AI In Telecommunications – Impact On Regulation

Tijana Milovanović
Telecommunications
Communications Regulatory Agency
Sarajevo, Bosnia and Herzegovina
tmilovanovic@rak.ba
ORCHID: 0009-0005-6147-0051

***Abstract*—Although most AI systems in the telecommunications sector are still in a development phase, artificial intelligence is expected to play an important role in this sector in the next period. The integration of artificial intelligence (AI) into telecommunications is transforming how networks are managed, services are delivered, and customer interactions are handled. However, this rapid technological shift presents significant regulatory challenges, particularly concerning algorithmic transparency, data privacy, and the accountability of automated decisions. This paper explores the impact of AI on regulatory frameworks governing the telecommunications sector. Through a comparative analysis of existing regulations and emerging AI use cases, the study highlights the gaps in current policies and the need for adaptive regulatory models. A 5-step regulatory roadmap is proposed, which states that regulators and decision-makers must develop robust and, most of all, forward-looking policies.**

Keywords—artificial intelligence, EU AI Act, regulatory roadmap, risk-based approach, policy frameworks

I. Introduction

Developing a clear understanding of the benefits and risks associated with the experience of relying on artificial intelligence (AI) is becoming essential to ensure that AI is developed and used exclusively for the benefit of society. To address all the challenges and make the most of the opportunities that artificial intelligence offers, the European AI2 Strategy was published in April 2018 [1]. Although many of the AI solutions are still under research and development phase, it is expected that soon AI will control most functions in telecom networks. In this context, it is necessary to further identify these developments and assess any potential impact on sector regulation and potential contribution to the sector taking advantage of the opportunities of artificial intelligence.

II. legal Framework

In 2017, the European Council concluded that the EU urgently needs to address new trends: to include issues such as artificial intelligence and blockchain technologies, while ensuring a high level of data protection, digital rights and ethical standards. In April 2018, the European Commission published a European strategy, the Communication on Artificial Intelligence for Europe. In April 2021, the Commission presented an AI package, which includes a Communication on fostering a European approach to AI [2]; an update of the Coordinated Plan on AI (with EU Member States) [3], a proposal for a regulation establishing harmonized rules on AI (the draft Law on Artificial Intelligence, hereinafter: the Law on Artificial Intelligence) [4] and the AI Liability Directive [5].

The AI Act should ensure that AI systems in the EU are human-centric, safe and compliant with the EU acquis, and provide legal certainty to facilitate investment and innovation in AI. This Act also provides a regulatory framework for the application of fundamental rights and safety requirements on AI systems. Finally, the AI Act must facilitate the development of a single market for lawful, safe and reliable AI applications and prevent market fragmentation.

In July 2024, the Artificial Intelligence Act (Regulation (EU) 2024/1689) was published as the world's first legal framework for artificial intelligence, addressing its risks [6]. The act gives developers and AI implementers clear requirements and obligations regarding specific uses of AI, while seeking to reduce the administrative and financial weight on businesses. The Artificial Intelligence Act is part of a wider package of policy measures to support the development of trusted artificial intelligence, guaranteeing the safety and fundamental rights of people and businesses when it comes to AI, while driving adoption, investment and innovation in AI across Europe. This Act entered into force on 1st August 2024 and will be implemented in phases:

- From 2nd February 2025 prohibited applications of AI take effect.
- From 2nd August 2025 the rules for general-purpose AI will take effect for new GPAI models,
- From 2nd August 2026 the rules for high-risk AI systems will take effect,
- From 2nd August 2027, the rules for AI systems that are products or safety components of products regulated under specific EU laws will apply.

III. Artificial intelligence In Telecommunications

Artificial Intelligence is a comprehensive technology that can be applied to a variety of use cases. In the telecommunications sector, processes are highly digitized, and digital data is available for training and operating AI systems, facilitating the adoption of AI technology. Furthermore, the scale of telecommunications networks and the complexity of managing these networks, as well as relationships with end users, encourage the adoption of automated systems.

A. Benefits

The application of AI in telecommunications primarily contributes to a reasonable reduction in costs and helps in the automation of complex and repetitive processes. Network operators, equipment manufacturers and application providers will use AI to provide their end-users with personalized services and improve the quality of networks, all by processing large amounts of data and improving the decision-making process.

The rapid pace of technological innovation inherent in network evolution, the exponential growth of data and connected devices, and continuously challenging service demands are resulting in increasingly complex network infrastructure operations. Network intelligence and automation are needed to manage the expansion and density of network infrastructure and devices in communications networks, especially for next-generation networks such as 5G and 6G, where AI is the driving force behind innovation and digital transformation of business models.

The main advantages in the industry come from generative artificial intelligence, which goes a step further than simple process automation. Such models have great potential, with commercial applications for sales, marketing and customer relations, and enable accelerated business opportunity creation by reducing process complexity.

The main advantages of AI, recognized by chief experienced officers (CxOs) from top communications providers, are shown in the Figure 1.

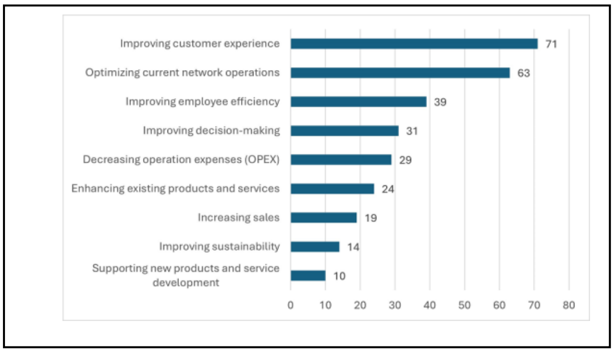

Fig. 1. The main advantages of AI in percentage [7]

B. Risks

Although not all computational approaches for AI systems require large amounts of data, access to real, high-quality data sets is critical for training and deploying AI systems. Low-quality, and especially one-sided data will lead to low-quality and non-objective results, and can negatively impact not only the AI user, but other stakeholders as well.

The introduction of AI-based solutions in telecommunications networks involves various actors in the value chain. Given the heterogeneous nature of the ecosystem and the automation of AI systems, there is uncertainty about the responsibility of everyone in case of unexpected or wrong outcomes.

1) Lack of trust in decision making: AI systems allow the processing of large amounts of data, automation of processes as well as the detection of patterns in datasets. Yet the complexity of AI systems, in particular AI systems using ML approaches, may render the evaluation of the results validation as a major challenge. Methods and procedures which ensure that the results presented by AI systems need to be understood and evaluated. In particular, the enhancement of the explainability of the outputs will be crucial to guarantee that disputes between stakeholders in the telecommunications sector can be tackled.

2) Privacy: In the context of accessing and processing large amounts of data in telecommunications, the privacy aspect also appears. Specifically, whether adequate safeguards are applied to the data used by AI systems to prevent misuse of that data. Data privacy, security and AI integration are the main challenges to be faced when implementing AI solutions. It seems that concerns about data privacy often arise from a reluctance to share data between different parts of the same organization.

3) Security: Cybersecurity research remains an important field for AI, for detecting and preventing cyberattacks. At the same time, appropriate measures need to be taken to ensure that these AI cybersecurity systems are robust and reliable. AI systems deployed by telecommunications providers themselves also need to be adequately secured to prevent malicious attacks with potentially wide-ranging impact. AI systems are vulnerable to automated adversarial attacks, often led by other AI systems, where data is manipulated to trick the model and result in erroneous outcomes [8]. Another example of a security risk would be unauthorized access to data resulting from a lack of control when data is aggregated across the company.

C. AI use case areas

This chapter will provide an overview of the variety of applications for AI systems in the telecommunications sector [9].

Network and capacity planning and upgrading are activities within the telecommunications sector that require enormous resources, both financial, material and human. The fact that networks are designed to anticipate their future usage further complicates this process. At the same time, the speed of development, especially in the mobile sector, requires frequent modifications to networks, which means that network planning and network upgrades are continuous activities.

For telecommunications providers, it is important to predict network usage and plan infrastructure accordingly. Network capacity planning aims to provide predictions and optimize the implementation or management of the infrastructure to cope with anticipated usage. AI systems can be applied to both fixed and mobile networks to facilitate network and capacity planning and upgrades. They can, for example, predict priority locations, identify optimal locations or routes for deployment, maximize energy efficiency, reduce electricity consumption, minimize the required number of transmitters or base stations, or design new network architectures. The main concern with this scenario is that different levels of data are available for urban and rural areas, which may lead to different levels of maturity in AI. Also, such AI systems may not be fully under the control of telecom operators, as they are embedded in network hardware.

Channel modelling is one of the most important research topics for wireless communication, since the propagation channel determines the performance of any communication system operating in it. Specifically, channel modelling is a process of exploring and representing channel features in real environments, which provides guidelines for network planning and optimization. The details provided by the respondents show the importance of real time network monitoring, which allows the early detection of anomalies, patterns and trends and therefore improved diagnosis and repair times in the network [10].

Classical spectrum management, based on a fixed spectrum allocation policy, leads to inefficient usage due to underutilization. ML techniques are used to optimize the flow of data between base stations and mobile networks. A well-functioning network needs different parameters that define the capacity and efficiency of the radio spectrum, such as distance to users and connected users. Those parameters can be improved by AI. The realization of dynamic spectrum access with cognitive radio largely depends on the willingness of the regulators to open the spectrum for unlicensed access, but it also involves a technical component that needs multidisciplinary approach from different fields, such as machine learning, computer networking, information theory or signal processing [11]. In recent years, there has been a trend for a more flexible approach to spectrum regulation.

QoS Optimization is instrumental in preventing and solving congestion in the network and providing end-users with the service level they require from the network. One of the most important tasks of QoS is to deal with real-time traffic that requires high bandwidth use, such as video calls and streaming services. With the adoption of 5G, the demand for real-time communication, for example for virtual reality (VR)-applications, increases. ISPs can employ various QoS techniques in their network, such as classification, marking, policing, shaping, congestion avoidance and queuing. These methods rely on several measurements including latency, error rate or jitter. AI can be used to optimize QoS by, for example, collectively analyzing a number of these parameters, such as those concerning the radio environment, quality of the perceived signal or the number of packets lost [12].

AI can analyze large amounts of data from different sources and identify unusual patterns in users' behavior, which could indicate a cyber-attack. When a potential threat is detected, AI-powered systems trigger real-time alerts and notifications to cybersecurity teams, enabling prompt and effective responses [13].

The number of attacks and their impact have particularly increased in the last years. The Communications Fraud Control Association (CFCA) estimates a 12% increase in fraud loss in 2023 compared to reporting the total amount of global telecom revenue loss in 2021 due to fraud at 2.5% of revenues ($38.95 Billion) [14]. In addition, it must be considered that fraud does not only impact telecommunication providers but often target their end-users.

Some of the most common frauds in the telecommunication sector include:

- Spoofing,
- A call back fraud based on massive missing calls,
- Subscription Fraud,
- SIM boxes are used to route international calls through the internet using VoIP and terminate those calls through a local phone.

At the same time, applications for fraud detection have progressed and have become more sophisticated, often making use of ML based AI for faster detection and prevention of frauds, such as text message scams and robocalls from reaching the public.

Of course, the importance that artificial intelligence can have in increasing sales productivity should not be overlooked. AI’s strength lies in task automation, interaction personalization, and workforce optimization. Through market segmentation, AI enables targeted access to different consumer groups. Given that large amounts of data are processed in a short time, the application of AI also reduces the costs of sales processes. Additionally, the process of providing support to end-users is transformed and makes it more personalized.

IV. Regulatory Implications

The use of AI creates several specific high risks for which existing legislation is insufficient. While there is already a robust legislative framework in EU and national level to protect fundamental consumer rights, certain specific features of AI technologies may create challenges in the enforcement of these laws and create high risks that require a regulatory response. The AI Act introduces a set of harmonized rules applicable to the design, development and use of certain high-risk AI systems, as well as restrictions on certain uses of remote biometric identification systems.

The proposed AI Regulation sets out rules to improve transparency and minimize risks to security and fundamental rights for AI systems to be used in the European Union. Its foundations are based on several key components that build a proportionate and risk-based European regulatory approach. First, it provides a technology-neutral and future-proof definition of AI systems, to the extent that it can cover techniques and approaches that are not yet known or developed [15]. Second, to avoid over-regulation, the proposal focuses on so-called “high-risk” AI use cases, i.e. where the risks posed by AI systems are particularly high. Whether an AI system is classified as high-risk depends on the purpose of the system and on the degree of potential harm and the probability of its occurrence. High-risk systems include, for example, AI systems intended to be used for lawful interception, fraud detection or automated decision-making for service provisioning. To ensure that the rules are future-proof and can be adapted to new uses and applications, there is a possibility to classify new AI systems as high-risk within certain predefined areas of use [16].

The Data Act includes provisions on data access, usage rights, interoperability and switching in cloud services. For AI technologies, especially generative artificial intelligence, access to vast amounts of data is critical for training algorithms and improving their capabilities, and the Data Act provides a framework for accessing, sharing and controlling data, seeking to ensure that it is shared and used in a way that is innovative, while protecting the interests of data creators and users [17]. Moreover, the Data Act establishes new rules to facilitate switching between cloud services and interoperability, which is essential to stimulate markets, address lock-in effects and ensure free choice and lower costs for users [18].

The deployment of AI in telecommunications introduces a series of regulatory challenges that stem directly from the technical and operational characteristics of industry. These particularities—such as real-time data processing, stringent network reliability requirements, and heightened user privacy concern necessitate specific regulatory frameworks to ensure that AI systems operate safely, fairly, and within legal bounds [19]. Table I shows AI regulatory aspects across 3 categories:

- Already regulated,
- Planned / in roadmaps,
- Those need to be addressed.

TABLE I. AI REGULATORY ASPECTS IN TELECOMMUNICATIONS

Regulatory Aspect	***Already Regulated***	***Planned / In Roadmaps***	***To be tackled***
Data privacy & protection	GDPR, ePrivacy Directive	EU AI Act	Specific data minimization
AI Transparency & explainability	GDPR	EU AI Act for high-risk systems	Standards for traffic classification, optimization models
Automated decision making	GDPR Art. 22	EU AI Act	Provisioning, credit checks
Surveillance & lawfull interception	National laws, GDPR	EU security policy discussions	AI-based bulk for interception, predictive surveillance
Cybersecurity& AI	NIS2 Directive, national security regulations	EU Cyber Resilience Act	AI-specific treat modleing frameworks
AI Use in Emergency services	National safety regulations	EU AI Act	Specific testing protocols for prioritization in crisis communicate
Spectrum Management	National telecom authorities	AI inclusion in spectrum automation roadmaps	Regulatory framework for autonomous spectrum sharing systems

V. AI REGULATORY ROADMAP

In the rapidly changing world of artificial intelligence, clear rules are needed to keep peace. Effective regulation is essential to ensure responsible access to this extremely powerful technology while preserving end-user confidence. Customer Experience Excellence Report UK 2024/25 [20] shows that none of the top-ranked companies in this report would be where they are without the use of AI. But at the same time, as AI is increasingly present in the business of companies, the question arises whether security and mutual trust with clients is at risk?

Now, when EU’s AI Act is adopted, it represents the framework from which the regulation should be further expanded. Each country needs to choose its own approach – whether to pass a new set of laws related to AI or to integrate it into existing regulatory frameworks.

The EU’s Act will come into effect across three phases (of 3, 6 and then 24 months) and its chief feature is to put AI use cases into four categories of risk: unacceptable (which will therefore be prohibited), high (this includes areas such as using AI to assist in credit scoring), limited (where the focus will be more on transparency that AI is involved) and minimal risk [21].

5-steps AI regulatory roadmap is presented in Table II. The first step in the regulatory process for any regulator would be to classify potential applications/industries as high, medium and low-risk AI applications and tailor further rules to the identified risk levels. Of course, chatbots for customer services do not require the same level of regulation as AI applications in the lawful interception assistance or billing. With this approach, it would be possible to focus on the most dangerous use cases and additionally monitor systems that can cause great harm to society frameworks.

In accordance with the identified risk levels, licensing should be introduced with a certain level of requirements that must be met. Although in Europe and the world there is a tendency towards deregulation and a system of general authorizations for the performance of certain activities, artificial intelligence requires a more traditional approach with establishing the appropriate balance between strong ethical approaches and the encouragement of innovation. Organizations that develop critical systems, such as those related to nuclear energy, pharmaceuticals, etc., could be required to obtain a license that confirms their technical competencies, data management methods, and the security protocols they use. will be more on transparency that AI is involved) and minimal risk [22].

TABLE II. AI REGULATORY 5-STEPS ROADMAP

Objectives		
Roadmap Steps	***Key Lesson***	***Example in Telecommunications***
Risk classification	Regulate AI proportionate to potential harm	Billing, Lawful Interception Assistance
Licensing & Certification	Ensure only qualified individuals & companies develop /operate critical AI	Cybersecurity
Testing & Validation	Test AI in controlled environment before full deployment	Load balancing, Fault predicition
Continuous Monitoring & Post-Market Surveillance	Track perfomance & address defects	5G Network slicing
Performance Reporting & Periodic Re-Certifications	Detailed documentation & mandatory repeating the licensing process	Network planning & optimization

A necessary step is also to define a rigorous testing and validation process before systems that apply AI are put into operation and widely deployed. Support efforts related to the development of a capabilities-focused risk-based approach, particularly the development and standardization of risk testing and evaluation methodologies and mechanisms. It is essential to ensure that AI reaches the required level of safety, security, and reliability before widespread deployment, especially in applications such as 5G network slicing. trust.

After all, mentioned before, ongoing audits, performance reporting, and periodic re-certifications can ensure AI doesn't drift in an unintended direction. Transparency and documentation of processes involving AI should be mandatory [21]. For important decision-making processes, such as hiring or network planning & optimization—explainability helps uncover and correct bias, thereby working to achieve greater public trust. trust.

The process of AI regulations presents a unique challenge and requires a high level of coordination in its implementation, the involvement and cooperation of all relevant institutions on state level, as well as business and civil society. Due to the comprehensive nature of this process, a good approach is to create a separate regulatory body that will be responsible for implementing and supervising the adopted laws and bylaws. This especially applies to defining who is legally responsible for AI-caused harm.

VI. Conclusion

Artificial Intelligence (AI) is rapidly transforming businesses, governments and society. From advanced customer support to complex medical diagnoses, AI brings great economic and social benefits. With all this enormous potential comes great risks that could bring huge harm to critical infrastructure or public health.

We have witnessed that throughout history, some major disasters, whether natural or political crises, have been 'trigger events' for the introduction of changes and the regulation of certain areas. Because AI technology is fast-moving and globally distributed, its regulation requires novel tools and international cooperation. It is a big challenge that the attitude towards AI is defined on a global level, and not that the regulation varies from country to country, because in this way large companies that operate globally will not be able to function.

Despite AI's promise, a significant gap in regulation remains. While some administrations have taken their first steps in this area, such as the European Union's AI Act and China's rules for generative AI, many regions still lagging behind. Even where frameworks exist, the rapid evolution of AI complicates further regulation. Regulators and decision-makers must, therefore, develop robust and, most of all, forward-looking policies.

References

[1] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Artificial Intelligence for Europe", April 2018.

[2] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Fostering a European approach to Artificial Intelligence", April 2021.

[3] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Annexes to the Fostering a European approach to Artificial Intelligence", April 2021.

[4] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS", April 2021.

[5] European Commission, "The Artificial Intelligence Liability Directive", September 2022.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), PE/24/2024/REV/1.

[7] Ericsson, "AI Business Potential understanding the value of AI for telecom operators", 2022.

[8] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[9] Body of European Regulators for Electronic Communications, "BEREC Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation", June 2023.

[10] https://www.researchgate.net/publication/335407971_Neural_Network-Based_Fading_Channel_Prediction_A_Comprehensive_Overview/fulltext/5d649eaf458515d6102666d8/Neural-Network-Based-Fading-Channel-Prediction-A-Comprehensive-Overview.pdf

[11] I. F. Akyildiz, B. F. Lo, R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey".

[12] R.E. Balmer, S.L. Levin, S. Schmidt, "Artificial Intelligence Applications in Telecommunications and other network industries" *Telecommunications Policy 44(6)*, 2022.

[13] https://www.datacenterknowledge.com/ai-data-centers/top-three-use-cases-for-ai-in-cybersecurity

[14] https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud/

[15] Body of European Regulators for Electronic Communications, "BEREC high-level position on artificial intelligence and virtual worlds", March 2024.

[16] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), PE/24/2024/REV/1

[17] European Commision, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Communication on boosting startups and innovation in trustworthy artificial intelligence", January 2024.

[18] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[19] World Economic Forum, "Artificial Intelligence in Telecommunications", White paper, February 2025.

[20] https://kpmg.com/uk/en/home/services/consulting/customer-consulting/customer-experience-excellence.html

[21] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[22] OECD, "Assessing potential future artificial intelligence risks, benefits and policy imperatives", November 2024