Privacy and security aspects of 5G technology

STUDY

Panel for the Future of Science and Technology

EPRS | European Parliamentary Research Service

Scientific Foresight Unit (STOA)

PE 697.205 – March 2022

EN

Privacy and security aspects of 5G technology

This study describes two main dimensions of 5G technology, i.e. privacy and security. The focus of this research paper is the analysis of cybersecurity risks and threats, privacy challenges and 5G technology opportunities, at the EU level and worldwide, as well as the relationship between cybersecurity risks and privacy issues.

The methodological framework for the impact assessment of 5G technology is built on three pillars: (i) a document-based analysis of technical specifications and scientific literature that aimed at identifying risks, challenges and opportunities related to the innovations introduced with 5G technology; (ii) a parallel analysis with stakeholder involvement consisting of a quantitative analysis to gather information from a wide array of stakeholders, and a qualitative analysis based on feedback from a group of experts; (iii) a selection of relevant case studies that illustrate the risks, challenges and opportunities identified. Potential impacts on EU citizens' privacy, including personal data protection, and location, identity and group privacy, have been assessed through stakeholder engagement tools and techniques, such as interviews, roundtables and surveys, as well as the 'sentiment analysis' methodological approach, used to collect trends on 5G technology.

The complexity of the 5G ecosystem, where new use cases of the technology are constantly emerging, has also led the authors to assess the prospects of using new 5G-enabled technologies, such as the internet of things, robotics and artificial intelligence.

Moreover, policy options are defined and put forward for consideration by the European Parliament's Committees on Legal Affairs, Internal Market and Consumer Protection, and Civil Liberties, Justice and Home Affairs and the Subcommittee on Security and Defence, as well as by other EU institutions and the Member States.

AUTHORS

This study has been drawn up by Carmela Occhipinti, Luigi Briguglio, Antonio Carnevale, Riccardo Santilli, Emanuela Tangari and Andrea Iannone of CyberEthics Lab. Srls at the request of the Panel for the Future of Science and Technology (STOA), and managed by the Scientific Foresight Unit (STOA) within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

The authors acknowledge and would like to thank all the external experts for their contributions to this paper. The full list is available in the Annex. Their expert judgement has contributed with objective evaluation of relevant aspects, and added valuable suggestions based on their own experiences and competencies.

ADMINISTRATOR RESPONSIBLE

Zsolt G. Pataki, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail STOA@ep.europa.eu

LINGUISTIC VERSION

Original: EN

Manuscript completed in October 2021.

PE 697.205
ISBN 978-92-846-8830-2
doi: 10.2861/255532
QA-01-21-577-EN-N

http://www.europarl.europa.eu/stoa (STOA website)
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

This study analyses the privacy and (cyber) security aspects of 5G technology. The paper considers 5G not just as a performance booster for current mobile communication networks, but also as a technology enabling the convergence of communication networks with another foundation of the digital era, i.e. computing. The entanglement of these two aspects defines a complex ecosystem, composed of heterogeneous stakeholders, technologies, methodologies and best practices.

On the one hand, this ecosystem offers new opportunities for digitalisation, a key reason for which 5G technology is seen as a cornerstone of European resilience and one of the seven flagship areas of the European Recovery and Resilience Facility.

On the other hand, the complexity of this ecosystem poses unexplored and unexpected concerns, risks and challenges, in particular for security and privacy aspects.

Through an impact assessment based on a research conceptual map divided in four categories (section 2), **this paper focuses on the identification and analysis of the new potential risks, challenges and opportunities that 5G technology entails with respect to privacy and security**. The assessment is performed along three pillars: (i) a document-based analysis (section 3) of technical specifications, regulations and scientific literature that aimed at identifying risks, challenges and opportunities related to the innovations introduced with 5G technology, specifically with respect to privacy and security; (ii) a second pillar, based on the involvement of stakeholders (i.e. citizens and experts), composed of two kinds of analyses (section 4) based on four impact assessment categories (i.e. technology, privacy, security, ethics/politics); the analyses are (a) quantitative, to gather information from a wide array of stakeholders, and (b) qualitative, based on feedback from a selected group of experts; (iii) a third pillar (section 5) illustrating a selection of relevant case studies that ground in reality the concerns, risks and challenges identified and analysed in the first two sections of assessment.

The first pillar of assessment (i.e. document-based) follows three steps: (i) analysis of the current regulatory framework; (ii) identification of the relevant concerns and challenges based on a document analysis (i.e. technical specifications and scientific literature), and (iii) definition of policy options to mitigate and address the concerns and challenges identified.

The second pillar of assessment (i.e. based on stakeholders' involvement) follows seven steps: (i) identification of the research topics for the quantitative analysis; (ii) performance of a first round of quantitative analysis; (iii) redefinition of the research topics; (iv) performance of a second round of quantitative analysis; (v) analysis and presentation of quantitative results; (vi) identification and engagement of experts; (vii) analysis of experts' feedback.

From both analyses, six privacy concerns, six security concerns and two ethics concerns have been identified (see Table 1).

Table 1 – Privacy, security and ethics concerns

Privacy concerns	Security concerns	Ethics concerns
Transboundary data flow and 5G	Network 'softwareisation' and flexibility	Lack of citizen awareness of the impacts of 5G on ethical aspects
High-speed data rate	Multiconnectivity and device density	Technology and use of personal data
High traffic density and location accuracy	Protocols and interoperability	
Huge number of connected devices (IoT)	Identifiers and encryption	
Internet protocol (IP)	New infrastructures and frameworks	
Privacy as open issue	Cybersecurity standards	

Identifying the concerns listed in Table 1 permitted a gap analysis of the current technical specifications (which are still under definition at the time of writing) and regulations. On this basis, the authors have put forward potential enhancements for the next releases of technical specifications and regulations (see Table 2).

Table 2 – Policy options

Policy options for privacy concerns	Policy options for security concerns	Policy options for ethics concerns
5G ecosystem parties establish controller/processor in the European Economic Area (EEA)	Consider standards for network components	Provide democratic access to information about 5G
Adopt hybrid data location store	Consider compulsoriness of security controls	Promote critical thinking about data practices in the 5G ecosystem
Adopt personal data wallet	Monitor the evolution of multi-connectivity	Produce an ethics regulatory framework for 5G
Revise data breach notification deadline	Facilitate collaboration to contribute to new protocols	Adopt indicators to measure the multidimensional societal impacts of 5G
Establish continuous consent	Foster the resolution of interoperability issues in new protocols and regulations	Promote accountability, trustworthiness and reliability of actors in the 5G ecosystem
Adopt state-of-the-art protection mechanisms	Adopt full, end-to-end anonymisation of subscribers' identity	Improve communication of 5G benefits
Consider 5G impacts in the final version of the proposed e-privacy regulation	Converge to new and standard cipher algorithms	
Consider a standard validation framework	Define clear roles for stakeholders	
Consider the impact of more attractive devices and services	Accelerate cybersecurity standards	
Observe evolutions of non-IP networking		
Monitor privacy aspects		
Ensure data sovereignty		

Identified opportunities, concerns and policy options are illustrated in three case studies, selected from the different domains that the experts involved considered to be most relevant: (i) vehicle-to-

everything in the automotive sector; (ii) factory-of-future in the manufacturing sector; and (iii) e-health in the health sector. These case studies provide evidence of the envisaged opportunities, in terms of societal benefits, for a sustainable development of 5G technology, as well as in terms of specific regulatory and specifications gaps to be addressed and mitigated with the suggested policy options. In other words, case studies represent a bridge between the impact assessment and the final policy options.

The whole analysis of this research study flows into the policy options defined at the end of this document. These are meant to inform the EU institutions and/or Member States about privacy, ethics and security concerns, as well as future potential improvements.

The analysis performed by this research study is based on currently available releases of the 5G technology specifications, updated in September 2021.

Table of contents

1. Introduction 1

1.1. 5G technology overview 3

2. Privacy and security in the context of 5G technology 4

2.1. Relationship between security and privacy 5

2.2. Privacy and data protection legal framework 7

3. Document-based impact assessment 8

3.1. Privacy risks and challenges 8

3.1.1. Transboundary data flow and 5G 8

3.1.2. High-speed data rate 9

3.1.3. High traffic density and location accuracy 10

3.1.4. Large number of connected devices (IoT) 11

3.1.5. Internet Protocol (IP) 12

3.1.6. Section summary: Policy options for privacy risks and challenges 13

3.2. Security and cybersecurity legal framework 13

3.3. Security risks and challenges 15

3.3.1. 5G Service-Based Architecture 16

3.3.2. Network softwarisation and flexibility 17

3.3.3. Multiconnectivity and device density 17

3.3.4. Protocols and interoperability 18

3.3.5. Identifiers and encryption 19

3.3.6. New stakeholders and frameworks 20

3.3.7. Section summary: Policy options for security risks and challenges 20

3.4. Cybersecurity, robotics and AI: relationship with 5G technology 21

4. Impact assessment based on stakeholders' involvement 22

4.1. Step 1 & 3: Identification of research topics 22

4.2. Step 2 & 4: Analysis of the interest in 5G technology ____ 22

4.3. Step 5: Quantitative analysis and results ____ 23

4.4. Step 6: Engaging experts ____ 25

4.5. Step 7: Gathering and analysing feedback from experts ____ 26

5. Case studies ____ 29

5.1. Vehicle-to-everything to reduce road-traffic-injuries ____ 30

5.2. Factory-of-future to reduce job-related-injuries ____ 32

5.3. eHealth to prevent diseases and ensure healthy lives ____ 33

6. Final policy options ____ 35

6.1. Feasibility of 5G technology adoption vs privacy and security risks ____ 35

6.2. Effectiveness of 5G technology through standardisation ____ 35

6.2.1. Promoting privacy and security standards ____ 35

6.2.2. Promoting ethics standards ____ 36

6.3. Sustainability of 5G technology driven by trustworthiness ____ 36

6.3.1. Enhancing the legal and regulatory framework ____ 36

6.3.2. Ensuring trust and control for future generations of 5G ____ 36

6.3.3. Supporting trustworthy investments by creating an EU public culture of technology ____ 37

7. Conclusions ____ 38

Annex – Experts engaged ____ 41

List of figures

Figure 1: Research study structure 2
Figure 2: Evolution of mobile networks 3
Figure 3: Research conceptual map 4
Figure 4: Threat modelling with STIX 15
Figure 5: High-level architecture of 5G networks 16
Figure 6: Sentiment Analysis - 1st set of results 23
Figure 7: Sentiment Analysis – 2nd set of results 24
Figure 8: Identification and engagement of experts 25
Figure 9: Judgement on citizens' concerns 26
Figure 10: 5G impacted sectors, estimation for 2026 29
Figure 11: V2X case study 30
Figure 12: FoF case study 32
Figure 13: eHealth services powered by 5G 33

List of tables

Table 1: Privacy, security and ethics concerns II
Table 2: Policy options II
Table 3: Policy options for privacy risks and challenges 13
Table 4: Policy options for security risks and challenges 20
Table 5: Concerns and policy options 38

List of abbreviations

3G	Third-generation mobile network
3GPP	Third-generation partnership project
4G	Fourth-generation mobile network
5G	Fifth-generation mobile network
AI	Artificial intelligence
a.k.a.	also known as
AHWG	Ad Hoc Working Group
API	Application programming interface
B2B	Business to business
B2C	Business to consumer
B5G	Beyond fifth-generation mobile network
CCAM	Cooperative connected and automated mobility
C-ITS	Cooperative intelligent transport systems
CJEU	Court of Justice of the European Union
CN	Core network
Cobots	Collaboration robots
CP	Control plane
CTI	Cyber threat intelligence
DN	Data network
DPIA	Data protection impact assessment
EEA	European Economic Area
ECCG	European Cybersecurity Certification Group
eNB	Evolved Node B – base station in 4G networks
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
FoF	Factory-of-future
GDPR	General Data Protection Regulation (Regulation EU 2016/679)
gNB	g Node B – base station in 5G networks
GSMA	Global system for mobile communications
GUTI	Global unique temporary identifier
IMCO	Committee on the Internal Market and Consumer Protection
IoT	Internet of things
IP	Internet protocol
ITS	Intelligent transport systems

ITU	International Telecommunication Union
JURI	Committee on Legal Affairs
LBS	Location based services
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MANO	Management and network orchestration
MEC	Multi-access edge computing
MIMO	Multiple-in multiple-out (MIMO antennas)
ML	Machine learning
MNO	Mobile network operators
NFV	Network functions virtualisation
OSI model	Open systems interconnection model
PNT	Positioning navigation and timing
RAN	Radio access network
RRI	Responsible research and innovation
RTLS	Real-time location service
RTL	Real-time location
SA	Sentiment analysis
SAT	Social acceptance of technology
SBA	Service-Based Architecture
SCC	Standard contractual clauses
SCCG	Stakeholder Cybersecurity Certification Group
SEDE	Subcommittee on Security and Defence
SSI	Self-sovereign identity
STIX	Structured threat information expression
STL	Seasonal trend decomposition using loess
STOA	Science and Technology Options Assessment
SUCI	Subscription concealed identifier
Tb/s	Terabit per second (1 terabit = 1 000 gigabit = 1 000 000 megabit)
TIA	Transfer impact assessment
UP	User plane
UX	User-experience
V2X	Vehicle to everything
WSR	Wireless service robots
WTS	Wireless tele surgery
ZSM	Zero-touch network and Service Management

1. Introduction

An increasingly large share of the ballooning global population accesses services via the web. Indeed, accelerated by the Covid-19 pandemic and driven by the by-now billions of connected internet of things (IoT) devices, [1] worldwide traffic peaked at 700+ terabits per second in 2020 [2]. More than 73 % of these accesses were performed ''while on the move'' [3] (i.e. through mobile phone networks or wireless connections). The sheer size of this traffic overburdens and strains existing networks, thus making the case for their upgrade. The fifth-generation mobile network (5G) is expected to respond to these growing needs in Europe and beyond. The intended outcome is for 5G to connect everyone and everything, anywhere. A reduction in the digital divide and the provision of unrivalled network performances should deliver positive ripple effects throughout society, which range from efficient and sustainable manufacturing and logistics processes to reliable and resilient facilities for healthcare and safety services. For this reason, 5G technology is viewed as a cornerstone of European resilience and is one of the seven flagship areas of the European Recovery and Resilience Facility [4].

To ensure this outcome, 5G advances a two-pronged strategy. First, 5G will offer a connectivity platform across different sectors of society to enable use cases that can disrupt traditional processes and improve humans' quality of life by making living environments smarter and safer. This improvement would be unattainable without the active and responsive IoT devices of today. Second, 5G re-envisions the network as a **dynamic** infrastructure that adapts to the changing requirements of the applications, and not vice versa. This revolutionary concept is stressed as a key characteristic, dubbed **purposeful**, in the specification of future generations of mobile networks beyond 5G. Purposeful networks are those that are driven by specific use cases and applications.

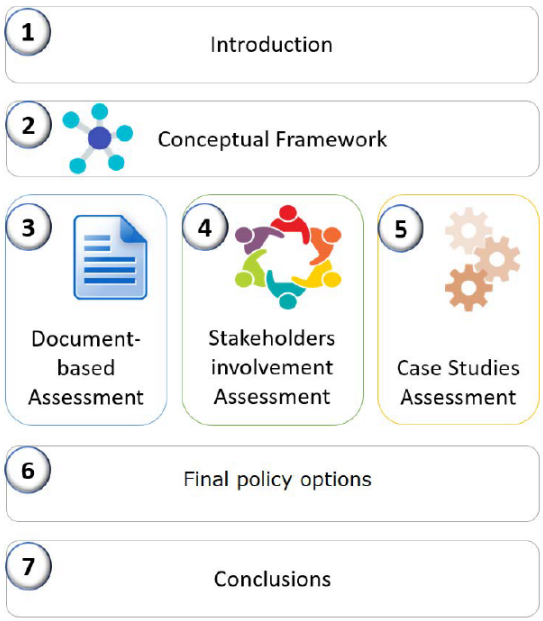
The unrivalled capability and flexibility of 5G has been made possible by a decades-long process of convergence between computing and telecommunications. Each discipline focused on a complex system with specific stakeholders, rules, processes, technologies and experiences. Their merger brings to light a new **ecosystem** [5], where telecommunications and computing collaborate to enable new scenarios, and where the two systems' stakeholders can extend their business offering and compete with each other.

Throughout this ongoing epochal shift, a wide debate around privacy and security has unfolded. **Privacy** is a fundamental right of any citizen, and it is ensured and strengthened by a wide and continuously evolving regulatory framework, both within Europe and outside, guaranteeing the right of individuals (data subjects) to own and control their personal data and to safeguard their individual identities.

On the other hand, **security** in the digital world establishes rules and measures for safeguarding data and, consequently, the trustworthiness of the ecosystem, thanks to the provision of reliable access to data by authorised persons only (**availability**) and the protection of stored and exchanged information from unauthorised access (**confidentiality**) or from unauthorised modification (**integrity**).

Having stated the crucial need to ensure human fundamental rights such as privacy, this paper describes the results of a research study focused on the privacy and security aspects of 5G technology. During this study, definitions, regulatory frameworks, risks, challenges and opportunities were investigated.

Figure 1 – Research study structure



Source: CyberEthics Lab.

The research study (see Figure 1) starts with an introductory section on the key aspects of 5G technology and its complex ecosystem (section 1).

Section 2 illustrates privacy and security in the context of 5G, describing the conceptual map and identifying four categories of potential concerns, risks and challenges (i.e. technologies, privacy, security, ethics/politics) to be used in the impact assessment methodology carried out in the successive sections.

Considering the many implications between the two objects of investigation – privacy and security – section 3 presents the landscape of the technical and legal frameworks for both concepts and highlights the risks and challenges that need to be addressed. This section is the first pillar of the assessment of 5G technology implications for privacy and security. A first list of policy options is suggested to mitigate and address the analysed risks and challenges.

In parallel, the study edifies a second pillar of assessment (section 4) based on the involvement of stakeholders (i.e. citizens and experts) through quantitative and qualitative analyses. The section opens with a description of the methodological approach and the seven steps undertaken to carry out two kinds of analyses: a quantitative sentiment analysis (SA) across the four impact assessment categories (i.e. technologies, privacy, security, ethics/politics) identified in the research conceptual map as key topics for gathering public interest, and a qualitative analysis through the engagement of expert judgement. The SA is performed on Google Trends data in order to measure the change in the general interest for the 5G technology over a five-year period (2016-2021). The results of the SA are the input for preparing the following qualitative analysis with experts. All the collected information is processed and analysed to identify further policy options.

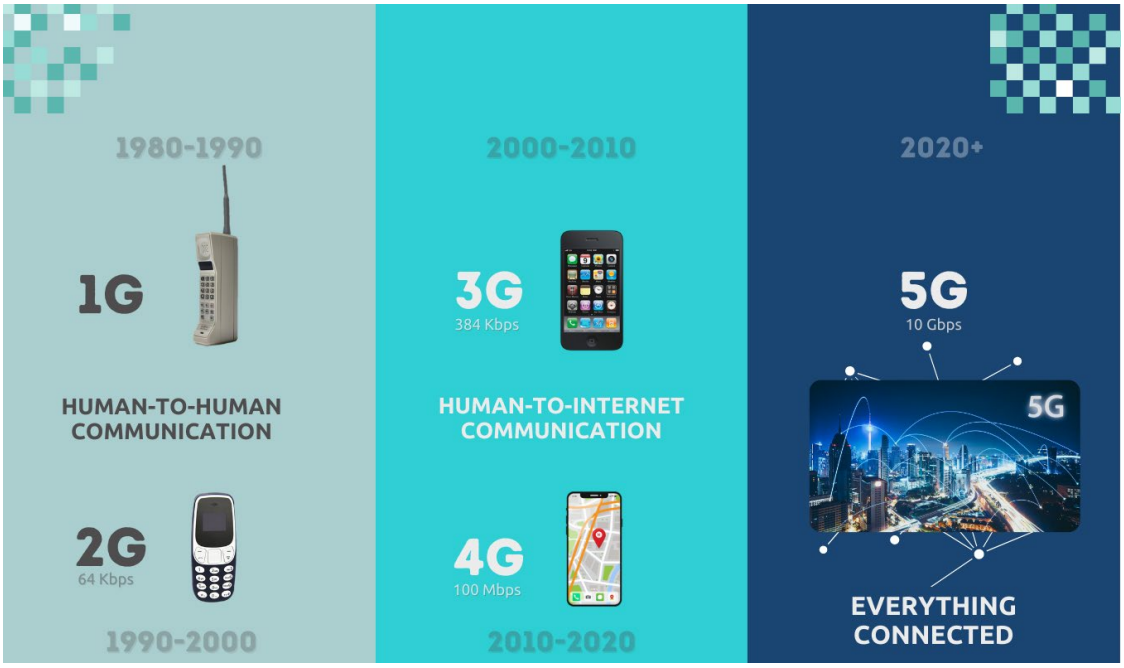
The analysis conducted in the first two assessment pillars constitutes the knowledge base for both analysing relevant use cases enabled by 5G and their impacts (section 5) and defining final policy options (section 6).

This paper is added to the 5G series of the Panel for the Future of Science and Technology (STOA) addressing impact analysis of 5G from different perspectives (including inter alia health and environmental).

1.1. 5G technology overview

Outside experimental settings, five generations of mobile networks with ever-increasing data speeds have been deployed over the last four decades. While each is characterised by specific standards, protocol stacks, technology architectures, and radio modulation schemes, the five generations can be divided into three distinct groups based on which additional services they enable. As shown in Figure 2, mobile networks have evolved from connecting people to connecting machines. Indeed, in the 5G paradigm, humans are no longer considered as necessary end points of network communication, which instead can potentially involve machines only, i.e. the internet of things (IoT).

Figure 2 – Evolution of mobile networks



Source: CyberEthics Lab.

While the leap between previous mobile network generations was made possible by extended spectrum usage and more efficient protocols and modulation schemes, 5G's essential innovation that ensures that 'everything is connected' consists in the 'softwareisation' of communication networks, their components and their functionalities.

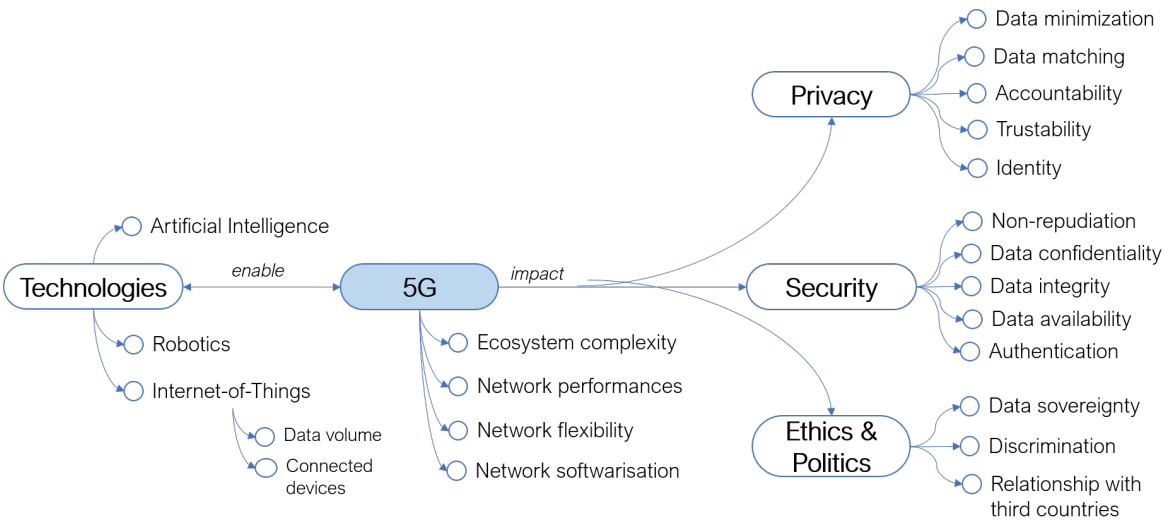
This 'network softwareisation' is made possible thanks to advances in cloud computing, which have led to a proliferation of related infrastructure. Thanks to the network virtualisation, 5G is able to:

- provide on-demand specific level of services (i.e. more security, more speed, less latency, more capacity density) to each user, by enacting a personal 'slice' of the network with the required conditions;
- shift data processing close to the data source (edge computing). This allows latency to be reduced and affords the opportunity to implement privacy-by-design and security principles where data are gathered and collected.

2. Privacy and security in the context of 5G technology

The complexity of the 5G ecosystem requires a deep insight into its main components, and especially how each component interacts with each other impacting privacy and security aspects. Thus, in order to describe privacy and security aspects in the context of the 5G ecosystem, this research activity starts by defining the conceptual map with key aspects and relationships to be analysed (see Figure 3).

Figure 3 – Research conceptual map



Source: CyberEthics Lab.

The research conceptual map provides the four categories of the impact assessment carried out in next sections.

As mentioned in section 1, **5G** may be considered as a complex ecosystem that has a strong relationship with other relevant **technologies**, specifically **artificial intelligence** (AI), **Internet of Things** (IoT) and **robotics**. A number of reasons have led us to focus on these technologies. AI is an enabling technology for governing the complexity of the 5G network and its resources [6], as well as to perform threat and anomaly detection [7] and predictive maintenance operations. Therefore, undoubtedly AI development will be boosted and enhanced to enable key features requested by 5G such as: (i) 5G resource management based on quality of service and flexible contracts with the customers; (ii) improved predictive threat detection. Consequently, AI will derive benefits as well.

Conversely, robotics and IoT are 5G-enabled technologies, and their wider deployment will be supported by the better performances made possible thanks to the flexibility and programmability of the 5G network. To achieve these relevant characteristics, 5G leverages concepts and mechanisms successfully crafted for and deployed in computing technologies, and now made available by the integration of these technologies in communication systems. Specifically when it comes to performing routing and other networking functionalities, computing technology allows the replacement of hardware equipment with a software layer. This layer enables the sharing of physical resources by executing functions in virtual machines.

On the one hand, this mix of components improves communication network in terms of flexibility, capability and reliability and accelerates the race towards a digital society. On the other hand, it has

to be put under observation for the introduction of novel privacy and security risks and challenges deriving from those accelerations.

Moreover, the complexity of the 5G ecosystem is characterised by the interconnection of heterogeneous stakeholders, namely the main players of the two constituting systems, i.e. computing (cloud and service providers) and communication networks (telecommunication operators, providers of connectivity solutions, equipment, and software). For this reason, the 5G ecosystem is defined as a multi-actor ecosystem [5], and all its involved actors may play different roles at different times, especially during the initial phase of 5G deployment, when each has specific expertise for supporting specific use cases. The actors on this stage are a sample of global companies that, thanks to their scale, can fluidly execute different functions in the communication flow. In other words, the fact that specific actors play one or more pivotal roles in the 5G ecosystem, can raise **ethics** and **political** risks that range from the undermining of relationships among countries to the systematic discrimination of groups of citizens. For instance, hyperscalers that provide cloud, networking and internet services could be relevant actors in 5G networks and consequently data might flow out of national borders.

In addition, traditional **security** mechanisms, enacted for protecting data from unauthorised operations and ensuring proper availability, cannot be applied without considering the factors (e.g. heterogeneity of domains, multiplicity of stakeholders, technologies and consolidated practices) that contribute to the composition and future evolution of the 5G ecosystem. Virtualisation of the network and changes in architecture are blurring the boundaries between Radio Access Network (RAN) and Core components, making possible to programme and arrange specific network capabilities based on specific needs of the applications, and this flexibility can be offered on-demand as well. This programmability can be exploited to reconfigure the network in case of issues and threats, improving its resilience. However, this flexibility and ad-hoc definition of functionalities without a clear distinction may introduce uncertainty in the identification of potential threats. Indeed, ambiguity on functionalities and lack of constraints in the technical specifications might incentivise service providers to not implement and deploy separations of functionalities among components, usually recognised as best practices, and this might be exploited to infer cyberattacks among components.

2.1. Relationship between security and privacy

Privacy is a term that calls to mind the concept of interference with the personal sphere from prying eyes that might spy from the keyhole, or ears that might eavesdrop through the wall. These two unfair actions harm individuals' dignity and freedoms. For this reason, the **right to privacy** is a

Article 8 - Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

Source: European Convention of Human Rights

https://www.echr.coe.int/documents/convention_eng.pdf

fundamental right aimed at protecting individuals and it is recognised both at the international level, with the Universal Declaration of Human Rights proclaimed in 1948 by the United Nations, and at the European level, with the European Convention of Human Rights defined in 1950 by the Council of Europe and the Charter of Fundamental Rights of the European Union.

In the context of 5G, mainly characterised by digitalisation and data communication, the term privacy assumes the specific meaning of respect and protection of individuals with regard to the processing of their personal data. The EU's General Data Protection Regulation (GDPR) [8] is a fundamental cornerstone that provides individuals (a.k.a. data subjects) with rules and tools to exercise their rights. With GDPR, individuals have to be explicitly and comprehensively informed on why and how their personal data are collected, processed and stored. Based on this information, individuals are able to decide and provide their consent to data treatment.

Those responsible for collecting, processing and storing data (data controllers/processors) have to establish all the necessary rules and deploy the right tools to protect data from unauthorised operations and from the undermining of data authenticity, integrity and confidentiality. These rules and tools belong to data security.

In light of these above clarifications, privacy, data protection and security cover different aspects that partially overlap. Privacy is a fundamental right; data protection is a means of recognising such a right and security is a means of protecting such a right. All of them need specific safeguards throughout the design and validation of systems for data treatment, as 5G will be.

In this context, compliance with ethics principles and the relevant legal framework on privacy and security (see sections 2.2 and 3.1.6) has to be guaranteed by adopting 'privacy-by-design' and 'security-by-design' principles, as well as the following considerations:

- Where legal and regulatory compliance is ensured, the question of fairness or goodness of a product/service or process should not be put on the back burner: legal compliance does not necessarily imply ethical behaviour. To this extent, it is thus necessary to promote and spread **ethics-by-design** methodology, which is not an ethics assessment of results 'a posteriori', but a systematic embedding of ethical considerations at every stage of the service/product development, from design to delivery and operation.
- The application of this methodology has to take into account needs of all the stakeholders (e.g. project sponsors, developers, operators, consumers, citizens) through their **engagement**. It necessarily requires an appropriate **communication** about the problems to be addressed and how the envisioned solutions solve those problems. In other words, the benefits, risks and rationale of the solutions should be made clear during decision-making processes across the service/product lifecycle. This consideration, that is a best practice in project management [9], will create a culture of responsible innovation, might maximise the impact of its activities, and reduce barriers against distrust and **social acceptance** of technology.
- **Transparency and accountability** should be inherently part of the risk identification and assessment processes: if the benefits, risks and the rationale cannot be understood by each stakeholder, or if roles and accountability of technology and service providers are ambiguous or not explicitly defined, the process of introducing the envisioned solution should be refined with further details. Lack of either transparency or accountability might undermine the evolution of the market and the innovation themselves.

2.2. Privacy and data protection legal framework

The EU data protection legal framework is currently composed of the General Data Protection Regulation no. 2016/679 (GDPR) [8], the Directive (EU) no. 2016/680 [10], the Regulation no. 2018/1725 [11], and the proposal for ePrivacy Regulation [12]. This legal framework is agnostic with respect to the technology [5] that is it was not designed to regulate a specific technological solution, but rather to be applied to all activities involving personal data processing, regardless of their technical nature and status. To this extent, this legal framework represents a shining example worldwide in the protection of the fundamental rights to privacy and data protection, providing EU citizens with a flexible tool for regulating the processing of personal data.

> **Article 4 - Definitions**
>
> 'Personal data' means any information relating to an identified or identifiable natural person […], who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
>
> Source: GDPR [8]

The following section analyses potential privacy risks and challenges that might arise in the context of the 5G ecosystem with a particular focus on GDPR and proposal for ePrivacy Regulation.

3. Document-based impact assessment

3.1. Privacy risks and challenges

3.1.1. Transboundary data flow and 5G

As stated in section 1, 5G is an ecosystem where functions are executed on a mix of virtual and physical infrastructures, and for this reason 5G may require the cooperation of various providers located in Europe or abroad. This brings implications on privacy regulations that must be considered for two different reasons.

On the one hand, the Regulation (EU) 2016/679 has extended the European Union ('EU') territorial privacy borders: compliance with the GDPR is mandatory both for legal persons based in the EU and those based abroad. Article 3, paragraph 1 of the GDPR states that it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not[1]. On the other hand, the GDPR imposes limitations on the transfer of personal data outside the EU to third-party countries or international organisations in order to guarantee that the level of protection of individuals afforded by the GDPR is not undermined.

The EU has strongly influenced the adoption of other privacy laws similar to the GDPR outside the European Economic Area (EEA) by limiting the transfer of personal data from member states to countries without a level of privacy protection considered adequate by the European Commission. Only a few countries globally have adopted an equivalent level of protection of personal data to that guaranteed in the EU.[2]

In the absence of an 'adequacy decision', the most common tools companies use to transfer data outside the EEA are the recently updated Standard Contractual Clauses (SCCs) [13]. The new SCCs require parties to perform and document an assessment with regard to the planned data transfer.

This assessment, called 'Transfer Impact Assessment' (TIA), is mainly a risk assessment of the factors related to the data transfer into third countries, and that must also include an analysis of relevant laws in the third country for safeguarding the data.

[1] For the sake of clarity, GDPR rules apply to the European Economic Area (EEA), which includes all EU countries and non-EU countries like Iceland, Liechtenstein and Norway.

[2] For a complete and updated list of countries covered by adequacy decisions, please consult the following link https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

This concern has a high likelihood of occurrence, and it impacts on the politics aspect as well, specifically with data sovereignty and relationships with third countries.

Policy options for privacy risks and challenges:

- ***POP1 '5G ecosystem parties establish controller/processor in the EEA'*** *- Any organisation involved in the EU 5G ecosystem should establish a controller or a processor in the EEA and should encourage its own legal departments to perform a TIA.*
- ***POP2 'Adopt hybrid data location storage'*** *- A potential alternative path could be to adopt a hybrid approach, where personal or sensitive data is stored locally, close to and within national boundaries of the individual (edge cloud) and less sensitive data is stored in the cloud. This provides individuals (data subjects) with more access and control over their data, and they can decide where and whom to share it with.*
- ***POP3 'Adopt a personal data wallet'*** *– A personal data wallet, that is a digital area where individuals can access data, provide consent and receive notifications, could be considered as a fundamental tool for exercising the rights to privacy and data protection. Some fragmented examples and case studies are available from the literature* [112]*, as well as part of functionalities made available on government portals (e.g. personal digital identification service). However, an integrated and standardised approach could accelerate the path for the European digital single market. Special care has to be devoted to usability, accessibility and the processes to be enacted, in order to avoid digital-divide concerns and to ensure that no citizen is left behind. Innovation means rethinking not only the technologies themselves, but also the processes for applying said technologies. A personal data wallet would provide individuals (data subjects) with more access and control over their data, and the ability to decide where and with whom to share it.*

3.1.2. High-speed data rate

One of the expectations for 5G mobile networks is that they will be characterised by high data speed and low latency, which eventually results in a huge volume of data [14]. It could be argued that other technologies (e.g. Wi-Fi) provide high volume data transmission capabilities. Despite that, they do not guarantee the same data delivery times that 5G technology promises [15].

The risk related to data rate is related to the big data concept. Big data risks are generally associated with the 'three Vs' attributes: volume, velocity, and variety of the processed data. Volume refers to the amount of data processed, variety to the number and diversity of data types, while velocity refers to the speed of data processing [16].

However, 5G introduces an addition: the fast transmission is associated with the level of data sharing between the different stakeholders in the 5G ecosystem.

The likelihood of occurrence of this concern is high, considering that many connected devices, including wearable or under-the-skin devices (e.g. pacemakers), will be associated with each individual, as it will be shown in section 5.3.

If an advanced dynamic and continuous consent process is not established, the fast transmission and sharing of data might impact rectification and erasure rights, as well as the safeguard of mandatory notification of a data breach targeting the restriction of damage. Article 33 of the GDPR aims at data breach reduction by establishing a 72-hour deadline for companies to notify the supervisory authority of where the breach occurred. With higher speeds of data transmission, the 72-hour time limit to report to the supervisory authority might be too long, impacting the data subject rights [17].

Policy options for privacy risks and challenges:

- ***POP4 'Revise data breach notification deadline'*** *– The European legislator will have to consider a downward revision, based on higher speeds and data rate, of the time limit to notify breach.*
- ***POP5 'Establish continuous consent' –*** *5G technology providers will have to establish advanced dynamic and continuous consent processes and notifications, to ensure individuals' rights to rectification, erasure and notification.*
- ***POP6 'Adopt state-of-the-art protection mechanisms' -*** *5G technology providers will have to adopt the most advanced encryption systems, and anonymisation or pseudonymisation techniques, and to design high-speed alert systems in case of data breaches.*

3.1.3. High traffic density and location accuracy

Nowadays, Location Based Services (LBS) are popularly used. Most online apps on mobile devices require location information. Companies track the current location of the user in order to provide improved services. By doing so, they constantly monitor the habits and routines of the user [18]. Tracking people through their smartphones was also the key to contact tracing in the fight against the coronavirus disease 2019 (COVID-19) outbreak.

5G technology will use antennas with Multiple-In Multiple-Out (MIMO) technology, allowing denser and higher capacity than the current 4G technology [19]. Since higher frequencies will be adopted, 5G networks will have coverage cells of reduced size. This will allow an improved accuracy in the localisation of devices, and consequently, it will be easier to reveal the location information of the data subject [20]. For this reason, it is not surprising that one of the most relevant business scenarios exploiting 5G capabilities is based on Real-Time Location Service (RTLS), which exploits longer device battery life, accuracy of location information and terminal cost with respect to traditional technologies (e.g. Bluetooth and Wi-Fi).

As per the ePrivacy Regulation, location data is 'metadata'. The importance of this kind of data is particularly marked in the ePrivacy Regulation draft, where Recital (2) emphasises how 'metadata' allows precise conclusions regarding the private lives of the persons involved in electronic communication, such as their social relationships, habits and everyday activities, interests and tastes [21].

Moreover, the unregulated disclosure of position information has personal and societal impacts requiring specific solutions for their mitigation [22]. For this reason, the first draft of the ePrivacy Regulation article 6 (c) foresaw the legal processing of communications metadata only with end-user consent given for one or more specified purposes [21]. However, the last draft seems to permit further metadata processing for specified, explicit and legitimate purposes [23].

3.1.4. Large number of connected devices (IoT)

Lower latency in 5G technology means more connected devices. According to the Global System for Mobile Communications (GSMA), 5G connections will grow from 500 million at the end of 2021 to 1.8 billion by 2025 [24]. 5G will have a potentially disruptive impact in several areas, including inter-alia: (i) from self-driving vehicles to smart grids for renewable energy, reduced traffic congestion, greenhouse gas emissions, and road-traffic-injuries; (ii) from smart cities and smart homes to the healthcare field through Wireless Tele-Surgery (WTS) and Wireless Service Robots (WSR); (iii) from collaborative robots to factories of the future for improving energy and resource efficiency, waste reduction, and less injured workers.

Policy options for privacy risks and concerns:

- ***POP7 'Consider 5G impacts in the final version of the proposed e-privacy regulation'*** – *European policy-makers will have to consider the impact of 5G technology when approving the final version of the proposed e-privacy regulation. On the GDPR side, 5G providers will have to adopt the most advanced encryption systems, anonymisation or pseudonymisation techniques, or obfuscation techniques for reducing the quality of location information, as well as carrying out Data Protection Impact Assessments ('DPIA'), a mandatory and valuable tool for recognising the risks of controlling and processing users' location information and for mitigating the large-scale impacts of such processing.*

Notwithstanding the number of possible fields of application, the Internet of Things (IoT) and the associated technologies that can be applied to connected objects are always associated with the same kind of architecture: data needing to be transported, stored, processed and made available [25].

If this massive amount of data involves personal data, the exercise of the data subject's rights becomes cumbersome or impracticable. This scenario has a high likelihood of occurrence, considering that each individual will have a number of associated connected devices for a wide number of activities, such as smart watches, vehicles, and domestic whitegoods. Data matching and correlation from data gathered from each of these devices can generate information on behaviour, habits, interests, and so on. In the worst case, correlation and information extraction can be wrongly biased, and damage or discriminate individuals, groups and communities. In case of such damage, someone will need to be held accountable, in order to mitigate widespread feelings of dissonance between the touted expectations of a technology and its actual implementation. Some argue that the legal mechanism of Data Trusts could be a solution. Indeed, connected by a fiduciary obligation of undivided loyalty, the data trustees would exercise the data rights conferred by the GDPR on behalf of the Trust's beneficiaries. In that way, an independent intermediary would be introduced between data subjects and data collectors [26].

Although the trust mechanism could be an innovative solution in managing large amounts of personal data, it may not be compliant with the GDPR, which only grants data subjects (or heirs in some national regulations) the exercise of their rights.

Another approach could be based on Self-Sovereignty Identity (SSI), an emerging concept associated with the way identity is managed in the digital world. According to the SSI approach, users should be able to create and control their own identity, without relying on any centralised authority [27]. SSI offers users ownership and full control over their personal data and ensures anonymity. However, the concept of SSI cannot be extended to specific areas where third-party authentication is necessary (e.g. public administrations, banks).

In any case, IoT developers should always apply the data minimisation principle, which states essentially that any data processing activity should only use the minimum amount of data necessary. Also, the data collected should not be used for any other purpose or process without consent from the data subject.

Issues related to IoT are extremely important both for privacy and for cyber protection, especially of vulnerable people and children.

Just think about a smart TV or console that streams the favourite kids' shows with a voice-activated speaker and interacts with a game console featuring virtual-reality technology. Parental control issues, addressed already in 4G networks, will increase with 5G technology because of the number of connected devices and because of new applications made available from the media and entertainment sector, which will offer an unprecedented immersive user experience. According to article 8, paragraph 2 of the GDPR, the consent concerning the offer of information society services to a child below the age of 16 years shall be given or authorised by the holder of parental responsibility for the child (the Member States may provide by law for an age no lower than 13).

It is an arduous challenge to ensure parental consent in practice when several family members own and manage many smart devices through various accounts (that are often conformed to be used by adults). There is a need to create greater awareness of the risks to children's privacy. Last but not least, according to [3] most of the connected users are young people and minors.

The introduction of codes that establish rules for online service providers could be a valid solution. The Children's code (or the Age appropriate design code [28]) adopted in the United Kingdom might be considered a valuable example. The code applies to services that can include inter-alia: connected toys, games, educational technology, and online retail and for-profit online services such as social media and video sharing platforms that have a strong pull for minors. It contains fifteen standards that online service providers need to follow in order to comply with their obligations under data protection law to protect children's data online [28].

Policy options for privacy risks and challenges:

- ***POP8 "Consider a standard validation framework"*** *- New European legislation will have to consider the impact of such a human-unmanageable number of connected devices, and how data matching, correlation and information extraction will be performed to profile and track users through their devices. Device and service providers should apply privacy-by-design principles, mainly data minimisation (justified collection based on the purpose). However, standard validation frameworks have to be considered in order to provide independent third parties with appropriate tools for validation purposes.*
- ***POP9 "Consider the impact of more attractive devices and services"*** *- The European legislator will have to consider the impact of more attractive devices and services available from the media and entertainment sector, and that most of the users are minors. Parental control alone is not an effective solution, and ethics principles at the design phase of the services need to be considered, as per the Age appropriate design code.*

3.1.5. Internet Protocol (IP)

5G mobile communication technology is still IP-based [18]. It is well known that, in certain circumstances, both dynamic and static IP addresses, as identifiers, are personal data. When a device is assigned a static IP address, the address does not change; vice versa, when devices use dynamic IP addresses, they connect and change over time. Dynamic IP addresses may constitute 'personal data' when a third party (e.g., an Internet Service Provider) holds additional information (e.g., account details) that can be used to link those dynamic IP addresses to the identity of the relevant individual [29].

However, the European Telecommunications Standards Institute (ETSI) has launched a new group on non-IP networking addressing 5G new services. This group is looking for candidate technologies that may serve their need better than the TCP/IP-based networking used in current systems, overcoming limits experienced in 4G in terms of throughput and latency, and it intends to develop standards that define technologies to make more efficient use of capacity, have security by design, and provide lower latency for live media [30]. For its implications in security aspects, further details of this topic are available in section 3.1.6.

Policy options for privacy risks and challenges:

- ***POP10 'Observe evolution of non-IP networking'*** *– New European legislation will have to observe the evolution and outcomes from the ETSI working group on non-IP networking addressing new 5G services.*

3.1.6. Section summary: Policy options for privacy risks and challenges

Based on available technical specifications and scientific literature, the first 5G technology impact assessment pillar identifies five main risks/challenges with respect to the privacy dimension. This research study suggests ten policy options to mitigate and address them. Table 3 summaries the analysed privacy concerns and related policy options.

Table 3: Policy options for privacy risks and challenges

Privacy risk/challenge	Policy option identifier	Policy option title
Transboundary data flow and 5G	POP1	5G ecosystem parties establish controller/processor in the EEA
	POP2	Adopt hybrid data location store
	POP3	Adopt personal data wallet
High-speed data rate	POP4	Revise data breach notification deadline
	POP5	Establish continuous consent
	POP6	Adopt state-of-the-art protection mechanisms
High traffic density and location accuracy	POP7	Consider 5G impacts in final version of the proposed e-privacy regulation
Huge number of connected devices (IoT)	POP8	Consider a standard validation framework
	POP9	Consider the impact of more attractive devices and services
Internet Protocol (IP)	POP10	Observe evolutions of non-IP networking

3.2. Security and cybersecurity legal framework

In 2013, the '**Cybersecurity Strategy of the European Union – an Open, Safe and Secure Cyberspace**' was launched with the aim to enhance security in cyberspace and to set out the actions required for achieving cyber-resilience objectives, supporting the internal market, boosting the security of the EU and drastically reducing cybercrime. With this launch, the EU promoted a more uniform legislative approach to tackle cybersecurity threats, particularly those having cross borders dimensions.

In this light, the Directive on Security of Network Information System EU 2016/1148 (a.k.a. '**NIS Directive**') [31] and the Regulation (EU) 2019/881 [32] (a.k.a. '**Cybersecurity Act**') have been

adopted. The first one provides legal measures to increase the overall level of cybersecurity in the EU; the second one introduces the first EU certification scheme for ICT digital products, services and processes.

Under the NIS Directive, the Network and Information Systems Cooperation Group was established to ensure cooperation and information exchange among the Member States. The Group aims to achieve a high standard of security for network and information systems in the European Union by supporting and facilitating strategic cooperation and exchange of information among EU Member States and by providing several non-binding guidelines to the EU Members States to allow effective and coherent implementation of the NIS Directive.

Among the guidelines, the Group has published several documents relating to the cybersecurity of 5G networks, including:

- a risk assessment of 5G networks [33] [34];
- a toolbox of risk-mitigating measures for 5G networks [35];
- and a report on the progress of Member States in implementing measures from the toolbox [36].

The **risk assessment of 5G networks** represents the first step in a process aimed at ensuring the solid and long-term security of 5G networks. As mentioned previously in this document, 5G has a wide and heterogeneous list of stakeholders coming from the two complex systems merged together in the 5G ecosystem, i.e. mobile network operators (MNOs), service and product providers (e.g. telecom equipment manufacturers, cloud infrastructure providers, systems integrators, security and maintenance contractors, transmission equipment manufacturer, manufacturers of connected devices and related service providers), and other stakeholders including service and content providers and end-users of 5G mobile networks.

This complex and 'entangled' group of stakeholders might be enticed to collaborate against potential attackers. However, there exist several, non-trivial differences in their approach to business. For instance, several mobile network operators deploy and manage their networks using multiple equipment suppliers, while others rely on a single supplier for the majority of their network. Those suppliers are not necessarily headquartered in the EU, and this fact leads to well-known threats of cyber espionage and cyber warfare, potentially made possible hidden malware in the equipment provided. In general, 5G networks present a number of threat scenarios such as local or global 5G network disruption (**Availability**), spying of traffic/data in the 5G network infrastructure (**Confidentiality**), modification or rerouting of the traffic/data in the 5G network infrastructure (**Integrity, Confidentiality**), destruction or alteration of other digital infrastructures or information systems through the 5G networks (**Integrity, Availability**).

The **toolbox of risk-mitigating measures for 5G networks** aims to identify possible common measures to mitigate the main cybersecurity risks of 5G networks and provide guidance for selecting measures that should be prioritised in mitigation plans at the national and the Union level [35]. These are not mandatory measures because the roll-out and operation of 5G networks is a matter of national security. Risk mitigation measures can be strategic or technical. Strategic measures are potentially highly effective in addressing certain 5G cybersecurity risks identified in the EU-coordinated risk assessment report. They cover increased regulatory powers for authorities to examine network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities (e.g. risk of interference by a third country), as well as possible initiatives to foster a sustainable and distinct 5G supply chain in order to avoid systemic, long-term dependency risks.

In conclusion, the toolbox recommends that all member states strengthen security requirements for mobile network operators (e.g. through stricter access controls, rules on secure operation and monitoring, limitations on outsourcing of specific functions, etc.). Moreover, member states should assess the risk profile of suppliers applying relevant restrictions for those considered to be high risk and ensuring that each operator has an appropriate multi-vendor strategy in order to avoid or limit any significant dependency on a single supplier or on suppliers with similar risk profiles.

As per best practices in risk management, risk assessment has to be continuously performed in order to catch new potential threats and evaluate the effectiveness of applied policies. This is mandatory specifically in the context of the still-evolving 5G specifications. Indeed, Release 17 [37] is expected to be available in March 2022 and followed by protocol coding in June 2022. To this extent, ENISA has published additional and updated guidelines, and specifically:

- a report on threat landscape for 5G networks [38];
- a report on security aspects in 5G Specifications [39]
- a 5G supplement to the Guideline on Security Measures [40]

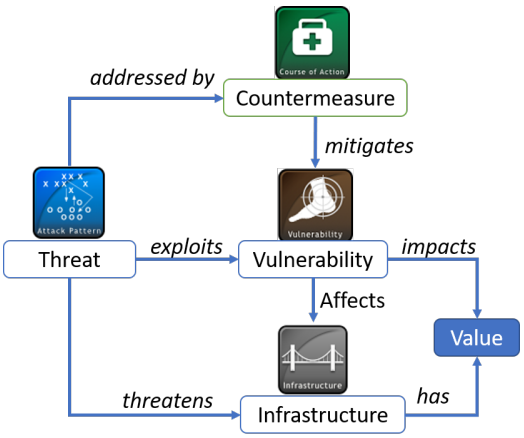
Recognising the importance to address the risks related to the technical vulnerabilities of 5G networks with a unified approach, the European Commission requested ENISA to develop a candidate European cybersecurity certification scheme for 5G networks (EU 5G scheme). To achieve this goal, ENISA has launched a call for expression of interest for participation in an Ad Hoc Working Group (EU5G AHWG) [41].

3.3. Security risks and challenges

Technical reports [42], research papers [43, 44, 45] and institutional reports [38, 39] highlight how 5G technology is significantly improving the privacy and security of wireless networks, by widely introducing protection mechanisms in 5G specifications. These improvements in security specifications are still under revision process, and protocol coding details will be available in a stable version 17, expected in June 2022. Indeed, a high level of security is one of the five pillars of the 5G New Radio architecture, together with new radio spectrum, massive bi-directional antennas (MIMO), multi-connectivity and network flexibility.

To this extent, the analysis of security risks and challenges takes in consideration the latest version of the technical specifications: TS23.501 'System architecture for the 5G System' released in July 2021, TS 33.501 'Security architecture and procedures for 5G system' released in September 2021 (V17.3.0), and integrated with scientific publications. This paper adopts the STIX [46] (Structured Threat Information eXpression), a language and serialisation format used to exchange cyber threat intelligence (CTI), to formally model and describe the security risks in the context of 5G technology. The use of STIX has been growing over the last years, and its evolution is under the control of OASIS [47] (a non-profit standards bodies). STIX and ISO/IEC 27005:2018 'Information technology - Security techniques - Information security risk management' [48] have many similarities in the information model.

Figure 4 – Threat modelling with STIX

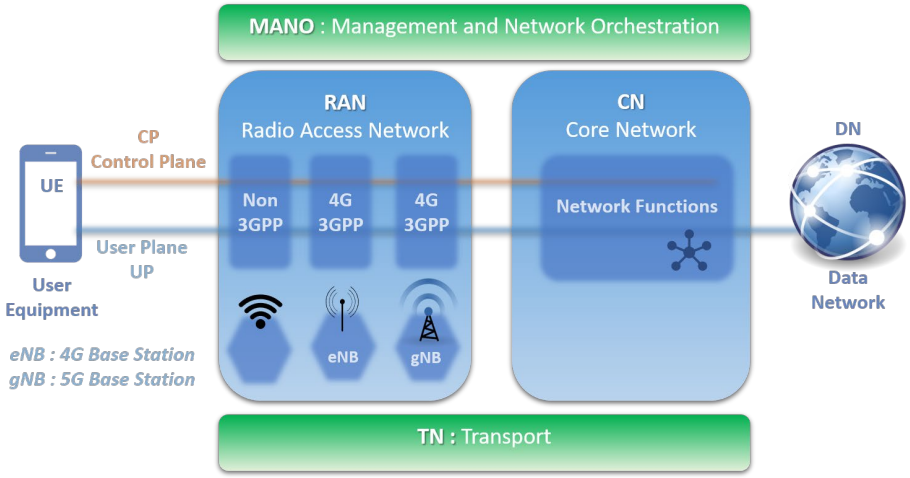


Source: CyberEthics Lab. based on [46]

3.3.1. 5G Service-Based Architecture

The 5G Service-Based Architecture (SBA) is the reference model for the 5G ecosystem, and it identifies four main component types (see Figure 5), i.e. (i) User Equipment (UE); (ii) Radio Access

Figure 5 – High-level architecture of 5G networks



Source: CyberEthics Lab. based on [37]

Network (RAN); (iii) the 5G Core (CN); iv) the Data Network (DN). Moreover, two layers (coloured green in Figure 5) provide interconnection functions (i.e. TN – Transport) and governance functions (i.e. MANO – Management and Network Orchestration) for all four components. It is important to highlight that these two layers include components that currently don't belong to 3GPP specifications.

Moreover, for the purpose of security risks analysis, two main communication channels referred to as planes are considered, namely the User Plane (UP) and Control Plane (CP). **User Plane** carries the user/connected device data, while the **Control Plane** (CP) deals with the control signalling traffic and interconnects any component in the 5G network architecture.

The Radio Access Network (RAN) represents the radio interface that provides wireless connectivity to devices and access to the 5G network through radio frequencies. RAN includes base stations (called eNB in 4G, and gNB in 5G) with antennas and other radio technologies, as well as the equipment to convert radio and digital signals. The 5G RAN will enable access to 5G equipment, as well as to current 4G devices and non-3GPPP technologies (e.g. Wi-Fi). This represents an opportunity to have a standard wireless technology for accessing the Data Network (DN) with everything, but this raises new concerns and challenges as detailed in the following sections.

The 5G Core Network (CN) provides all the network functionalities such as routing, authentication and policy control for enabling the communication within the accessed UE and the Data Network (DN). One of the most important innovations in the 5G architecture is the complete virtualisation of the Core Network [38], and this softwareisation of network functions will improve portability, scalability and flexibility of systems and services, but it will also raise new concerns and challenges.

All the components in the 5G SBA communicate through Application Programming Interfaces (APIs).

The following subsections analyse security concerns related to 5G technology

3.3.2. Network softwareisation and flexibility

Certainly, network softwareisation introduces many advantages in terms of flexibility, empowering network operators and service providers to select suitable solutions in a wider and more competitive market. Telecommunication operators have often considered as a vulnerability the use of hardware equipment from a reduced set of companies. Moreover, softwareisation represents a capacity to resist, mitigate or recover from a potential threat. Indeed, network functions can be scaled and replicated according to specific needs, therefore any node of the network might be opportunely reconfigured and scaled to hinder hazards in the system and its connected resources, as well as flexibly defined based on specific needs of the application served. However, the flip side of the coin is that specifications define as optional some security controls (e.g. lack of encryption of control plane data [38]) and physical deployment configurations (e.g. RAN and CN functions maybe potentially deployed on one site [49]), leaving a degree of freedom to providers on how to interpret, implement and utilise controls. This might blur the distinction of functions, roles and responsibilities of components in the architecture from a security perspective, by making more difficult the identification of potential vulnerabilities and threats, thus undermining the resilience of the network as a whole.

3.3.3. Multiconnectivity and device density

Policy options for security risks and challenges:

- ***POS1 'Consider standards for network components'*** *– Standard rules and procedures have to be considered to reduce ambiguities between network components.*
- ***POS2 'Consider compulsory security controls'*** *– Security controls cannot be considered optional in an architecture specification that claims to adhere to security-by-design principles.*

Network softwareisation in 5G technology will enable connection of new generation mobile devices (i.e. 5G devices), as well as ensure connectivity to devices, both 3GPP-based (e.g. 4G devices) and non-3GPP-based (e.g. Wi-Fi). This capacity is referred to as multiconnectivity and represents a step towards a standard wireless connectivity infrastructure. This is a relevant innovation and one of the five pillars of 5G, and for this reason it is expected that 5G will boost the deployment of IoT devices and enable the 'everything connected' mode, in which new, smarter scenarios are possible (e.g. factories of the future and connected robots, automotive and vehicle-to-everything, e-healthcare).

Security mechanisms have been deeply enhanced and strengthened, with stronger encryption algorithms and authentication protocols, but multiconnectivity might hide a wider set of new potential risks, deriving from interconnection with legacy systems that are not implementing the latest security guidelines. To this extent, even if protection mechanisms (e.g. proxies and Multi-access Edge Computing components) exist, legacy systems and non-3GPP connected devices might represent backdoors for potential attacks.

Moreover, virtualisation and the huge number of connected devices might represent a concern if exploited by threat campaigns that fraudulently clone virtual nodes (digital twins) of the network and route data traffic (both for eavesdropping and for jamming). This potential concern might be

Policy options for security risks and challenges:

- ***POS3 'Monitor the evolution of multiconnectivity'*** *– Evolution of multiconnectivity and related protection mechanisms has to be monitored by the service providers and frequently reported, in order to evaluate trends in attacks and the efficacy of protection.*

mitigated if predictive threat identification algorithms are able to preventively clone nodes, and therefore improve resilience of the network to attacks.

3.3.4. Protocols and interoperability

Network softwareisation will extend the use of IP-based protocol in 5G (see Section 3.1.5). This protocol was designed more than 40 years ago for worldwide connectivity, and 20 years ago its implementation was reviewed to ensure more addressable and connected devices. IP has always been based on data packets with a minimum set of data to be transmitted (e.g. header of data packet) and it is not efficient for IoT devices that perform frequent and short data communications. For this reason, specialised protocols have been defined for these devices, e.g. ZigBee and LoRaWan. Moreover, the IP-based protocol has many vulnerabilities (e.g. address spoofing, IP and source routing) that can allow attackers to get information about the sender and the receiver of a data packet, or to change the route of data, thus disrupting network communication in confidentiality, integrity and availability. In March 2020, ETSI launched a new working group on Non-IP Networking addressing 5G new services [30] in order to address the challenges of this new digital era where everything is connected, improving performances in terms of throughput, latency, interoperability and security. New protocols are under analysis for IP-based protocol replacement, and this challenge will represent another important revolution in communication networks.

Moreover, the need for the revision of protocols has to take into consideration the interoperability perspective, which is another relevant concern that might impede 5G effectiveness of and threaten its security. Even if 3GPP is specifying standard interfaces, protocols and messages among user equipment, radio access network and core components, gaps have to still be bridged since 5G will support use case scenarios from different domains (e.g. from automotive to healthcare).

Indeed, current specifications and standardisation efforts are focusing on the lower layers of the Open Systems Interconnection (OSI) model that are typically domain-independent, and specifically from the physical (defining the components enabling communication functions) to the session layer (defining how the interfaces of components interact). Intercommunication specifications are still not covering higher layers of the OSI model (i.e. presentation and application layers), where data syntax, semantics and relative security mechanisms have to be defined [50]. This lack of specifications and regulations might raise mismatches among applications of different domains and consequently interoperability issues. These issues, if not properly addressed, might undermine 5G technology since (i) applications from different domains might not dialogue (e.g. implementation of proprietary protocols); (ii) ambiguous interconnections might be interpreted as anomalous and consequently denied or (iii) the 5G network as a whole might be threatened by attacker nodes exploiting the protocol ambiguity and their lack of interoperability. In some cases, security concerns might impact privacy and safety of human beings, as well (see Section 5). To this extent, interoperability should be considered within the new regulations still under definition such as ePrivacy regulation or regulation for automotive cybersecurity [51].

Policy options for security risks and challenges:

- ***POS4 'Facilitate collaboration to contribute to new protocols'*** *– A common effort from all the stakeholders should be made to contribute to new protocols would be a game-changer in cybersecurity.*
- ***POS5 'Foster the resolution of interoperability issues in new protocols and regulations'*** *– Regulators and standardisation organisations have to consider interoperability among different applications within ongoing specifications, standards and regulations.*

3.3.5. Identifiers and encryption

As mentioned in section 3.3.1, according to current specifications, data encryption is ensured between gNBs (5G base stations) and User Equipments (UEs), while single operators have flexibility to implement it in the rest of the SBA. Based on throughput and latency constraints, encryption might be a barrier in many time-critical scenarios (e.g. automotive, remote-surgery), and for this reason, many functions might not implement encryption mechanisms. To this extent, RAN and Core are both critical components of SBA 5G networks, and as a result of this, gNBs might have full access to all data to and from devices in plaintext [49]. However, research on improved encryption mechanisms is moving forward with new efficient and effective solutions such as SNOW-V [52], a stream cipher offering 256-bit security that, thanks to its improvements in terms of throughput and latency, promises to be implemented as the encryption primitive in 5G, also in lightweight architectures.

Moreover, 5G has introduced relevant improvements in terms of protection mechanisms against the catching of identifiers, i.e. the capability of intercepting identifiers through eavesdropping.

The 4G mobile network uses one permanent identifier (called IMSI - International Mobile Subscriber Identity) and this identifier is exchanged in plaintext.

In 5G, three types of identifiers are exchanged through the protocol: (i) SUPI - Subscription Permanent Identifier (i.e. the identifier available from the device's 5G SIM card); (ii) SUCI – Subscription Concealed Identifier (i.e. the encrypted and concealed transformation applied to SUPI); and (iii) GUTI – Global Unique Temporary Identifier assigned by the 5G Core to the mobile device and periodically refreshed. However, only SUCI is encrypted, and so data exchanges between mobile devices and the 5G Core are at risk of eavesdropping at the onset of the communication.

Policy options for security risks and challenges:

- ***POS6 'Adopt full anonymisation of end-to-end subscriber identity'*** *– Stakeholders involved should make a joint effort to fully anonymise subscribers' identity end-to-end (i.e. from mobile equipment to core network).*
- ***POS7 'Converge to new and standard cipher algorithms'*** *– Stakeholders involved should make a joint effort to converge to new cipher algorithms, to be standardised for wider adoption in 'everything connected'.*

New stakeholders and frameworks

Current developments are moving towards the adoption of new infrastructures for extending the 5G (and beyond) network coverage, i.e. making available 5G connectivity in urban or rural areas indistinctly. This will reduce the current digital-divide, one of the main objectives of the European Commission.[3]

Network softwareisation will introduce global cloud service providers among stakeholders and their roles might change over time based on specific needs. However, if not appropriately controlled, third-countries cloud services could be interested to offer their services to European countries. This concern might raise instability in the market and represent a key political concern, but contemporarily might be seen as a trigger to foster European infrastructures, in order to avoid that specific classified or confidential information impact on national security concerns.

3.3.6. Section summary: Policy options for security risks and challenges

Policy options for security risks and challenges:

- ***POS8 'Define clear roles of stakeholders'*** *– Stakeholders involved should make joint effort to clearly define roles, and set up a constant collaboration to agree on the implementation of common security measure standards.*

Based on available technical specifications and scientific literature, the first 5G technology impact assessment pillar identifies five main concerns with respect to the security dimension. This research study suggests eight policy options to mitigate and address them. Table 4 summaries the analysed security concerns and related suggested policy options.

Table 4 – Policy options for security risks and challenges

Security risk/challenge	Policy option identifier	Policy option title
Network softwareisation and flexibility	POS1	Consider standards for network components
	POS2	Consider compulsoriness of security controls
Multiconnectivity and device density	POS3	Monitor the evolution of multiconnectivity
Protocols and interoperability	POS4	Facilitate collaborations to contribute to new protocols
	POS5	Foster the resolution of interoperability issues in new protocols and regulations
Identifiers and encryption	POS6	Adopt full anonymisation of the end-to-end subscriber identity
	POS7	Converge to new and standard cipher algorithms
New stakeholders and frameworks	POS8	Define clear roles of stakeholders

[3] EUROSTAT reported that the percentage of households with access to broadband internet was 88% in aggregate across the European in 2019, with a high of 98% in the Netherlands and a low of 75% in Bulgaria. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

3.4. Cybersecurity, robotics and AI: relationship with 5G technology

A relevant increase in the overall complexity of 5G results from the virtualisation layer and the transformation of networks into programmable, software-driven, service-based and managed architectures [6]. Moreover, 5G provides unprecedented operational agility to support new business opportunities enabled by technological breakthroughs (including inter alia Network Slicing, that is the provisioning of network functions to applications/users according to specified or run-time needs).

Complexity, agility and transformation require novel and sophisticated paradigms for network and service management and for coping with ever-evolving cyberattacks.

ETSI has defined the Zero-touch network and Service Management (ZSM) [6] as the standard architecture framework for tackling 5G network management and security. The ZSM framework is envisaged as a next-generation management system that aims to have all operational processes and tasks (e.g., planning and design, delivery, deployment, provisioning, monitoring, and optimisation) executed automatically, ideally without human intervention (hence called 'zero-touch').

Artificial intelligence (AI), supported by machine learning (ML) and Big Data analytics, is a key enabler to empower the ZSM framework and autonomous networks [53], and provides potential benefits for security improvement, enabling more effective and efficient security solutions in the cognitive network management, and predictive or proactive security functions in the anticipatory networking context, even in the case of 5G encrypted communication [7] [54].

Reminiscent of the computer HAL 9000 in '2001: A Space Odyssey', an AI governing a complex and fundamental infrastructure poses ethics and security concerns. However, any implementation of technology may have relevant positive impacts for the society, if properly designed, implemented and used.

Robotics will derive benefits from the wider adoption and deployment of 5G and AI. Many sectors are expected to massively adopt robotics in order to, just to mention some examples: (i) extend their productive capacity (e.g. manufacturing and its scenarios of 'factory of the future'); (ii) reduce the harmfulness of work activities and improve the safety of work environments (e.g. collaborative robots that are usually called as 'cobots'); (iii) replace human operators in dangerous tasks (e.g. healthcare of infected patients).

However, even if there are many good proposals for using AI, 5G and robotics (e.g. robots to collect COVID19 throat swabs, reducing cross-infection and risks for sanitary operators [55]), there are always case studies that highlight ethics and legal concerns, such as autonomous robots performing surveillance [56] in urban areas to identify potential 'bad behaviours', as in the Robocop science-fiction films.

These examples can impact the public's opinion on disruptive technologies, distort the perception of benefits, risks, and capacities, and create sentiments of distrust, consequently raising barriers against the adoption and wider deployment of the technologies.

For this reason, the impact analysis has been enriched by a second branch with the involvement of stakeholders such as citizens – to analyse their interests, as well as experts -to gather their feedback with respect to 5G and its implications.

4. Impact assessment based on stakeholders' involvement

To complement the document-based assessment described in section 3, two kinds of analyses were carried out): a quantitative analysis and a qualitative analysis, which respectively aimed to detect the evolution of interest of a large basis of stakeholders and to collect information and judgement from experts on topics derived from the document-based and the quantitative analyses. This impact assessment pillar was centred on involving stakeholders across all four categories defined in the research conceptual map (Figure 3) by following the 7-step procedure detailed below:

- Step 1 - The macro research topics for the quantitative analysis were identified.
- Step 2 - The quantitative Sentiment Analysis (SA) was performed on Google Trend data that spanned a five-year period (2016 – 2021) in order to measure the interest for the 5G technology.
- Step 3 - Macro research topics were refined in view of a second round of quantitative analysis.
- Step 4 - The second round of the quantitative analysis was performed.
- Step 5 - Results of the quantitative analysis were used to derive policy options.
- Step 6 – A pool of experts in the domain of 5G technology, privacy, security and disruptive technologies was identified and engaged.
- Step 7 – Based on their expertise, experts provided feedback on the document-based assessment and SA results. Their contributions were collected and analysed in line with best practices from the theory of stakeholders' engagement of project management [9], and specifically the technique of **Expert Judgement**, through interviews, roundtables and questionnaires. Policy options were derived from the qualitative analysis.

4.1. Step 1 & 3: Identification of research topics

As shown in the overall conceptual map of this research study (Figure 3), the research team identified a set of hot topics relevant for the SA. A preliminary set of topics were extracted and used in a preliminary SA. Whilst such an analysis was fruitfully employed for the final selection of the topics, it did not allow for the collection of a sufficient amount of data from web crawling. As a result, a wider net was cast to analyse the evolving interest in 5G technology across eight different categories, i.e.: (i) all categories; (ii) computer security; (iii) network security; (iv) privacy issues; (v) machine learning and artificial intelligence; (vi) robotics; (vii) intelligence & counterterrorism; viii) discrimination & identity relations. Web crawling was carried out in five European countries that provided a solid geographical coverage of Europe (i.e. Spain, Italy, Greece, Germany, the Netherlands) and the USA.

4.2. Step 2 & 4: Analysis of the interest in 5G technology

The quantitative analysis of the interest towards the 5G technology was carried out using SA, which uses techniques such as natural language processing, text analysis, and computational linguistics. SA can be deployed to take the pulse of a population of individuals by monitoring and analysing their online activity (without invading their privacy) and thus decide on the implementation of a wide range of strategies or policies. In the context of the present research study, SA was performed using Google Trends data, which is a good proxy for general interest. The results of the SA were later useful for engaging experts.

Despite being a relatively new technique, SA has been extensively discussed in literature and many evidences of its accuracy are available. For instance, in [57] SA has proved to provide valuable information in the 2012 U.S. election, whereas in [58] and [59] theoretical arguments are given to

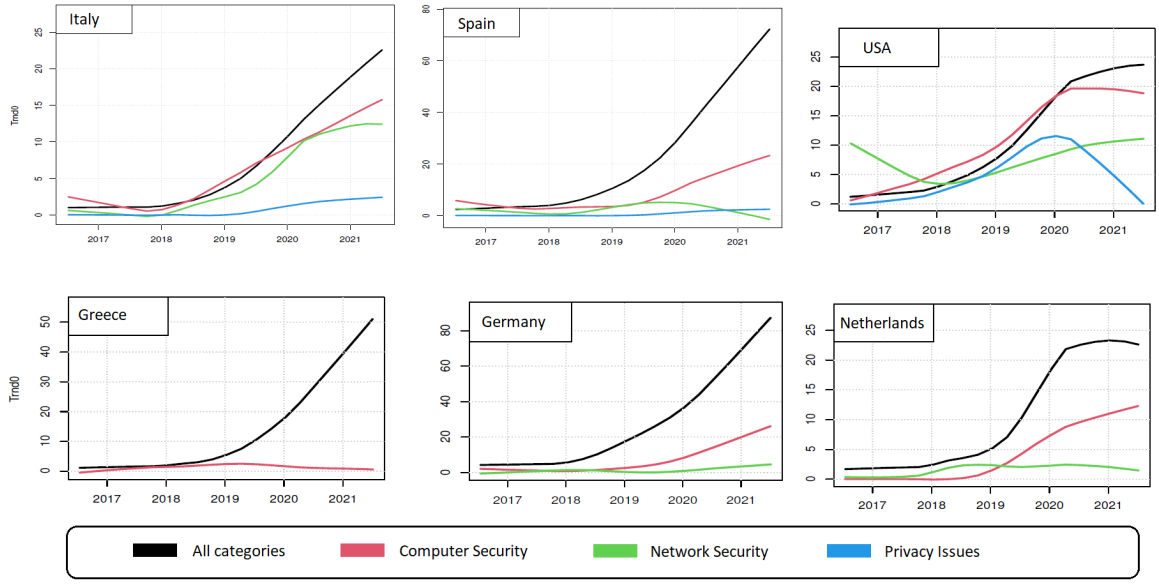
support its validity. Finally, the excellent book [60] presents a comprehensive study on the use of SA in the field of social media.

4.3. Step 5: Quantitative analysis and results

Results from the first SA campaign

The results from the first SA campaign are illustrated in Figure 6. They are based on weekly data provided by the search engine Google (Google Trends data) for the time window January 2016-July 2021. In essence, Google Trends data shows the evolution in time of the frequency of searches – a proxy for interest – for a term or a string of terms.

Figure 6 – Sentiment analysis - 1st set of results



Source: CyberEthics Lab.

For an improved readability, the time series have been smoothed using the algorithm STL (Seasonal Trend decomposition using Loess) [61] based on a regression model of the type local polynomial. All the plots have been generated keeping the STL window constant (four weeks). The results obtained reflect the evolution over time of the interests expressed by citizens towards different aspects of the 5G technology.

The analysis has raised the following concerns:

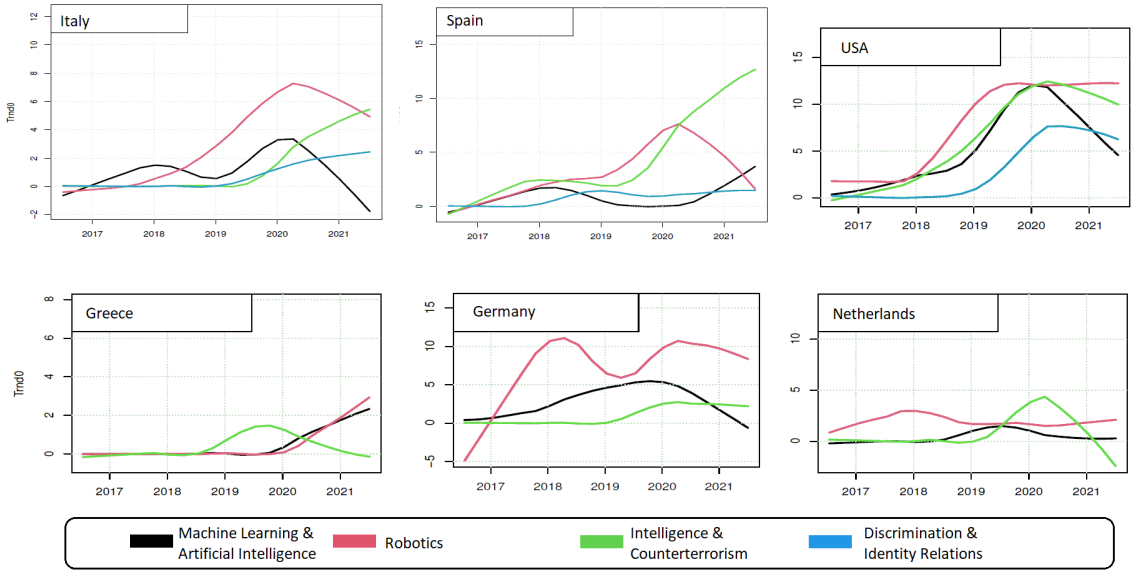
- **Stakeholders' interest on 5G technology based on all categories of research topics**: Generally speaking, it emerges that interest in 5G is growing among European and American citizens starting from 2018 (black line in all plots in Figure 6).
- **Security concerns**: According to the trend analysis, security concerns ('computer security' and 'network security') are growing together with the tendential emergence of 5G. Such a result might be deemed consistent with findings related to the analysis of security concerns (see section 3.3), where the importance of security as one of the five pillars of 5G technology has been highlighted. In a digitalised world, security and cybersecurity are of increasing importance and interest.
- **Privacy concerns**: On the other hand, privacy and personal data protection (blue line in Figure 6) appear as to be of less interest for European citizens, against any expectation due to the fact that Europe, since 2018, has been the cradle of the GDPR. Moreover, the

data from SA shows a lower relevance of privacy with respect to security, something that has not changed substantially over the observation period. The analysis highlights how in some European countries the interest in privacy related to 5G is practically negligible with respect to the others. This fact highlights that the path to guaranteeing the right to the protection of personal data, started with the entry into force of the GDPR, is still very long, and must pass through an increased awareness of citizens of how certain technologies may undermine their right.

Results from the second SA campaign

The results from the second SA campaign are illustrated in Figure 7.

Figure 7 – Sentiment analysis – 2nd set of results



Source: CyberEthics Lab.

The analysis has raised the following concerns (data time span and smoothing method the same as specified above):

- **5G vs cyber threats**: As can be seen from Figure 7, in some countries (i.e. Italy, Spain, USA) there is a great deal of interest on the 'Intelligence and Counterterrorism' topic (green line) when associated with the keyword '5G'.
- **5G technology vs ethics concerns**: Fears of 'discrimination and misrecognition' of social identities also seem to not be of primary interest for citizens in half the countries of our sample, while they are in Italy, Spain and the USA.
- **5G technology vs robotics and artificial intelligence**: There is also the last consideration on the categories of the SA with a greater technological vocation. Robotics and AI are generally presented as the themes that most condition the general emergence of 5G as a theme of interest.

Deriving policy options from the quantitative analysis

Analysing the SA data, the first immediate inference is that most of the interest regards technological and security aspects (e.g. cybercrime) rather than morally relevant issues (e.g., violation of privacy, effects of discrimination, etc.). This might depend on the current low-level of knowledge of the impacts of 5G on ethical aspects, which connotes and highlights the **lack of citizen awareness** on how their **personal data** are used by technologies. It therefore highlights the need to inform citizens more and to have a regulatory framework that ensures human rights and social equity (data justice) are guaranteed.

Policy options for ethics risks and challenges:

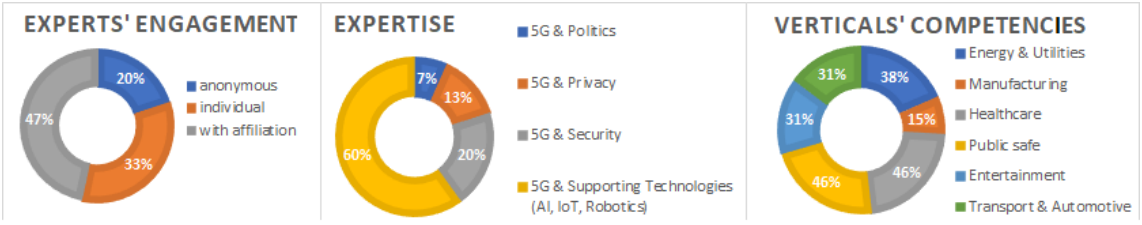
- ***POE1 'Provide democratic access to information about 5G'*** *- Democratic access should be granted to an adequate amount of information on 5G ethics impacts.*
- ***POE2 'Promote critical thinking about data practices in the 5G ecosystem'*** *- People's awareness and critical thinking should be nurtured in the context of digital and data literacy within lifelong education projects, as well as in schools.*
- ***POE3 'Produce an ethics regulatory framework for 5G'*** *- A tailored regulatory framework for applied 5G ethics (in the same way as there are other kinds of applied ethics, such as AI ethics, roboethics, etc.) should be produced at the EU level.*

4.4. Step 6: Engaging experts

A group of experts was engaged to provide feedback regarding results from the SA. The feedback gathered functioned as a validation of the policy options envisioned after the first five steps. The identification of experts has been done through a list of known candidates actively involved in 5G research projects and initiatives (e.g. 5G Industry Association [62], 5G Infrastructure Private Public Partnership [63]), as well as candidates with a relevant experience in security, privacy and ethics/politics. In practice, four groups of experts have been identified (see Figure 8) according to the four categories of the impact assessment, i.e. (i) 5G and privacy; (ii) 5G and security; (iii) 5G and related technologies (IoT, AI, robotics); and (iv) 5G and ethics/politics.

Based on the candidate list, a first, direct contact was held either via conference call, email exchange or phone call. These techniques were chosen because they involved direct interaction between the candidates and, therefore, allowed the interviewer to take advantage of all the potential of interpersonal communication, and to establish how to move forward with the next step of analysis. The number of identified candidates was greater than the selected experts effectively engaged in the next steps, ensuring expert anonymity (20% of the experts' group exercised this right through the consent form).

Figure 8 – Identification and engagement of experts



Source: CyberEthics Lab.

Experts were surveyed regarding public interest (as described through the SA), the four categories of the research conceptual map (see Figure 3) and any concerns regarding the 5G technology (both those derived from the desktop analysis in Section 3 and others they may have held as individuals). The interviews were composed by a set of three questionnaires, following the structure of the above three steps. The interviews lasted between 20 to 30 minutes.

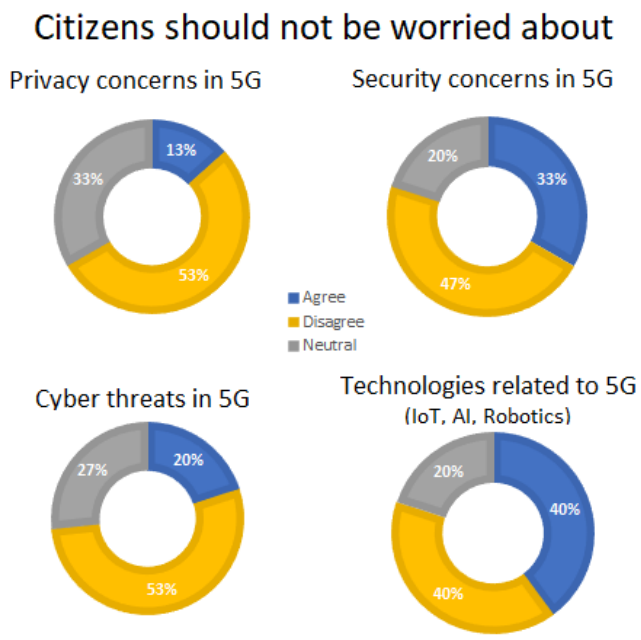
4.5. Step 7: Gather and analyse feedback from experts

Judgement on citizens' concerns

Based on the assumption that the lack of awareness in terms of benefits (as well as risks) of 5G technology often raises barriers to its acceptability [64], a set of four questions in the form of 'Citizens should not be worried about…' was submitted to the experts to gather their opinions on citizens' concerns. Experts' answers provided interesting feedback, confirming that **privacy** is still considered to be a more open issue than security. Indeed, Figure 9 shows that only 13% of the experts agree with the statement 'Citizens should not be worried about privacy concerns in 5G', while 53% disagree and 33% are neutral. Experts have justified their answers with many comments, confirming that the improvement in privacy protection mechanisms in 5G is essential, but that methods and approaches for countering increasingly sophisticated privacy-related attacks are urgently needed.

Moreover, experts concur that privacy concerns are impacted not only by the methods and mechanisms adopted to hinder attacks, but also by the complexity of the 5G ecosystem.

Figure 9 – Judgement on citizens' concerns



Source: CyberEthics Lab.

The multitude and the heterogeneity of actors that make up this ecosystem may entail, in a non-ideal scenario, that consensus-building processes regarding adequate protection mechanisms proceed more slowly than expected or that, in the worst-case scenario, 5G-based applications and services are implemented without adequate protection mechanisms. For this reason, the experts surveyed are eagerly awaiting the next release of 5G technology specifications (scheduled for July 2022) to see whether privacy is ensured across all levels holistically, including non-3GPP compliant technologies.

Policy options for privacy risks and challenges:

- ***POP11 'Monitor privacy aspects'*** *- The European legislator should monitor the evolution of the privacy issue in the next specification and deployment of 5G technology.*
- ***POP12 'Ensure data sovereignty'*** *– The 5G ecosystem requires the cooperation of various stakeholders located worldwide. Implications for data sovereignty should be considered in EU Member State regulations and strategic plans (93 % of experts agreed).*

A less certain position is coming from the experts on **security** aspects: 33% of experts agree on the statement 'Citizens should not be worried about security', while 20% are neutral and 47% disagree. This split confirms that the topic is widely treated and the wider scientific literature demonstrates how security is addressed in its multiple facets (e.g. encryption algorithms, identifiers' management, antennas, 5G frequencies).

However, with respect to **cyber threats** in 5G, experts are once again more divided: 27% are neutral and 20% agree with the statement 'citizens should not be worried about cyber threats in 5G'.

Policy options for security risks and challenges:

- ***POS9 'Accelerate the development of 5G cybersecurity standards'*** *- While existing cybersecurity guidelines are implemented by service and component providers in line with their internal procedures, 5G should adopt common standards for cybersecurity (87 % of experts agree).*

Conversely, 53% of those surveyed consider necessary to stay alert in this regard, even if 5G is improving protection mechanisms through predictive detection and maintenance. They argue that, as in the case of privacy, attacks might occur under unexpected, novel forms and that we should be prepared to confront an increasing and creative landscape of threats. To this extent, experts fully agree that security certification standards and processes for IoT devices, which will represent the majority of connected entities in 5G, will be important to effectively address security concerns. In fact, 87% of experts surveyed agree that the development of cybersecurity standards and certifications processes/procedures/approaches for 5G services/infrastructures/enabled technologies/devices, should be accelerated.

Finally, concerning the **technologies related to 5G (i.e. IoT, AI and robotics)**, 40% of experts agree that 'citizens should not be worried about advanced technologies (such as artificial intelligence, robotics, Internet of Things) related to 5G, because these will derive benefits in terms of improved

Policy options for ethics risks and challenges:

- ***POE4 'Adopt indicators to measure the multidimensional societal impacts of 5G'*** *- Improvements promised by 5G and related technologies should be evaluated with key societal indicators such as energy efficiency, wellbeing and life expectancy, environmental footprint, and reduced harmfulness to human beings (87 % of experts agree).*
- ***POE5 'Promote accountability, trustworthiness and reliability of actors in the 5G ecosystem'*** *- Accountability, trustworthiness and reliability of 5G and related technologies (e.g. AI, IoT, robotics etc.) should be considered in the regulatory framework for the implementation of 5G verticals (e.g. e-health, smart cities, energy, etc.) (87 % of experts agree).*
- ***POE6 'Improve communication of 5G benefits'*** *- Communication of benefits and risks associated to 5G and its related technologies should be improved at all levels of the 5G ecosystem (58 % of experts agree).*

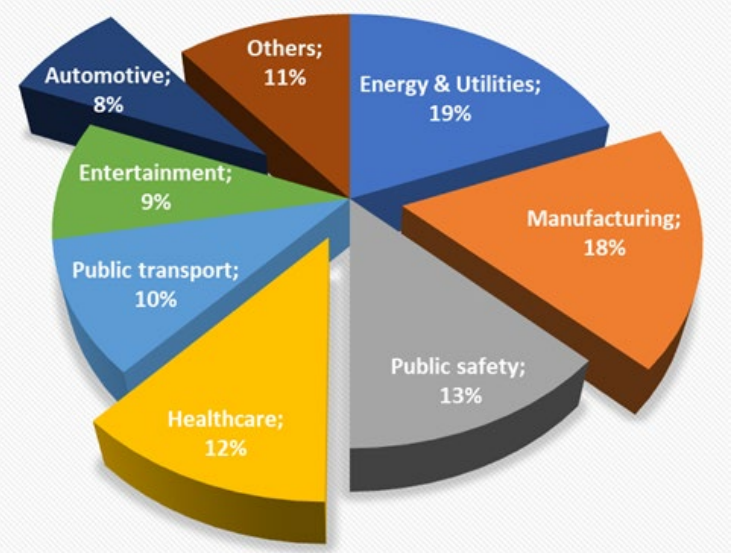
quality of life (e.g. pollution/waste reduction, reduced harms for workers, prevented incidents in transportation sector)'. Conversely, 20% are neutral and 40% disagree. The optimistic experts justify their answers with comments such as: 'Advanced technologies are designed to help citizens'. The only worry is the reduction of manpower. On the other hand, the sceptic experts argue that the current regulatory framework has gaps regarding how and to what extent these technologies will be used, and that citizens should be made more aware of both the benefits and the dangers of these advanced technologies.

Finally, experts have identified **Healthcare**, **Public safety**, **Transport and Automotive** as the sectors where **privacy** might have most relevant challenges, whereas **Energy & Utilities**, **Public safety**, **Transport and Automotive** have been considered as sectors that present unique challenges in terms of **security** aspects.

5. Case studies

As mentioned elsewhere in this paper, 5G technology will enable technological scenarios in which everything is connected. The mix of 5G with AI will allow to efficiently govern the heterogeneity and amount of data, enabling real-time support for decision making in everyday life. Last but not least, robotics is emerging as another fundamental building block in the support of human activities, especially in the case of dangerous or tiring ones. Moreover, 5G promises to be an alternative solution to positioning navigation and timing (PNT) and real-time location (RTL) services [65], essential utilities for many operations in different domains. To this extent, 5G will impact almost all business sectors (see Figure 10).

Figure 10 – 5G impacted sectors, estimation for 2026



Source: Data available from *[90]*

Both results from the document-based analysis and from the engagement of experts highlight how the Healthcare, Public safety, and Transport and Automotive sectors are those that present the greatest amount of privacy and security concerns. This section details three case studies, one for each of the aforementioned sectors, which exemplify those concerns by presenting a more concrete, detailed and contextualised picture of them and serve to further justify the proposed policy options.

The high specificity of the case studies was intended to provide a **looking glass into the near future**, with the dual aim of increasing awareness of the benefits and risks of 5G (something that the previous analyses underscored as being underdeveloped) and strengthening the link between 5G as a new technology and the state of the art.

5.1. Vehicle-to-everything to reduce road-traffic-injuries

According to the 2021 United Nations report on 'Road traffic injuries' [66], 'every year the lives of approximately **1,3 million people** are cut short as a result of a road traffic crash. Between 20 and 50 million more people suffer non-fatal injuries, with many incurring a disability as a result of their injury'. Even if Europe has been bucking the trend in recent years, more than 23.000 EU citizens died in road accidents in 2018, equal to more than 63 per day.

Figure 11 – V2X case study

Source: Hans-J Brehm CC-BY-SA 4.0 *[110]*

5G technology applied to the Intelligent Transport Systems (ITS) might be a potential solution to this problem and an opportunity to demonstrate a concrete and sustainable value for responsible innovation.

ITS are systems in which information and communication technologies are applied in the field of road transport, including infrastructures, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport. In other words, ITS integrate telecommunications, electronics and information technologies with transport engineering in order to plan, design, operate, maintain and manage transport systems [67].

5G technology offers ITS a new way to become fully integrated with everything by providing massive simultaneous connections and network ubiquity, even under high mobility situations or in densely populated areas. In this way, 5G will become a key enabler for 'Vehicle to everything' (V2X) [68], i.e. the interconnection between a vehicle and any entity that may affect it or may be affected by it. This use case, supported by 5G and its related technologies, might lead to the proactive identification of potential accidents and preventative actions to avoid them.

Connected devices on board the vehicle and in the surrounding environment would need to be massively deployed (see risks in section 3.1.4 and the relative policy options) for the success of this use case. These devices will gather and exchange a continuous amount of data, including inter-alia location data. According to the Court of Justice of the European Union (CJEU) [69] location data are metadata derived from electronic communications which may reveal very sensitive and personal information and allow precise conclusions to be drawn regarding the private lives of persons (see concerns in section 3.1.3). Recital 17 of the first draft of the ePrivacy Regulation recognises that location data are often used to display traffic movements, and public authorities and public operators benefit from these metadata to develop new infrastructure. Typically, the processing of this kind of data should require the data subjects' consent. However, the last draft version of the ePrivacy Regulation seems to allow the use of the metadata through the same presumption of the compatibility process stated by the article 6, paragraph 4 of the GDPR. In any case, the use of such data without the consent of the interested parties might cause a high risk to the rights and freedom of natural persons. In these cases, a data protection impact assessment and a consultation with the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of the GDPR.

Moreover, it is important that security is ensured during data exchange, because an attack or fault might represent an additional risk for human beings involved.

For this reason, as stated in [70], messages exchanged by the protocols used in V2X case studies should not contain any identifying information and should not reveal users' identity. Rather, they need only to contain user permissions. Moreover, for the security concerns, the V2X case study implements suitable protection mechanisms against attacks, that are (i) sandboxing, which limits the types of data accepted by the system, and (ii) authentication, which refers to the application identifier, rather than to the user identifier.

The V2X case study could deliver potential societal benefits in terms of reduction of traffic congestion, greenhouse gas emissions and enhanced flexibility of public transportation. To this extent, this use case might be an opportunity to redeem the perception of fear and distrust towards 5G technology, provided that identified indicators will be used to demonstrate the efficacy of the solution, and that protocols and protection mechanisms will respect ethics, regulatory and legal frameworks.

A further step in the ITS field should be achieved by adopting common rules within the Union. Currently, the framework for the deployment of ITS for road transport is the Directive 2010/40/EU that identifies four priority areas of intervention (Article 2):

- Optimal use of the road, traffic and travel data;
- Continuity of traffic and freight management ITS services;
- ITS road safety and security applications;
- Linking the vehicle with the transport infrastructure.

In 2016, the European Commission with the 'European Strategy on Cooperative Intelligent Transport Systems (C-ITS, Cooperative Intelligent Transport Systems) – a milestone towards cooperative, connected and automated mobility', highlighted the risk of fragmentation and unevenness of the internal market in the C-ITS sector. The communication of the European Commission stated that '*with technology rapidly evolving and the public and private sector investing substantial amounts into developing and testing C-ITS technologies, there is a risk that, without a framework at European level, EU-wide interoperability will not be achieved on time.*' [71] Furthermore, the European Commission pointed out that fragmented security solutions jeopardise interoperability (see concerns in section 3.3.4 and relative policy options) and the safety of end-users. In this way, The European Commission adopted a delegated regulation pursuant to Article 290 of the Treaty on the Functioning of the European Union (TFUE). The delegated regulation of 13/3/2019 supplements Directive 2010/40/EU and establishes the minimum legal requirements for C-ITS interoperability and to enable large-scale deployment of C-ITS services and systems [72].

This interoperability concern is fundamental for the interconnection of multiple devices from different domains, especially in light of the fact that certain aspects of the C-ITS, V2X and Cooperative Connected and Automated Mobility (CCAM) chain are not regulated at all. One such aspect is the message formatting for autonomous vehicles [73]. Another, the trans-border reselection of network, i.e. the reselection of a network operator when crossing national borders: this operation still takes a long time, in the order of several minutes. Therefore these issues, if not properly managed, might be critical for the V2X case, since they impact security and privacy (see concerns in section 3.1.1) and safety, too. A regulation for automotive cybersecurity is under definition by United Nations Economic Commission for Europe (UN-ECE) [74] and will be applied in the framework of EU Regulation 2019/2144 [75], General Safety Regulation, starting from July 2022 for all new vehicle models. However, these regulations do not flag interoperability as a main security and privacy concern.

5.2. Factory-of-future to reduce job-related-injuries

According to the report on 'Occupational safety and health' of the International Labour Organisation published in 2003 [76], '**2.3 million women and men** around the world succumb to work-related accidents or diseases every year; this corresponds to over 6.000 deaths every single day'. Unfortunately, almost 20 years later, the data continues to be alarming: in 2018, there were more than 3.000 fatal accidents at work in Europe, an increase of 60 deaths compared to the year before. Most of these accidents concerned: wounds and superficial injuries; dislocations, sprains and strains; or concussion and internal injuries [77].

Figure 12 – FoF case study

Source: Daimler und Benz Stiftung, CC BY-SA 3.0 de, [111]

Manufacturing is expected to be the second-most-impacted sector by 5G technology. For this reason, the term 'Factory-of-Future' (FoF) has been coined to define the disruption that 5G-enabled IoT, AI and robotics will bring about in this sector.

Exoskeletons, wearable robots, collaborative robots (cobots) are becoming more and more relevant topics in research and innovation. Exoskeletons have been initially studied in the rehabilitation of patients, and for this reason they are perceived as a fair and socially acceptable technology. However, a new trend is recently appearing for the exploitation of this technology, enhanced by the 5G technology, to support humans in their productive activities. Indeed, when dealing with production processes, the capacity to responsively react in very short times (tenths of a milliseconds) is important.

This case study might have many opportunities to deliver societal benefits in terms of reduced incidents of work-related injuries and of achieving 'decent work and economic growth', that is the eighth sustainable development promoted by the United Nations and European Commission [78].

To this extent, it is fundamental that these technologies respect human beings, and that they will be not used as tools for simply augmenting the power of human workers and improving production efficiency. As for the V2X case study, suggested human-oriented indicators that document the increase in wellbeing should be adopted for demonstrating the positivity of the innovation for individuals and society as a whole.

Together with this ethics perspective, reliability and resilience of production processes should considered as main constraints for introducing the 5G technology in this context. Cyberattacks can discontinue business operations, as illustrated by the many occurrences of industrial espionage against pharmaceutical companies during the early stages of the COVID-19 pandemic [79]. Moreover, in an era in which industries are exploiting data lakes replenished by consumer-generated data to plan productions, unauthorised FoF data lake accesses could have serious consequences for individuals' privacy if not properly managed, as mentioned in section 3 and its related policy options. In essence, the improved flexibility of a 5G-powered pipeline cannot compromise and accept optional security controls, as specified in section 3.3.2 and policy options contained therein.

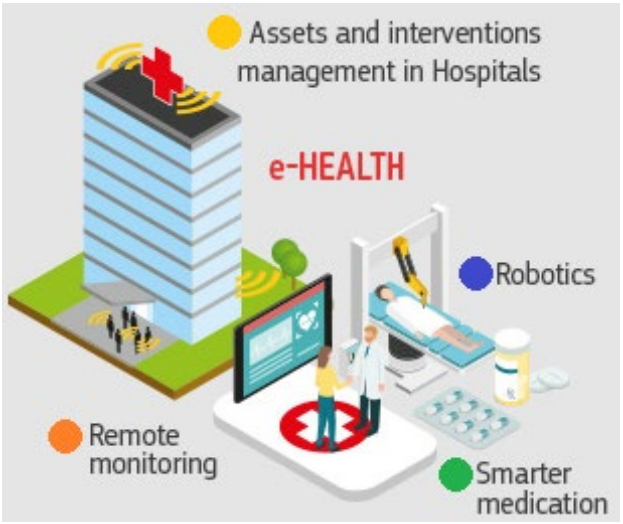
5.3. eHealth to prevent diseases and ensure healthy lives

The COVID-19 pandemic has exacerbated the conditions of worldwide health services, demonstrating their vulnerabilities and lack of resources and capabilities to mitigate sudden outbreaks of diseases. Vulnerable groups have been disproportionally the most impacted (around 90% [80]) among European citizens. This impact has been measured in terms of lives lost, with profound implications for the health of our people, economic progress, trust in government, and social cohesion. Moreover, due to pressing requests for emergency care, hospitals and healthcare services have postponed routine assistance of patients with chronic diseases. This tragedy has highlighted the need to innovate healthcare by introducing digitalised, distributed 'neighbourhood healthcare centres' capable of offering wider access to care to inhabitants.

Every year, more than **2 million European citizens** are diagnosed with cancer and 50% of them die from it. Over 40% of cancer cases are preventable, and mortality can also be reduced through earlier diagnoses [80]. Therefore, the prevention of non-communicable diseases such as cancer is a priority for promoting well-being, as defined in Sustainable Development Goal 3 of the 2030 Agenda for Sustainable Development of the United Nations [81]. This digital transformation aims to deliver better healthcare, ranging from health monitoring for prevention and early detection, to diagnosis and remote assistance and surgery, for citizens of all ages.

To this extent, eHealth will be characterised by (see Figure 13): (i) preventive healthcare based on diffused remote monitoring through connected devices (IoT) and predictive disease detection through computing capabilities (AI); (ii) prevention actions, continuous contact with healthcare providers and smarter medication; (iii) remote and in-hospital assistance and surgery with dedicated robotics; (iv) asset- and intervention-management in hospitals and healthcare centres.

Figure 13 – eHealth services powered by 5G



Source: CyberEthics Lab. adapted from *[113]*

For instance, robotics and drones might be used to more promptly deliver medical equipment, therapies, and organs [82] over long distances, potentially saving more lives. Such technologies require a reliable and seamless connection, the capacity to support network access for a wider range of sensors and broadband able to transfer high-definition data in real-time, and currently 5G is the only technology on the market that can meet these requirements.

When dealing with healthcare of citizens, systems manage and process special categories of personal data. Therefore privacy and security are non-negotiable dimensions and constraints for any technology in this field. For this reason, it is important to take care of concerns identified in sections 3 and 4.

In 2020 and 2021, many healthcare institutions have experienced ransomware attacks. As a consequence, they have either not been able to ensure availability of services to their patients or have reported the personal data of patients as stolen [83]. The long-term impacts of these consequences are non-trivial, and make it important for 5G to establish all the opportune solutions

in order to address them. Remote monitoring of patients will extend the attack surface of the healthcare ICT systems and therefore it will have to adopt strong cipher algorithms in each wearable and medical device as mentioned in section 3.3.5 and its related policy options. Furthermore, healthcare services have been recognised as a critical sector, and their protection from cyberattacks will also be considered under the ongoing review of the NIS Directive [84].

Last but not least, the results from European success stories [85] should be considered such as the adoption of a personal data wallet, so that patients might have the tools to fully exercise their fundamental rights on personal data (see section 3.1.1 and its relative policy options). If policy makers at all level address these concerns, they will certainly improve the degree of social acceptability of the involved 5G technologies.

6. Final policy options

Based on the analysis carried out in this research study, where potential privacy and security risks, challenges, opportunities and suggested policy options have been identified and described, this section provides policy options.

6.1. Feasibility of 5G technology adoption vs privacy and security risks

On one side, privacy and security risks are a threat to the feasibility of the future development of 5G technology; on the other, the awareness around these risks is of paramount importance. In fact, both those factors might lead to vulnerabilities that may leave personal data or sensitive information at risk. The sentiment analysis and roundtables carried out during this research have indeed highlighted how guaranteeing citizens' right to privacy is an ongoing process, since their awareness must be improved. The 5G ecosystem could capitalise on this weakness as an opportunity to promote the benefits at all levels of the 5G technology.

Many research exercises [86] have demonstrated the need to promote **a new mindset**, where ethics, social, legal and regulatory competencies are merged into the system development lifecycle from its **conception** (promoting a new approach this paper refers to as '**ethics-by-conception**'). This would allow risks to be handled effectively and, as far as 5G is concerned, facilitate its adoption. This new paradigm should also include the active participation of 5G technology users, especially concerning the implementation of 5G use cases and scenarios.

Best practices coming from the entanglement of communication and computing systems, such as **DevSecOps** [87], which stands for development, security and operations, might be adopted to combine different integrated approaches.. This best practice, derived from the Agile methodology, creates cultural transformation in the value chain stakeholders, by innovating the way operations, developers and testers collaborate during the development and delivery processes.

The DevSecOps paradigm might be extended into **EthDevSecOps**, where Eth stands for ethics, by incorporating multidisciplinary skills to address any concern about human beings and the respect of their fundamental rights (e.g. privacy, freedom, participation, non-discrimination, inclusion, democracy).

6.2. Effectiveness of 5G technology through standardisation

6.2.1. Promote privacy and security standards

To enhance the framework for 5G cybersecurity and secure 5G deployment in the European Union, closer collaboration among Member States should be encouraged. During the preparation of this report, The European Union Agency for Cybersecurity (ENISA) established a call for a 5G Cybersecurity Certification Working Group, with the aim of developing an EU-wide cybersecurity certification scheme for 5G networks. To facilitate the implementation of the same security measures to mitigate privacy and security risks, at the same pace, in all Member States, ENISA will have to stress and monitor the adoption of those shared standards..

Moreover, it is fundamental to consider the interconnectivity and interoperability of 5G-powered systems. Indeed, the increase in communication capabilities, and the consequent data sharing, will certainly have a bigger impact. Privacy and security risks have been considered, but the interoperability dimension is related to these. Special care should therefore be paid to potential

mismatches among different interconnected devices and networks, especially with respect to interoperability across national borders. To this extent, interoperability should be ensured not only at lower layers of the OSI model, but also at the application and presentation layers, thanks to dedicated standards.

6.2.2. Promote ethics standards

The acceleration of data communication provided by 5G networks should be compliant with high standards, not only in the legal and security fields, but also in ethics. One of the great ethical and political issues of data-driven technologies is to avoid the possibility that errors and defects in human action can be transferred, intentionally or otherwise, to technological systems, thus replicating, for example, discriminatory phenomena such as race, gender or religion. It is necessary to act at several levels, by:

- Designing and implementing technologies through inherently sensitive value-based approaches such as 'ethics by-design'.
- Improving the governance and the organisational structure of ICT companies through appropriate ethics-monitoring procedures.
- Encouraging the political accountability of policy-makers, under the scrutiny of independent ethical experts, ethical auditors etc. appointed by an EU ethics compliance regulatory body.
- Stimulating public and private investment in school education and professional training to create the knowledge base for ethical problem-solving in the curricula of developers, programmers and other network actors.

6.3. Sustainability of 5G technology driven by trustworthiness

The idea of sustainability is linked to the capacity of (i) ensuring trustworthiness from the legal standpoint, (ii) promoting a high degree of trust in future 5G applications in society, and (iii) creating a trustworthy environment for future 5G technology enhancement.

6.3.1. Enhance the legal and regulatory framework

Enhancing legal and regulatory frameworks to monitor and control the roles and market positions of all the stakeholders involved in the 5G ecosystem, as their fluid participation in the revenue stream might cause conflict and uncertainty, impacting almost all of the sectors (e.g. energy and utilities, manufacturing, safety, public transportation, healthcare, automotive, entertainment). Moreover, the involvement of multiple providers in the supply chain might create vulnerabilities due to accountability issues and greater exposure to errors. Harmonisation policies should be promoted and regulated by defining specific and clear roles and responsibilities for each 5G ecosystem stakeholder. The application of all envisaged safeguards, such as 'adequacy decisions' and standard contractual clauses for example, should be carefully monitored by the authorities, to ensure accountability and trustworthiness, especially in the case of suppliers from hostile countries outside the EU.

6.3.2. Ensure trust and control for future generations of 5G

In imagining a future in which 5G technology is universally accepted, regulators must establish the degrees of trust with which to delegate the exclusivity of certain decisions to the network, and, conversely, the level of human control to be maintained in order to verify that those decisions and their consequences are in line with what had been planned. To this end, regulatory arrangements must be strengthened or created, for the purpose of:

- Clarifying the conditions, risks and preventative measures under which we can opt for a greater replacement of human activity without gradually removing human responsibility in favour of the network and its governance.
- Harmonising measures and regulations at the international and EU level, which can currently differ greatly case by case.
- Promoting approaches to computer engineering and data science in school education and professional training which, while teaching how to delegate some decisions to technologies, do not make certain tasks obsolete and, above all, do not reduce the importance of human skills.
- Encouraging obligations to respect an 'explainability' principle for technologies (especially if AI-based). Wherever technologies involve important moral decisions, these solutions should be provided with clear and accurate descriptions of how (a) they are backed by evidence, and (b) they are accountable and operate within the limits for which they were designed.

6.3.3. Support trustworthy investment by creating an EU public culture of technology

As the European Commission has already stated, for the trustworthy development of AI [88], the increasing demand for connecting 'things' and physical infrastructures powered by 5G opens a high market potential for real-time, power-efficient and privacy-preserving solutions, where Europe can seize the opportunity as an early adopter and position itself as the global leader, particularly in serving B2B and B2C markets. To ensure this market leadership, a set of policies to be adopted might:

- encourage, at an institutional level, mechanisms of social innovation and co-participation in public decisions in terms of 5G adoption with the aim not only of listening to individual actors (citizens, companies etc.), but also of promoting the emergence of a stronger European Union public sphere;
- foster a favourable policy and an investment environment for 5G roll-out, as well as large investment volumes in software toolchains for edge hardware design, computing infrastructure and distributed, beyond-machine-learning AI;
- promote a longer-term and participatory infrastructure perspective to extend the capabilities of existing infrastructure;
- transform large industries to digital hubs, securing cutting-edge research and competencies at a global scale.

7. Conclusions

We are facing another challenging passage in the history of technological innovation, in which human values and technical knowledge seem to be progressively intertwined, raising questions of opportunity and risk, not only for humans, but also for the entire 5G ecosystem.

The impact assessment carried out in this paper has identified six privacy and six security concerns related to 5G technology. In addition, two ethics concerns have also been identified. For each concern, the paper has suggested the policy options shown in Table 5.

Table 5 – Concerns and policy options

Privacy Concerns	**Policy Options**	
Transboundary data flow and 5G	POP1	5G ecosystem parties establish controller/processor in the EEA
	POP2	Adopt hybrid data location store
	POP3	Adopt personal data wallet
High-speed data rate	POP4	Revise data breach notification deadline
	POP5	Establish continuous consent
	POP6	Adopt state-of-the-art protection mechanisms
High traffic density and location accuracy	POP7	Consider 5G impacts in final version of proposed e-privacy regulation
Huge number of connected devices (IoT)	POP8	Consider a standard validation framework
	POP9	Consider the impact of more attractive devices and services
Internet protocol (IP)	POP10	Observe evolution of non-IP networking
Privacy as open issue	POP11	Monitor privacy aspects
	POP12	Ensure data sovereignty
Security Concerns	**Security Options**	
Network 'softwareisation' and flexibility	**POS1**	**Consider standards for network components**
	POS2	**Consider compulsoriness of security controls**
Multiconnectivity and device density	POS3	Monitor the evolution of multiconnectivity
Protocols and interoperability	POS4	Facilitate collaborations to contribute to new protocols
	POS5	Foster the resolution of interoperability issues in new protocols and regulations
Identifiers and encryption	POS6	Adopt full anonymisation of the end-to-end subscriber identity
	POS7	Converge to new and standard cipher algorithms
New stakeholders and frameworks	POS8	Define clear roles of stakeholders
Cybersecurity standards	POS9	Accelerate cybersecurity standards
Ethics concerns	**Policy Options**	
Lack of citizen awareness on the impacts of 5G on ethical aspects	POE1	Provide democratic access to information about 5G
	POE2	Promote critical thinking about data practices in the 5G ecosystem
	POE3	Produce a regulatory framework for 5G
Technology and use of personal data	POE4	Adopt indicators to measure the multidimensional societal impacts of 5G
	POE5	Promote accountability, trustworthiness and reliability of actors in the 5G ecosystem
	POE6	Improve communication of 5G benefits

No technology is bad in itself, but there is also no technological innovation that is free of contraindications. This is also the case for 5G's impacts on privacy and security. Technology is not a means to an end, but rather enables knowledge and, therefore, dependent on the robustness of security, as well as on the awareness and responsibility of the society in which it operates.

Better digital connections and communications are functional for human development, especially in the pandemic context. The spread of use of the internet, connected devices and broadband connections all over the world have mitigated the forced isolation. The social distancing has moved us to fall in love again with our social nature as human beings and, more importantly, as citizens made free by rights and modern legal protections.

Against this backdrop, the right to information, one of the fundamental rights of individuals, should be interpreted with a broader meaning as the right to be connected, in such a way as to avoid damage to our personal spheres.

However, laws and legal norms, while very important in introducing new visions of moral obligations, are not enough. We need 'by-design' approaches that are embedded into the practices of **responsible research and innovation** (RRI). The conformity of technological goods or services with health and security protection standards is not a new fact.

The European Commission designed CE markings during the 1980s, to allow manufacturers to comply with mandatory regulations on safety, health and the environment. This has undoubtedly contributed to improving citizens' perception of trust in CE-marked products and to raising their awareness of products that can harm individuals. The time has come to implement standardisation processes that no longer (or not only) ensure final products' conformity with abstract ethics principles and requirements, but rather ethics-by-design principles that also 'internalise' the value-sensitive backgrounds, both of legal codes and people's claims, during the design and development phases of the technology.

In this paper, we have called this approach '**ethics-by-conception**', i.e. a novel form of compliance with ethics, privacy and security that could complement CE marking in relevant and as yet uncovered dimensions. This could contribute to creating a climate of greater public trust in disruptive technologies and govern technology use for the benefit of the individual and society as a whole.

This study was an opportunity to perform an in-depth analysis of aspects that are not usually the focus of research on 5G technology. Currently, most of the focus is on performance and feasibility studies for validating the real capacities of this technology. Due to this specific attention to techno-economic aspects, public opinion lacks awareness of the complexity of the 5G ecosystem and the real innovations it will promote. As already mentioned, the complexity of the 5G ecosystem is due to the convergence of two complex systems, i.e. communication and computing. This complexity is recognised in the research community that continues work on improving privacy and security risks, and is reflected in the ongoing specifications of this technology as described in section 2, such as the identification of new protocols overcoming the limits and weaknesses of obsolete ones (including internet protocol), the creation of new, flexible and configurable architectures for supporting specific scenarios, as well as the analysis of stronger and more efficient algorithms for extending encryption implementation in the everything-connected network.

This study highlights that 5G, as confirmed by the experts' judgement in section 4, is not just the arrival point of a long march that started in the 1980s with the first mobile generation, but a new platform for rethinking innovation thanks to new, digital-era concepts. Indeed, 5G will connect 'everything' by using new approaches and other disruptive technologies (such as AI, robotics and

IoT). This combination will result in an exponential growth of the threat surface, posing new risks, challenges and also presenting opportunities for privacy and security.

The new trend that arises after the first experiences with 5G, is that the next generation will focus on creating purposeful, seamless and sustainable networks and services for specific tasks, rather than large sectors or domains (e.g. transportation, energy, automotive, healthcare, manufacturing). At the basis of this new trend is the emergence of real-time digital representations of everything belonging to the 'machine world' and the 'human world', and the need to connect them. However, it is important in the next decades not to forget that representations are conceptual models aiming at describing real facts and entities, and the definition of these models can hide dimensions and characteristics that might affect the accuracy and effectiveness of the description itself. When merging representations of these two worlds (i.e. machine and human) the risk of confusing one with the other might arise, as well as the risk of making the comprehension of their real status critical, i.e. what is machine and what is human.

With this in mind, this trend has to be considered with its new challenges and opportunities for the ethics-by-design principle, and for future impact assessments of new disruptive technologies.

Annex – Experts engaged

The authors acknowledge and would like to thank the following external experts for their contributions to this paper.

Expert	Affiliation / Expertise
Andrea Di Giglio	5G-SOLUTIONS, project coordinator
Teresa Numerico	Assistant Professor RomaTre University, Philosophy and Technology
Muhammad Shuaib Siddiqui	i2CAT Foundation, Cybersecurity Research Area Manager
Ioanna Mesogiti	5G-VICTORY, Exploitation Work-Package Leader – Senior R&D Engineer
Mauro Capo	Infrastructure Services for the Health and Public Services expert
Saverio Romeo	Centre for Innovation Management Research, Birkbeck, University of London
Giampaolo Fiorentino	NRG5, project coordinator
Sofia Tsekeridou	INTRASOFT International, Senior Research and Innovation Manager – Expert, Head of Security & Safety Lab
Ioannis Markopoulos	NOVA, Innovation Department Director
Antonello Corsi	SMART5GRID, technical director
Herwig Zeiner	JOANNEUM RESEARCH, Key Researcher Industrial Internet
Piercosma Bisconti Lucidi	Philosophy and technology researcher
Wafa Ben Jaballah	THALES, cybersecurity expert
Eduard Fosch	LEIDEN UNIVERSITY, Assistant Professor on Law, Robots and AI
Silvia Fichera	Research Assistant

Together with the experts mentioned above, a further group opted to contribute anonymously. Their contribution was no less important for that.

The experts' judgement has contributed to this paper with objective evaluations of relevant aspects, and added valuable suggestions based on their own experiences and competencies.

References

[1] S. Behm and et al., "Digital ecosystems for insurers: Opportunities through the Internet of Things," 2019. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things.

[2] International Telecommunication Union, "Measuring digital development Facts and figures," 2020. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf.

[3] Eurostat, "Digital economy and society statistics - households and individuals," 2020. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals.

[4] European Commission, "5G for Europe's Digital and Green Recovery," 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/5g-europes-digital-and-green-recovery.

[5] 5G IA Vision and Societal Challenges Working Group, "5G ecosystems," 2021. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2021/09/White_paper_5G-Ecosystems_1-0-final.pdf.

[6] ETSI, "Network Transformation - ETSI White Paper No. 32," 2019. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_White_Paper_Network_Transformation_2019_N32.pdf.

[7] N. Garcia and et al., "Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence," 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520303362.

[8] European Parliament and Council of European Union, "REGULATION (EU) 2016/679 - General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[9] P. G. Standard, A Guide to the project management body of knowledge, 2016.

[10] European Parliament and European Council, "Directive (EU) 2016/680 of 27 April 2016," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/680/oj.

[11] European Parliament and European Council, "Regulation (EU) 2018/1725 of 23 October 2018," 2018. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

[12] European Commission, "Proposal for an ePrivacy Regulation," 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

[13] European Commission, "Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council," 2021. [Online]. Available: http://data.europa.eu/eli/dec_impl/2021/914/oj.

[14] M. Liyanage, J. Salo, A. Braeken, T. Kumar and S. Sen, "5G privacy: Scenarios and solutions," 2018. [Online]. Available: http://jultika.oulu.fi/files/nbnfi-fe2019081524261.pdf.

[15] T. Neumuth, C. Bulitta and S. Hamm, "5G Health - The need for 5G technologies in healthcare," 2020. [Online]. Available: https://www.researchgate.net/publication/3453.

[16] Publications Office EU, "Handbook on European Data Protection Law, 2018 Edition," 2018. [Online]. Available: https://www.key4biz.it/wp-content/uploads/2018/06/fra-coe-edps-2018-handbook-data-protection_en.pdf .

[17] S. Rizou, E. Alexandropoulou-Egyptiadou and K. E. Psannis, "GDPR interference with next generation 5G and IoT networks," 2020. [Online].

[18] M. Liyanage, I. Ahmad and A. Abro, "A Comprehensive Guide to 5G Security," 2018. [Online].

[19] S. Goudos, M. Deruyck, D. Plets, L. Martens, K. E. Psannis, P. Sarigiannidis and W. Joseph, "A novel design approach for 5G massive MIMO and NB-IoT green networks using a hybrid Jaya-differential evolution algorithm," 2019. [Online].

[20] S. Farhang, Y. Hayel and Q. Zhu, "PHY-layer location privacy preserving access point selection mechanism in next-generation wireless networks," 2015. [Online].

[21] European Commission, "EU Regulation concerning the respect for private life and the protection of personal data in electronic communications," 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010.

[22] R. Gupta and U. Rao, "An Exploration to Location Based Service and Its Privacy Preserving Techniques: A Survey," 2017. [Online].

[23] T. C. o. E. Union, "Mandate for negotiations with EP - Regulation concerning the respect for private life and the protection of personal data in electronic communications," 2021. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[24] GSMA, "The Mobile Economy 2021 Report," 2021. [Online]. Available: https://www.gsma.com/mobileeconomy/ ..

[25] B. Dorsemaine, J. Gaulier, J. Wary, N. Kheir and P. Urien, "Internet of Things: A Definition & Taxonomy," *9th International Conference on Next Generation Mobile Applications; Services and Technologies,* pp. 72-77, 2015.

[26] S. Delacroix and N. D. Lawrence, "Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance," *International Data Privacy Law,* vol. 9, no. Issue 4, November 2019.

[27] European Commission, "Eidas Supported Self-Sovereign Identity," 2019. [Online]. Available: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf.

[28] ICO - Information Commissioner's Office, "Introduction to the Age appropriate design code," 2021. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/.

[29] Court of Justice of the European Union (CJEU), "Judgment in Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland," 2016. [Online]. Available: https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.pdf.

[30] ETSI, "ETSI launches new group on non-IP networking addressing 5G new services," 2020. [Online]. Available: https://www.etsi.org/newsroom/press-releases/1749-2020-04-etsi-launches-new-group-on-non-ip-networking-addressing-5g-new-services.

[31] European Parliament, "Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[32] European Parliament and of the Council, "Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification," 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

[33] NIS Cooperation Group, "EU coordinated risk assessment of the cybersecurity of 5G networks," 2019. [Online]. Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

[34] European Commission, "EU-wide coordinated risk assessment of 5G networks security," 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[35] NIS Cooperation Group, "Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures," 2020. [Online]. Available: https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf.

[36] European Commission, "NIS Cooperation Group," 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

[37] 3gpp, "Release 17," 2020. [Online]. Available: https://www.3gpp.org/release-17.

[38] ENISA, "ENISA Threat Landscape for 5G Networks Report," 2020. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

[39] ENISA, "Security in 5G Specifications," 2021. [Online]. Available: https://www.enisa.europa.eu/publications/security-in-5g-specifications.

[40] ENISA, "5G SUPPLEMENT To the Guideline on Security Measures under the EECC," 2021. [Online]. Available: https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc.

[41] ENISA, "Ad-Hoc Working Group on 5G Cybersecurity Certification," 2021. [Online]. Available: https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification.

[42] Ericsson, "A guide to 5G network security insight report," 2021. [Online]. Available: https://www.ericsson.com/en/security/a-guide-to-5g-network-security.

[43] R. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9099823.

[44] D. Schinianakis and e. al., "Security Considerations in 5G Networks: A Slice-Aware Trust Zone Approach," 2019. [Online]. Available: https://zenodo.org/record/3268630/files/Security_STZ_paper.pdf.

[45] A. Sheikhi, S. M. Razavizadeh and I. Lee, "A Comparison of TDD and FDD Massive MIMO Systems Against Smart Jamming," *IEEE Access,* vol. 8, pp. 72068-72077, 2020.

[46] O. Open, "Introduction to STIX," [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.html.

[47] O. Open, "OASIS Open," 2021. [Online]. Available: https://www.oasis-open.org/.

[48] ISO, "ISO/IEC 27005:2018 "Information technology - Security techniques - Information security risk management"," 2018. [Online]. Available: https://www.iso.org/standard/75281.html.

[49] P. Teppo and K. Norrman, "Security in 5G RAN and Core deployments," 2020. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments.

[50] S. Sullivan and et. al., "5G Security Challenges and Solutions: A Review by OSI Layers," 2021. [Online]. Available: https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=1506&context=enece_facpub.

[51] United Nations Economic Commission for Europe, "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," 2020. [Online]. Available: https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[52] A. Caforio, F. Balli and S. Banik, "Melting SNOW-V: improved lightweight architectures," *Journal of Cryptographic Engineering,* 2020.

[53] INSPIRE-5Gplus, "D2.1 - 5G Security: Current Status and Future Trends," 2021. [Online]. Available: https://bscw.5g-ppp.eu/sec/bscw.cgi/d430315/i5-D2.1_5G%20Security%20Current%20Status%20and%20Future%20Trends_v1.6.pdf.

[54] B. Aryal, B., R. Abbas and I. B. Collings, "SDN Enabled DDoS Attack Detection and Mitigation for 5G Networks," 2021. [Online]. Available: http://www.jocm.us/uploadfile/2021/0618/20210618052054569.pdf.

[55] News18.com, "China is using robots to collect covid-19 throat swabs reducing cross-infection," 2021. [Online]. Available: https://www.news18.com/news/buzz/china-is-using-robots-to-collect-covid-19-throat-swabs-reducing-cross-infection-3286196.html.

[56] T. S. Times, "Autonomous robots check on bad behaviour in Singapore's heartland," 2021. [Online]. Available: https://www.straitstimes.com/singapore/autonomous-robots-checking-on-bad-behaviour-in-the-heartland.

[57] H. Wang and et al, "A System for Real-time Twitter Sentiment Analysis of 2012 US Presidential election Cycle," *Proceedings of the ACL 2012 system demonstrations,* 2012.

[58] T. Wilson and et al, "Recognizing Contextual Polarity in Phrase-level Sentiment Analysis," *Proceedings of human language technology conference and conference on empirical methods in natural language processing,* 2005.

[59] LI U, B. , Sentiment analysis: Mining Opinions, Sentiments, and Emotions., Cambridge University Press., 2005.

[60] F. Pozzi and et al., Sentiment analysis in social networks, Morgan Kaufmann, 2016.

[61] R. B. Cleveland, W. S. Cleveland, J. E. Mc Rae and I. Terpenning, "STL: A Seasonal-Trend Decomposition Procedure Based on Loess," 1990. [Online]. Available: https://www.wessa.net/download/stl.pdf.

[62] 5G-IA, "The voice of European Industry for the development and evolution of 5G," 2017. [Online]. Available: https://5g-ia.eu/.

[63] 5G-PPP, "The 5G Infrastructure Private Public Partnership," 2014. [Online]. Available: https://5g-ppp.eu/.

[64] L. Briguglio, P. Nesse, A. Di Giglio, I. Markopoulos, C. Occhipinti and P. Durkin, "Business Value and Social Acceptance for the Validation of 5G Technology," in *IEEE International Mediterranean Conference on Communications and Networking 2021 Proceedings*, Athens, 2021.

[65] ESA, "ESA leads drive into our 5G positioning future," 2019. [Online]. Available: https://www.esa.int/Applications/Navigation/ESA_leads_drive_into_our_5G_positioning_future.

[66] WHO, "Road traffic injuries," 2021. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries.

[67] European Parliament, "Directive 2010/40/EU of 7 July 2010 on The framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport," 2010. [Online]. Available: http://data.europa.eu/eli/dir/2010/40/oj.

[68] L. Guevara and F. Auat Cheein, "The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems.," 2020. [Online]. Available: https://doi.org/10.3390/su12166469.

[69] Court of Justice of the European Union (CJEU), "Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others," 2014. [Online]. Available: https://curia.europa.eu/juris/liste.jsf?num=C-293%252F12.

[70] 5G America, "Vehicular connectivity: C-2VX and 5G - Whitepaper September 2021," 2021. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2021/09/Vehicular-Connectivity-C-V2X-and-5G-InDesign-1.pdf.

[71] European Commission, "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0766&from=IT.

[72] European Parliament, "Commission delegated regulation of 13/3/2019," 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM:C(2019)1789&from=EN.

[73] 5G PPP, "5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors - Challenges and Opportunities," 2020. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf.

[74] "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," 2020. [Online]. Available: https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[75] "Regulation (EU) 2019/2144 of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles," 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/2144/oj.

[76] ILO, "The enormous burden of poor working conditions," 2003. [Online]. Available: https://www.ilo.org/moscow/areas-of-work/occupational-safety-and-health/WCMS_249278/lang--en/index.htm.

[77] Eurostat, "Accidents at work statistics," 2020. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_at_work_statistics.

[78] United Nations, "Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all," 2015. [Online]. Available: https://sdgs.un.org/goals/goal8.

[79] A. Nawrat, "Covid-19 pandemic: Russian hackers target UK, US and Canadian research," 2020. [Online]. Available: https://www.pharmaceutical-technology.com/features/covid19-ncsc-russian-cyber-attack/.

[80] OECD/European Union, "Health at a Glance: Europe 2020: State of Health in the EU Cycle," 2020. [Online]. Available: https://doi.org/10.1787/82129230-en.

[81] United Nations, "Health and population," 2015. [Online]. Available: https://sdgs.un.org/topics/health-and-population.

[82] PWC, "The global economic impact of 5G," 2021. [Online]. Available: https://www.pwc.com/gx/en/tmt/5g/global-economic-impact-5g.pdf.

[83] Interpol, "Cybercriminals targeting critical healthcare institutions with ransomware," 2020. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

[84] European Parliament, "The NIS2 Directive: A high common level of cybersecurity in the EU," 2021. [Online]. Available:

https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)689333.

[85] European Commission, "Putting data privacy back in the hands of EU citizens," 2021. [Online]. Available: https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/putting-data-privacy-back-hands-eu-citizens.

[86] A. Bianchini, E. Sartini and L. Briguglio, "Applying Privacy-by-Conception in Cybersecurity," 2021. [Online]. Available: https://ercim-news.ercim.eu/en126/special/applying-privacy-by-conception-in-cybersecurity.

[87] DevSecOps, "DevSecOps Manifesto," 2020. [Online]. Available: https://www.devsecops.org/.

[88] High-Level Expert Group on AI, "Ethics guidelines for trustworthy AI," 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[89] A. Ding and M. Janssen, "Opportunities for applications using 5G networks: requirements, challenges, and outlook," 2018. [Online]. Available: http://dx.doi.org/10.1145/3278161.3278166.

[90] Ericsson and Arthur D. Little, "The 5G Business Potential: Second Edition," 2017. [Online]. Available: https://cfile1.onoffmix.com/attach/M4wGkubyFE8B71oshv3YjZdRWeJrOaUc.

[91] European Parliament, "5G Deployment: State of play in Europe, USA and Asia," 2019. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf.

[92] European Parliament, "5G Knowledge Map," 2021. [Online]. Available: https://map.sciencemediahub.eu/5g.

[93] World Economic Forum, "The Impact of 5G: Creating New Value across Industries and Society," 2020. [Online]. Available: http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf.

[94] Nokia, "How 5G is bringing an energy efficiency revolution," 2020. [Online]. Available: https://onestore.nokia.com/asset/f/207360.

[95] J. Salo, "5G Privacy: Scenarios and Solutions," 2018. [Online]. Available: http://jultika.oulu.fi/files/nbnfi-fe2019081524261.pdf.

[96] V. Cunha, "Network slicing security: Challenges and directions," 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/pdf/10.1002/itl2.125.

[97] Wiley Law, "5G and Government: A Regulatory Roadmap," 2021. [Online]. Available: https://www.wiley.law/media/handbook/550_2021-Wiley-5G-Roadmap.pdf.

[98] European Commission, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

[99] European Court of Auditors, "Implementing secure 5G networks in the EU and its Member States," 2020. [Online]. Available: https://www.eca.europa.eu/Lists/ECADocuments/AP20_14/AP_5G_Security_EN.pdf.

[100] European cybersecurity centre of expertise, "Cybersecurity competence survey, EU 2018," 2018. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/98a912dd-b56d-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-77938379.

[101] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," *Conference: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC),* 2020.

[102] G. Box and G. JENKINS, "Time series models for forecasting and control," San Francisco, 1970.

[103] United Nations, "World Population Prospect 2019: Highlights," 2019. [Online]. Available: https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf.

[104] 3GPP, "About 3GPP," 2021. [Online]. Available: https://www.3gpp.org/about-3gpp/about-3gpp.

[105] M. Chen, S. Gonzales, Q. Zhang and M. Li, "A 2G-RFID-BASED E-HEALTHCARE SYSTEM," 2010. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.337.9126&rep=rep1&type=pdf.

[106] 3GPP, "The Evolved Packet Core," 2021. [Online]. Available: https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core.

[107] Eurostat, "Digital economy and society statistics - households and individuals," 2021. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access.

[108] ENISA, "Risky business or a leap of faith? A risk based approach to optimise cybersecurity certification," 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/risky-business-or-a-leap-of-faith-a-risk-based-approach-to-optimise-cybersecurity-certification..

[109] 5.-S. Consortium, "The 5G-SOLUTIONS Project," 2021. [Online]. Available: https://5gsolutionsproject.eu/.

[110] H.-J. Brehm, "Car2x_communication.jpg," 2020. [Online]. Available: https://en.wikipedia.org/wiki/Vehicle-to-everything#/media/File:Car2x_communication.jpg.

[111] D. Stiftung and B. Stiftung, "Db tuda jes2899 a.jpg," 2012. [Online]. Available: https://commons.wikimedia.org/w/index.php?curid=32261969.

[112] G. Riccio, A. Peduto, F. Iraci, L. Briguglio, E. Sartini, C. Occhipinti, I. Gutierrez and D. Natale, "The PoSeID-on Blockchain-based platform meets the "right to be forgotten"," *MediaLaw,* pp. 194-211, May 2020.

[113] 5Growth, "Europe advancing in 5G – new wave of projects launched to accelerate 5G take-up in vertical industries," 2019. [Online]. Available: https://5growth.eu/2019/04/26/europe-advancing-in-5g/.

This study describes two main dimensions of 5G technology, i.e. privacy and security. This research paper focuses on the analysis of cybersecurity risks and threats, privacy challenges and 5G technology opportunities at EU level and worldwide, as well as the relationship between cybersecurity risks and privacy issues. The methodological framework for this assessment of the impact of 5G technology is built on three pillars: (i) a document-based analysis; (ii) a parallel analysis with stakeholder involvement; and (iii) a selection of relevant case studies. The complexity of the 5G ecosystem, where new use cases are constantly emerging, also led the authors to assess the prospects of using new 5G-enabled technologies, such as the internet-of-things, robotics and AI. Moreover, policy options are defined and put forward for consideration by the European Parliament's Committees on Legal Affairs, Internal Market and Consumer Protection, Civil Liberties, Justice and Home Affairs, and the Subcommittee on Security and Defence, as well as by other EU institutions and the Member States.

OA-01-21-577-EN-N

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

ISBN 978-92-846-8830-2 | doi: 10.2861/255532 | QA-01-21-577-EN-N