CHAPTER 5

AI in 5G: High-Speed Dilution of the Right to Privacy and Reducing the Role of Consent

AI in 5G: High-Speed Dilution of the Right to Privacy

Mykyta Petik, KU Leuven, Centre for IT & IP Law, Leuven, Belgium

The telecommunications industry has gradually migrated from legacy telephony networks to telephony networks based on an Internet Protocol (IP) network to deliver communication services. (Zhang, 2018) It is projected that by 2025, 5th generation of mobile networks (5G) will occupy 20% of the market share of mobile telecommunication technologies worldwide (O'Dea, 2020). The majority of Europeans use smartphones and share their sensitive personal data via mobile networks. This reinforces the notion of humans being 'always connected' due to the large-scale utilization of modern technologies and inherent challenges to privacy it entails (Madhusanka, et al., 2018). 5G takes advantage of numerous technological novelties to provide lower latency and faster data processing. Artificial intelligence (AI), Machine Learning (ML), and cloud-based solutions bring new actors into the EU mobile networks, change the way networks are secured, affect how privacy is protected, and personal data is processed.

Against this backdrop, new legal research is needed to fill the gap between the deployment of AI in 5G networks and the legal mechanisms behind the use of such technology aimed at protection of privacy and personal data. AI and ML may prove to become both enablers of privacy-preserving solutions and significant privacy disruptors. It comes as no surprise that the emergence of novel technologies like AI and 5G is associated with the challenges to privacy and balance of interests. Given the recent changes in data protection regulation and the evolving

case law in this regard (Case C-131/12 (“Google Spain”) and Case C-311/18 (“Schrems II”)), the issues of privacy and data protection have become a prime factor in the modern digital economy.

This chapter will analyze the complex interplay between two rapidly evolving technologies – AI and 5G – and the legal concepts of privacy and consent to processing personal data. It is not the intention here to deliberate over a substantial volume of legal, ethical, economic, and societal challenges pertaining to the use of the abovementioned technologies but rather concentrate on how the AI and 5G brought together threaten to dilute the legal boundaries of privacy and reduce the importance of the consent to the processing of personal data.

1 Privacy and Data Protection: Clarifying the Setting

The legal discussion about privacy in relation to an individual’s home, reputation, and written communication existed for centuries, with some legal cases concerning eavesdropping dating back to 14th century England (Holvast, 2009). Privacy as a right had a long way to be formed and universally recognized, though. More than 130 years ago, American lawyers S. Warren and L. Brandeis published an article titled ‘The Right to Privacy’, which greatly contributed to recognizing and developing the new legal right of the same name. “*Political, social, and economic changes entail the recognition of new rights*”, as stated by the authors in the introduction to the article, was not a newly invented idea but served as a foundation for the argument for the recognition of the right to privacy (Warren & Brandeis, 1890).

Privacy was mainly associated with the integrity of the reputation and protection of home, personal life and communications and interpreted as “*the right to be let alone*” until the 1960s. It was then that the breakthrough in technological development – computers and their use for the storage of data – reignited the debate over privacy as a legal right. Early computerization and automated systems in the 1960s made the collection and transfer of personal data much

easier, which prompted first discussions over the need for the legal regulation of the processing of personal data (Kosta, 2013). Technology caused us to re-think the approaches to understanding privacy. The concept of privacy as “the right to be let alone” gradually shifted towards the right to exercise control over the information recorded about a particular individual (Kosta, 2013).

Through numerous discussions and legislative developments in the 20th century, the right to privacy has become an accepted concept in Europe. The process was not universal and straightforward, though. It took various working groups and a board of experts from the Council of Europe, OECD, European Communities, and different national states to develop multiple legislation extending the application of the right to privacy to the new legal relationships caused by technological developments. The European Court of Human Rights (ECtHR) has adopted a dynamic and evolutive interpretation of the concepts of ‘private life’, which was stated to have a broad character “*incapable of exhaustive definition*”, and ‘personal interests’, in order to produce decisions in line with technological advances (European Court of Human Rights, 2020). Moreover, in several cases (Copland v. the United Kingdom, Bărbulescu v. Romania, Wieser and Bicos Beteiligungen GmbH v. Austria, Petri Sallinen and Others v. Finland, Iliya Stefanov v. Bulgaria) the ECtHR asserted that technologies come within the scope of Article 8 of the European Convention on Human Rights (ECHR) (European Court of Human Rights, 2020).

Privacy, being a fundamental right according to both the ECHR and the Charter of Fundamental Rights of the European Union (CFREU) is aimed to protect the body, family, home, and communication of the individual (European Court of Human Rights, 2020). The above-mentioned article by Samuel Warren and Louis Brandeis raised the issue of privacy in the context of newspaper publications and gossip, which may harm the individuals’ reputation and

psychological well-being. Recent technological advances such as the massive use of mobile networks for storage of data, AI, and surveillance provided grounds for large scale invasion of privacy and the need to impose stricter rules on handling personal data. Implementation of 5G networks will have a dramatic impact not only on the economy and society, but also on the legal safeguards and protection of privacy and personal data.

The adoption of the General Data Protection Regulation (GDPR) by the European Union and its entry into force in May 2018 recognized the protection of personal data as a fundamental right distinguishing it from the right to privacy, guaranteed by the ECHR and CFREU. The GDPR serves as the general act on the protection of natural persons with regard to the processing of their personal data and applies, among other things, to mobile networks. The GDPR was adopted as a technology-neutral, risk-based, and future-proof law based on principles and deals primarily with the legal basis, aims, instruments, and limits regarding the processing of personal data and individuals' rights to the protection of their personal data.

The concept of personal data is particularly important since it essentially defines the scope and aim of the whole regulation. According to Article 4(1) of GDPR personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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".

The European Commission stated that the implementation of new technologies does not put the foundational principles of GDPR into question but rather affects the application of these principles to specific technologies (European Commission, 2020). Unlike the previous

generation of mobile technologies such as 4G, a wide range of principles and rights established by the GDPR, such as privacy by design, right to be informed, right to rectification, and right to object will have a substantial effect on the implementation of 5G networks and AI in the EU (Rizou, Alexandropoulou-Egyptiadou, & Psannis, 2020). The GDPR sets several grounds for the legitimate processing of personal data, one of which is the data subject's consent. Consent, in general, is a complex legal and ethical concept giving legitimacy to specific actions regarding the individual or their property and is a core principle of the system of protection of human rights. Article 7 GDPR states that consent must be given freely, specific, informed, unambiguous, and the data controller can demonstrate that the data subject has consented to the processing of their personal data. The request for consent must be clearly distinguishable from other information or requests and use clear and plain language. In this chapter, we interpret consent as an affirmative action concerning the processing of personal data following the GDPR meaning. In the context of EU law, data protection and privacy are treated as separate concepts, with discussion ongoing on

their precise legal nature.[1] Despite considerable overlapping, the legal nature of data protection and privacy differs in their scope.

2 AI in 5G Networks: Disruptive Novelties and the Role of Consent

Being an evolution of previous mobile network technology, 5G offers substantially higher data transfer rates, significantly shorter network latency, and greater bandwidth, allowing more significant download and upload speeds and a broad spectrum of use cases. 5G shall become a major enabler for the Internet of Things ('IoT'), which paves the way for among other things, remote surgery, telemedicine, autonomous cars, smart homes, offices, warehouses, highways, and eventually the entire smart cities ecosystem (Blackman & Forge, 2016). Likewise, the IoT technologies will transform sectors that are not traditionally associated with Internet technologies, such as agricultural, automotive, and construction sectors. The innovation brought by 5G shall become possible by deploying millions IoT devices (sensors, trackers, smartphones, home appliances), generating massive amounts of data. 5G enables fast transfer of this data to

1 See, for instance, Serge Gutwirth and Paul De Hert, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E Claes, A Duff and S Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006); Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology 73; Gloria González Fuster and Serge Gutwirth, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 Computer Law & Security Review 531; Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" Of A Right To Data Protection In The EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569;.

the computing facilities, where it is analyzed, and the response is carried back to the device, hence to the end-user.

5G networks rely partially on previous generations of mobile networks' technologies and infrastructure, namely 4G and 3G. Is it possible to say that considering all the technological novelties, 5G is not just succeeding 4G as the next generation of mobile networks but paves the way for a completely new type of mobile network.[2] Moving forward, Higher reliance on Internet-based services and a drastic increase in cellular data volume growth forces network operators and service providers to change existing approaches to establishing and maintaining core networks by paying more attention to security and efficiency. Modern telecommunication service providers face several challenges related to growth in mobile data exchange and in a number of devices such as increasing operational costs, the necessity to accommodate the coexistence of different generations of cellular networks such as 3G, 4G, and 5G, the need to upgrade equipment and the need to expand network capacity to accommodate an unprecedented number of Internet-connected devices. The pressure on existing mobile networks shall grow because of rising numbers of personal smart mobile devices and industrial Internet of Things (IoT) devices, with research claiming that Machine-to-Machine (M2M) communications shall generate larger amounts of data than all data generated by humans combined (Zhang, 2018). The expansion of physical infrastructure alone is not enough to keep up with the changes in mobile technologies and their usage. To cope with the challenge of processing immense data, there is a

2 "*Because 5G is not the same as the Gs that came before. Implementing this technology does not simply require an upgrade of the current network, it demands a new type of network altogether*". per Ivezic, M. (2020). Unlocking the Future – Why Virtualization Is the Key to 5G. 5G Security – 5G, MIoT, CPSSEC, Security Blog by Marin Ivezic. https://5g.security/5g/virtualization-key-5g/.

need to use advanced and efficient algorithms routing the data through the mobile network. Researchers indicate that to become fully operational and efficient, 5G networks must employ AI systems (Morocho Cayamcela & Lim, 2018). The security and privacy architecture of 5G networks will be much more complex and multi-layered than previous generations of mobile networks. These requirements arise from the immense amount of data processed in 5G core network. AI and ML solutions have been used before for modeling attack patterns to enhance security and privacy against sophisticated cyberattacks and hacks. This will most likely be the case for 5G network use cases as well. AI and ML may help identify the weaknesses in critical security points in authentication, identity, and assurance layers (Haider, Zeeshan, & Imran, 2020).

High speed of data processing in 5G networks enabled by AI and ML implementation may lead to practical problems in obtaining data subject's consent, providing information on processing, informing authorities, and affected data subjects on data breaches as well as concerns regarding interoperability and the execution of the right to erasure and rectification of personal data (Rizou, Alexandropoulou-Egyptiadou, & Psannis, 2020). 5G networks paired with AI algorithms will contribute to gathering and processing unprecedented amounts of personal data, which may require stricter standards of handling and processing, and will be transferred and processed continuously.

But with high speed comes a challenge to privacy. It would be tough to obtain an individual's valid consent for processing their personal data by AI and ML in 5G networks before such processing takes place because of the almost simultaneous transfer and processing of substantial amounts of personal data. A valid consent is a legal basis for processing of personal data and is mandatory in certain cases. According to Article 7 GDPR "[t]he data subject shall have

the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent". As was pointed out by Eleni Kosta, "The role of consent in this era is reduced, as the control of the individual over his personal information is overcome by the facilitation of everyday activities in electronic communications and especially the internet, to the extent that the privacy of the individual is not infringed" (Kosta, 2013). Extensive information about the devices and wearables of the data subject including sensitive health data such as pulse rate or fitness will be gathered and processed using AI almost instantly without the possibility to obtain valid consent the moment such data subject is within the range of 5G-based IoT systems. While data subjects may provide their consent to gather and process such data locally or for a specific purpose (e.g. tracking the pulse or other health data), the use of such data for training ML algorithms may be considered too extensive. According to 'A first assessment based on stakeholder inputs – Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem' by the Body of European Regulators for Electronic Communications (BEREC) there is a risk of inability to obtain a valid consent by multiple data processing actors in 5G value chain since such actors will not have a direct relation to end-users (BEREC, 2019). Another significant challenge is the feasibility of verifying child's consent to data processing. According to Article 8 of GDPR "Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child" and "The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology". The data controller has an obligation to undertake 'reasonable efforts' to

verify whether child's parents or caretakers indeed provided their consent to processing child's personal data.

AI and ML solutions will also enable real-time profiling and individual automated decision-making regulated by Article 22 GDPR. The Article states that the right of the data subject bot to be subject to a decision based exclusively on automated processing unless such profiling: (a) is necessary for entering into or performing a contract between a data subject and a controller; (b) is authorized by EU or Member State law; (c) is based on the explicit consent of the data subject. The last requirement is the toughest to comply with, considering the problem of obtaining data subject's consent before the processing of data occurs. Article 7(2) GDPR directly requires to inform the data subject of the content of consent *before* the data subject can give it.

5G relies on a larger number of base stations, IoT devices and sensors than previous generations of mobile networks. Precise geolocation of data subjects assisted by AI and ML algorithms under such conditions becomes much more accessible. In its Opinion 13/2011 on Geolocation services on smart mobile devices Article 29 Working Party (Article 29 WP, replaced by the European Data Protection Board after the adoption of GDPR) stated that "*smart mobile device is very intimately linked to a specific individual*" (Article 29 Working Party, 2011). The owner of the smartphone stores large amounts of personal data on the device and is unlikely to give it to another person for a considerable amount of time, which allows to use a smartphone as a unique identifier of the individual. Anyone who gets lawful or unlawful access to the geolocation data may learn the home address, workplace, habits, and routine of the data subject. Geolocation data may be qualified as a special category of personal data if it reveals political opinions (e.g. attendance of political rallies, gatherings, meetings), religious beliefs (attendance of religious establishments or sites), trade union membership (attendance of trade union

meetings) of the data subject as stated in Article 9(1) of GDPR. While geolocation was possible in 3G and 4G networks, 5G networks bring it to another level by using AI and ML on a larger scale and enabling the high precision and speed of such geolocation not possible in previous mobile networks. Correspondingly, the requirements for informed consent may be stricter since the impact of the data breach or data leak is higher.

Obtaining an informed and freely given consent is a major challenge, since it might be hard to articulate all required information properly and accurately regarding the technology involved (AI), specific aims of data processing, and timeframe of storage of data, among other things. Technical issues deepen this challenge, as data controller must obtain consent before the processing actually takes place, which is not always realistic in the setting of AI in 5G networks. Possibly, solution providers will provide very limited information in the consent and ask for it *as hoc*, after processing personal data they only ask the consent for. These factors greatly contribute to reducing the role of consent in 5G networks.

3 The Impact of AI in 5G Networks on Privacy and Principles Relating to the Processing of Personal Data

The issue of possible adverse effects on privacy posed by AI implementation was addressed by the Parliamentary Assembly of the Council of Europe in its Recommendation on Technological convergence, artificial intelligence, and human rights. The Recommendation recognized the possibility of consequences for human rights in light of the intersection between various technology sectors, including AI solutions (Parliamentary Assembly, 2017).

AI and ML were described as "*perfect match*" for the use in 5G networks since AI algorithms can learn from complex patterns and assist with autonomous operations within the network, creating a scalable and data-driven solution (IEEE Future Networks World Forum 2021).

AI can be used for developing 5G network architecture, automating functions such as optimization, security analysis, and fault prediction. Both AI and ML algorithms will analyze user's data transferred by 5G networks to develop more efficient services and applications. An important feature of AI in 5G is that it is used in all layers – from Radio Access Network (RAN) to core network and edge computing layer. AI is not limited to specific operations but may be rather omnipresent in 5G. In relation to privacy and protection of personal data AI and ML solutions can be deployed to optimize the use of resources for data processing in the cloud, detect anomalies and generate predictive analytics based on user's data. To train the AI algorithms and obtain useful and accurate results, large data must be fed to the algorithm. The more precise and up-to-date data is provided, the more tailored AI algorithm is obtained. Under normal circumstances developing a working AI would take years and the large number of resources. 5G network may serve as a great source of data for training AI algorithms since virtualization and edge computing technology significantly contribute to practical storage and management of ever-expanding human-generated data. In a context where AI technology is deployed as a part of the larger 5G ecosystem, there is a need to protect individuals' rights to privacy and protection of personal data while simultaneously refraining from unnecessarily hindering technological development.

One of the crucial challenges is determining the statuses of (joint) controllers and processors in 5G networks. Data controller is a natural or legal person or public authority or agency that determines the purposes and means of processing personal data, and data processor is any entity that processes this personal data on behalf of the controller. Joint controllers jointly determine the purposes and means of processing personal data, according to Article 26 of GDPR. However, the controller's status is autonomous, and the allocation of legal responsibilities must

be where the real influence on data processing-related decisions is. AI and ML solutions can be provided by multiple companies and individuals from different jurisdictions, possibly involving non-EU states. This complexity causes the need for consideration of cross-border transfers of data, establishing effective data governance, resolving the problem of data ownership, and ensuring transparency.

AI and ML algorithms used in 5G networks will also have to comply with the principles relating to processing personal data described in Article 5 GDPR which serve as a foundation of protecting personal data in the EU. These principles can be applied in different contexts and are not limited to a particular technical, social, or economic domain (Kuner, Bygrave, Docksey, & Drechsler, 2020). The principles include:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality.

An additional principle of accountability states the responsibility of the controller to demonstrate compliance with the rest of the principles. Linking the principles relating to processing of personal data to specific privacy and data protection challenges posed by the AI in 5G networks will give us an understanding of how the AI contributes to dilution of the right privacy and the

right to data protection – a potential diminishing of existing privacy and data protection safeguards present in ECHR, CFREU, and EU legislation.

The principle of lawfulness, fairness, and transparency incorporates three requirements and aims to protect personal data from fraudulent gathering and processing. Lawfulness is the first requirement of the principle and means that solutions providers such as AI and ML must respect all applicable laws and regulations concerning processing personal data.

The specific elements of transparency of data processing include: (a) easy access to information regarding processing; (b) clear identity of the controller and the purposes of the processing; (c) provision of information regarding risks, rules, safeguards, and rights. The vendors in AI in 5G networks use cases must ensure compliance with these elements, namely give the information regarding processing personal data, identify the structure of (joint) data controllers and exhaustive explanations regarding purposes of processing and provide the information on possible risks, rules, safeguards and data subject's rights. The complex and dynamic architecture of 5G networks with AI and ML algorithms may prove to be an obstacle to compliance with this principle. Moreover, it is pretty challenging to explain the nature of AI and ML themselves in simple terms. Providing information on specific risks, rules, and safeguards concerning the processing of personal data by AI solutions in 5G networks will be even more difficult. It does not preclude the use of AI in 5G networks. Still, it requires AI solution providers to spend considerable resources on articulating the necessary information to data subjects.

Fairness requires that personal data must be obtained through valid and fair means and not through fraud, deception or without awareness of the data subject (Kuner, Bygrave, Docksey, & Drechsler, 2020). Fairness also implies that controllers and processors should process data only in ways that data subjects would reasonably expect (Information Commissioner's Office,

2020). This essentially means that data subjects must be aware of how their data will be used for AI algorithms enhancing 5G networks. Considering the real-time application of AI in 5G this would not always be possible. Moreover, if the AI or ML algorithm produces erroneous, biased, or discriminatory results due to inaccurate or unreliable data, it may negatively affect the rights of data subjects (Norwegian Data Protection Authority, 2018). Biased or discriminatory results generated by the AI and ML algorithms may substantially affect an individual's right to privacy as stipulated by Article 8 ECHR, which is amplified by a massive number of users in 5G networks. Appropriate safeguards must be implemented to prevent any AI and ML applications from interfering with the right to private life by creating algorithms emphasizing racial or ethnic origin, sexual orientation, political opinion, religion or beliefs, genetic or health status, membership in trade unions. A faulty decision based on a discriminatory algorithm may lead to large-scale consequences in a huge mobile network with many users like 5G.

Purpose limitation is the second processing principle defined by GDPR and requires that personal data is gathered for a specified, explicit, and legitimate purpose. Data controllers AI and ML solutions in 5G networks will need to ensure the provision of free, accessible, specific, and unambiguous information on personal data processing. Such purposes may vary depending on the particular vendor or party processing personal data. Purposes themselves must be clear, precise, explicit and legitimate. Legitimate purposes should not lead to a disproportionate interference with the rights, freedoms, and interests of the data subject favoring the data controller's interests (Kuner, Bygrave, Docksey, & Drechsler, 2020).

The data minimization principle requires limiting the processing of personal data to 'what is necessary in relation to the purposes for which they are processed' providing a clear link with the principle of Purpose limitation. It is vital to ensure that privacy-preserving technologies and

techniques accompany the roll-out of virtualized 5G networks. This principle may prove to be extremely challenging to comply with for AI and ML applications in 5G networks. As was stated before, the development of an AI algorithm or model requires an enormous amount of data. The data minimization principle forbids the excessive processing of personal data, which may hinder the development of AI and ML algorithms in 5G networks. Data controllers aiming to use personal data for creating AI-based solutions will have to define specific purposes and characteristics of data (type, amount, level of detail) in order to develop any kind of AI algorithm based on personal data from 5G networks. Re-using old personal data is possible, but data controllers cannot re-use it for any other purpose than the one used to gather this data. Data minimization also requires the data controllers to respect the right to privacy and refrain from using excessively detailed or non-anonymized data (Norwegian Data Protection Authority, 2018). This forces the AI and ML developers to spend considerable resources on carefully defining the purposes of processing and the intended area of application of AI solutions.

The principle of accuracy requires controllers to keep the data up to date and rectify or erase inaccurate and incomplete data (Kuner, Bygrave, Docksey, & Drechsler, 2020). Considering the technological novelties brought by the new generation of mobile networks and complications related to processing vast amounts of data, it is unclear how exactly this principle will be implemented in virtualized 5G networks. In practice, it may be virtually impossible to rectify or erase personal data from the technological perspective. Another technical problem is to keep detailed records of data processing activities using AI and ML technologies and track the flow of personal data. Such records may require substantial computing and storage resources, and their implementation can be complicated.

The storage limitation principle requires controllers to clearly indicate the specific and adequate timeframe for storing personal data. It is prohibited for data controllers to retain gathered personal data beyond the timescale necessary to process data according to the purposes for such processing (Kuner, Bygrave, Docksey, & Drechsler, 2020). Data controllers using AI and ML will need to apply privacy-preserving techniques, like in the case of data minimization principle. While assessing the risks posed by blockchain, Commission Nationale de l'Informatique et des Libertés (CNIL, French Data Protection Authority) stated that some information can be stored without a retention period in exceptional cases.[3] However, in such cases, a data protection impact assessment (DPIA) is required. Certain exceptions are likely possible for AI applications in 5G networks, but they are constrained and must be backed by legal grounds.

Appropriate security (labeled as 'integrity and confidentiality principle') means that processing of personal data is done "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental

3 "If justified by the purpose of the processing and if a data protection impact assessment (DPIA) has proven that the residual risks are acceptable, personal data may exceptionally be stored on the blockchain, in the form of a traditional fingerprint (without a key) or even in cleartext. Indeed, some data controllers may have the legal obligation to make some information public and accessible, without a retention period: in this particular case, the storage of personal data on a public blockchain can be envisaged, provided that the DPIA concludes that the risks for data subjects are minimal". Commission Nationale de l'Informatique et des Libertés. (2018). Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

loss, destruction or damage, using appropriate technical or organisational measures" (Information Commissioner's Office, 2020). As mentioned above, multiple actors will be responsible for different elements in 5G networks and may apply different security standards and tools. 5G networks relying on efficiency of AI algorithms may be reconfigured in numerous ways to create various types of networks with different standards and solutions pertaining to privacy and security. AI and ML developers may be wary of sharing their architectural and IT solutions or commercial secrets like business and data practices in order to ensure transparency and react to inquiries from individuals and regulatory bodies. Lack of formal requirements on transparency may result in different objectives in trust pursued by various actors and causes a situation where users cannot obtain reliable information on the security standards and tools used to protect their data. Another concern is related to the use of AI and ML solutions with their unresolved security vulnerabilities. Complex software systems like AI require rigorous testing in a protected environment before any real-life application, but no test can guarantee absolute security. Bugs, deficiencies, and code vulnerabilities may be present and exploited for a considerable time before they are revealed and corrected. The providers of services have to implement state-of-the-art security is solutions. It is hard to identify state-of-the-art in AI and ML, however.

The final principle is the principle of accountability, and it is essentially an obligation to ensure compliance with all other principles listed in Article 5(1) of GDPR. Article 29 WP referred to 'data deluge' effect "where the amount of personal data that exists, is processed and is further transferred continues to grow" (Article 29 Working Party, 2010). The principle of accountability requires data controllers to adopt measures to effectively comply with the data processing principles and demonstrate such compliance. Technological developments contribute to the growth of the amount of data being processed, so the impact of data breaches and data leaks and

risk of misuse of personal data increase.[4] Article 29 WP also mentioned legal certainty as one of the challenges towards the implementation of principle of accountability since the requirements of the principle are not detailed (Article 29 Working Party, 2010). The ways and instruments to assess the level and effectiveness of compliance with the principle of accountability may differ and are flexible. According to the Opinion of Article 29 WP, "[f]or larger, more complex and high risk processing, internal and external audits are common verification methods" (Article 29 Working Party, 2010). There is no list of means of verification or authorized methodologies, but the Opinion of Article 29 WP mentions voluntarily certification as one of the instruments of achieving compliance. EU and national legislation usually regulate the accreditation of certification programs. Since 5G networks definitely fall within the category of 'complex and high risk processing' and may contribute to 'data deluge' effect mentioned by Article 29 WP, it is likely that the compliance of vendors and actors processing data through 5G networks with the principle of accountability will be subject to scrutiny by national DPAs.

Article 25 of GDPR established principles of data protection by design and by default, which require all controllers to implement technical and organizational measures "[t]aking into account the state of the art, the cost of implementation and the nature, scope, context and

4 The EDPB maintained that "[…] nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data […]" and "[a]s usual, during risk assessment the type of the breach and the nature, sensitivity, and volume of personal data affected are to be taken into consideration" linking volume of data to the impact of data breaches. See: EDPB 'Guidelines 01/2021 on Examples regarding Data Breach Notification', 12–19. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" in order to protect the rights of data subjects both at the time of the determination of means for processing and during the processing itself. Therefore, the implementation of technical and organization measures is needed to ensure that 'by default' only personal data which is necessary to achieve purposes according to purpose limitation is processed.

The principle of data protection by design and by default requires developers of applications, services and products to consider privacy and data protection principles early at the development of their respective goods and services. The idea is that incorporation of privacy and data protection requirements early substantially improves the privacy and data protection resilience and compliance of applications, services and products (Kuner, Bygrave, Docksey, & Drechsler, 2020). These legal provisions are aimed at ensuring the high efficiency of protection of data subjects' rights. The data controllers have a legal duty to implement technical and organizational measures to ensure compliance with data protection principles. These measures go beyond the security and reliability of software and include business practices, organizational principles etc. (Kuner, Bygrave, Docksey, & Drechsler, 2020). There is no exhaustive list of such measures, but they include, among others, training of personnel, automated erasure of outdated data, economic approaches to processing data, evading excessive processing of data or storing unnecessary data. AI and ML providers also must adopt a risk management approach to implement appropriate and effective technical and organizational measures to comply with the principle of data protection by design. The aim is to ensure the protection of data subjects' right to privacy and protection of personal data.

Objectively, compliance with this principle may prove to be a major obstacle for implementation of AI algorithms in 5G networks. The path to compliance with data protection by design principle is mainly linked with principles relating to processing of personal data, specifically data minimization and storage limitation. As was stated before, the complex and dynamic architecture of both AI and 5G, involvement of multiple actors from multiple jurisdictions, possible hesitation of involved actors to comply with transparency principle or give up commercially valuable personal data to comply with data minimization and storage limitation principles are factors hindering the fulfillment of legal requirements and ensuring the protection of data subjects' rights. This inevitably leads to tougher government control and loss of trust in the ability of technology to protect privacy.

Lastly, the implementation of AI and ML solutions in 5G will almost certainly require performing the Data Protection Impact Assessment (DPIA) which is an important instrument and requirement devised in the GDPR to get a clear understanding of possible impact of using certain technology or setting for processing personal data. According to Article 35(1) of GDPR, "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". Criteria required for such assessment are evident concerning AI in 5G networks:

- New technologies – both AI and 5G are disruptive novel technologies;
- Nature and scope – AI and ML will be used at a large scale up to becoming omnipresent in 5G networks and will continuously process personal data;

– High risk – due to large amounts of data and unclear safeguards the AI and ML solutions in 5G networks can be qualified as high risk.

DPIA is crucial but resource-consuming procedure. It is possible that many solution providers in 5G, including but not limited to AI, will hesitate to gather and provide full and accurate information in order to perform the DPIA.

4 Conclusion

It is evident, that numerous challenges related to implementing AI and ML solutions in 5G networks may impact the privacy and data protection safeguards and lead to the dilution of the right to privacy and diminishing the role of consent to personal data protection.

The telecommunications industry relies on technological novelties such as AI and ML to deliver the better, faster, and more reliable connections to users. The personal data processed via 5G networks may prove to have a high commercial value, attracting a considerable number of vendors and application developers. However, the new generation of mobile networks is vulnerable to software bugs, data leaks, lack of coordination between different parties involved in processing personal data, and cyber attacks. Other issues include the dynamic and complex architecture of 5G networks, issues of sharing confidential data on software elements or business practices, and resource-demanding compliance procedures.

Implementation of effective privacy-preserving technologies, data protection measures, and security standards is a requirement of law and a necessity enabling the operation of 5G network as a whole. As was noted by S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis (2020), “[t]he scope of privacy protection would be not only the effort to avoid the

administrative fines of millions of euro, but to establish from the beginning of 5G technology, a fair integrated treatment for data protection rights". Adherence to GDPR requirements, namely to principles relating to processing personal data, the principle of data protection by design and by default is crucial for ensuring privacy and data protection. Users must be able to easily obtain full and clear information on the processing of personal data, the data controllers, purposes of the processing, profiling, and automated decision-making, and the ways to exercise their rights to rectification and erasure of data. AI and ML providers must ensure that the consent to processing personal data is given freely, and it is specific, informed, and unambiguous. Considering the use of edge computing and cloud services and the option of distributed processing of personal data in 5G networks, traceability mechanisms must be implemented, which may prove to be a substantial challenge (AEPD, 2020). The fact that 5G contributes to generating an immense amount of personal data highlights the importance of effective data minimization measures.

The privacy, security, and data protection in 5G networks largely depend on the 5G value chain actors. Ultimately it is up to AI and ML providers to comply with the EU privacy and data protection legal framework. Their decisions, management practices, procedures applied will have a decisive impact on the functioning of 5G networks in general.

Acknowledgement

This research has received funding under EU H2020 MSCA-ITN action 5GhOSTS, grant agreement no. 814035.

Bibliography

AEPD. (2020). *Introduction to 5G technologies and their risks in terms of privacy*. Agencia Española de Protección de Datos.

Article 29 Working Party. (2010). *Opinion 3/2010 on the principle of accountability, 00062/10/EN WP 173*.

Article 29 Working Party. (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN WP 185*.

BEREC. (2019). *A first assessment based on stakeholder inputs – Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem*.

Blackman, C. and Forge, S. (2016). *European Leadership in 5G*. Directorate General for Internal Policies of the European Parliament.

European Commission. (2020). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – two years of application of the General Data Protection Regulation*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115.

European Court of Human Rights. (2020). *Guide on Article 8 of the European Convention on Human Rights*. Council of Europe.

Haider, N., Zeeshan, M. and Imran, M. (2020). Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends.

Holvast, J. (2009). History of Privacy. In F. H. S. Matyáš V., *The Future of Identity in the Information Society. Privacy and Identity. IFIP Advances in Information and Communication Technology*. Berlin, Heidelberg: Springer.

IEEE Future Networks World Forum (2021). AI and Machine Learning Track, https://ieee-wf-5g.org/ai-ml-track/.

Information Commissioner's Office. (2020). *Guide to the General Data Protection Regulation (GDPR).* ICO.

Kosta, E. (2013). *Consent in European Data Protection Law (Nijhoff Studies in European Union Law).* Martinus Nijhoff.

Kuner, C., Bygrave, L. A., Docksey, C., and Drechsler, L. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press.

Madhusanka, L., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. *2018 IEEE 5G World Forum (5GWF)*.

Morocho Cayamcela, M., & Lim, W. (2018). Artificial Intelligence in 5G Technology: A Survey. *International Conference on Information and Communication Technology Convergence (ICTC)*.

Norwegian Data Protection Authority. (2018). *Artificial intelligence and privacy*. Norwegian DPA.

O'Dea, S. (2020). *Mobile technology share by generation 2016–2025.* Statista.

Parliamentary Assembly. (2017). *Technological convergence, artificial intelligence and human rights.* Council of Europe.

Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR Interference With Next Generation 5G and IoT Networks. *IEEE Access*, 108052–108061.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 193–220.

Zhang, Y. (2018). *Network Function Virtualization*. Hoboken, NJ: Wileys, IEEE Press.