 of the GDPR.

This new diversity scenario of services and products entails a new opportunity to develop the certification schemes envisaged by the GDPR. The certification schemes are very useful for the implementation and verification of compliance with the proactive responsibility measures in personal data processing. The establishment of a frame of trust in security with regard to data processing in 5G is an essential factor to guarantee its success.

Finally, it is necessary to think about the current regulations and standards related to the processing and preservation of traffic data by telecommunication operators, particularly in relation to geolocation. For instance, Law 25/2007 (transposing Directive 2006/24/EC), of October 18th, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, was approved when the standard resolution for geolocation in 1G to 3G networks required operators to locate users with an accuracy between 100m and 300m on the plane. Currently, in 2020, 4G networks require an accuracy of 50m, but with 5G resolutions of less than 1m will be achieved, also in 3D. The threat to privacy posed in 2007 by the preservation of geolocation information is not comparable to the new scenario in which 5G networks will be deployed. Therefore, it is necessary to adapt the regulations to establish adequate guarantees for the processing of new traffic information and, above all, in relation to its retention.

VII. REFERENCES

5G Americas TM, "The Evolution of Security in 5G"

Data Protection Officers and teams from Ericsson España, Huawei España, Movistar, Orange España and Vodafone España, information provided at meetings held by the AEPD.

European 5G Observatory, 5G Observatory Quarterly Reports

European Commission, EU coordinated risk assessment of the cybersecurity of 5G networks

Federal Communications Commission, 5G Edge Computing Whitepaper

Federal Communications Commission, 5G Network Slicing Whitepaper

R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," in IEEE Communications Surveys & Tutorials.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne and M. Ylianttila, "5G Privacy: Scenarios and Solutions," 2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, 2018, pp. 197-203.

Manuel Lorenzo, Ericsson España, talk at t3chfest - The Convergence of 5G, AI and IoT

José Picó J., Pérez D., CCN-CERT, Plataforma Vanesa, Seguridad en los protocolos de comunicaciones 5G

Privacy International - "Welcome to 5G: Privacy and security in a hyperconnected world (or not?)"

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons in relation to the processing of personal data and the free circulation of these data and repealing Directive 95/46/EC (GDPR).

Organic Act 3/2018, of 5 December, on Protection of personal data and guarantee of digital rights