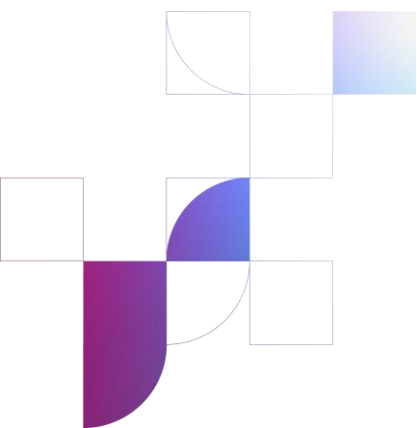**BEREC Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation**

8 June 2023

Content

EXECUTIVE SUMMARY

Although most artificial intelligence (AI) systems in the telecommunications sector are still in a development phase, AI is expected to play an important role in the sector in the mid-term. This BEREC report seeks to identify these developments in selected use cases, to assess if those use cases may have an impact on regulation, and to raise further awareness of the different use cases as well as the benefits and risks of opportunities regarding the application of AI in the sector.

Since 2017, the European institutions have intensified their attention on AI, fostering its development while ensuring that EU values and citizens' rights are preserved. At the moment of writing this report, a draft Artificial Intelligence Act is being discussed by the European co-legislators. The objective of this regulation is ensuring that AI systems in the EU are safe and in line with EU law as well as providing legal certainty to facilitate investment and innovation in AI. This legal framework will be complemented by the recently proposed draft AI Liability Directive.

AI relies on the input of multiple enablers, including access to large amounts of reliable data, adequate capacity to store and process this data, and as the relevant Electronic Communication Network (ECN) connectivity. In addition, it is expected that technologies such as edge computing architectures will contribute to fully exploiting the potential of AI, making it more accessible and enhancing its performance. BEREC notes that difficulties to access one or more of these enablers may imply unbalances between different players in developing and adopting AI. BEREC also underlines the relevance of standardisation to help decrease time to market and development costs as well as enhancing a level playing field, interoperability and innovation, market surveillance and mitigate potential lock-in effects.

AI may bring significant benefits for the sector. AI technologies promise considerable savings in terms of costs and can help automate complex and/or repetitive processes with AI techniques to optimize network operation, improve customer service or detect new business opportunities as well as to support the expansion and densification of network infrastructure and devices in communication networks. Furthermore, the appropriate application of AI can promote energy efficiency of networks, which can contribute to positive environmental impacts in addition to costs saving associated with lower energy consumption. On the other hand, AI also entails a number of risks related to the availability of unbiased and reliable data; liability in case of error due to the complexity of AI ecosystems; ensuring the explainability in the decision-making; privacy issues and cybersecurity implications.

The proliferation in the use of AI systems may also have an impact on the design of telecommunications networks such as new hardware requirements and the integration of different hardware and software components. AI systems based on cloud services may require low latency and could lead in some cases to decentralisation in terms of data centre distribution. AI systems deployed together with internet of things (IoT) infrastructure entailing

a large number of devices connected to one system may affect the network load in case of malfunctioning.

Telecom market players consider that the adoption of AI in the operational procedures will become a norm approximately in the next six to ten years. Many of these changes in networks driven or enabled by AI systems are linked to network virtualization. Other developments could potentially impact on what networks do as well as how networks function[1] or allow automatically orchestrate and manage network resources while assuring the Quality of Experience demanded by users.

BEREC develops further on six AI use case areas in telecommunications: Network and Capacity Planning and Upgrades; Channel Modelling, Prediction and Propagation; Dynamic Spectrum Sharing; Quality of Service Optimization and Traffic Classification; Security Optimization and Threat Detection and Fraud Detection and Prevention.

Finally, the report describes the possible uses of AI solutions by NRAs. AI systems could be used by public administrations such as NRAs, to improve processes related to policy-making, to public service delivery and the internal management of public authorities. Whilst some NRAs have studied the use of AI in the telecommunications industry, for the time being, few have explored ways about how AI could be used within the internal processes of the NRA.

Although the potential benefits of AI are paramount, there are also risks associated with the applications of AI. Good decision-making depends on unbiased and reliable data. How the algorithms use the data is often not clear, possibly leading to a lack of trust in the automated decision making. Privacy and security remain important aspects that justify close monitoring of AI solutions.

Whereas operators have found many ways to apply AI solutions, the NRAs have not, so far, much experience in making use of AI. Literature and some examples from European regulators, or regulators from outside Europe show that there are a good number of use cases for AI. AI solutions could be used for policy making, public services or internal management. BEREC expects AI to mature more over the years, both with operators as with NRAs.

With the growing importance of AI, NRAs have to acquaint themselves also with the risks associated with AI, the methods of monitoring and the methods of assessing. A good knowledge of the workings of AI is required when making the choice of implementing AI solutions in order to assess the outcome and impact of the use of AI, or the workings of the algorithm itself.

In addition, BEREC signals that NRAs could play a role in the implementation of the AI Act in a national level, in particular when AI is being used in the provision of ECN/S by coordinating with other relevant bodies and providing technical support based on their specialized

---

[1] For instance, networks could be used as sensors for AI applications or for managing responses in case of disasters

knowledge and experience in the sector. NRAs should also be equipped to address potential sectoral competition concerns that might arise in the future regarding the application of AI.

1. INTRODUCTION

Developing a clear understanding of both the benefits and risks associated with use cases relying on AI becomes essential to ensure that AI is developed and used for societal wellbeing. Following this standpoint, the EU has fostered a coordinated approach for the development of AI with both the objective of promoting the uptake of AI, seizing the opportunities brought by this technology, and of addressing the associated risks. To address these challenges and make the most of the opportunities AI offers, the Commission published a European AI strategy in April 2018[2]. The strategy places people at the centre of the development of AI. More recently, the Commission has put forward a draft Artificial Intelligence Act following this human-centred approach.

While AI is progressively being deployed in all types of economic and societal activities, this BEREC report is focused on delivering a high-level view of the application of AI solutions for the provision of electronic communication networks and services (ECN/S), on the one hand, and of AI solutions used for regulatory purposes, on the other hand.

Although many of the AI solutions related to the provision of ECN/S services are still under research and development phase, it is expected that in the mid-term AI will control the majority of functions in telecom networks[3]. In this context, BEREC seeks to further identify these developments and assess any potential impact on sector regulation and, the potential contribution to seizing the opportunities of AI by the sector.

In this report, BEREC provides a general overview of the impact of AI in the sector, potential AI risks and benefits to consider when adopting AI solutions, and the future developments foreseen in the mid-term. In addition, BEREC explores more granularly a number of selected use case areas, some of them still being developed, some already adopted by the providers, to gain efficiencies in relation to several areas of network deployment and services provision, and possibly enabling new opportunities for value creation.

While currently the majority of NRAs have not incorporated yet any AI solution to carry out their regulatory functions, BEREC notes the potential of these tools to gain efficiencies to carry out public activities, including supporting the fulfilment of regulatory tasks. One example identified in the report is the FCC project for the use of AI in broadband mapping.

Although BEREC has not specifically analysed AI before, some of its reports touch on relevant issues for the uptake of AI. Among those BEREC documents to consider are the Input paper

---

[2] https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)237&lang=en
[3] Managing AI use in telecom infrastructures. Dialogic. 2020.

on Potential Regulatory Implications of Software-Defined Networking and Network Functions Virtualisation[4], the Report on the Data Economy[5], the Summary Report on the conclusions of the BEREC's Workshop on Open RAN[6], the Report on Enabling the Internet of Things[7] and, more recently the High-Level Opinion on the European Commission's proposal for a Data Act[8].

For the elaboration of this report, BEREC gathered information by means of three surveys. One of these was addressed to the NRAs and focused on the adoption of AI solutions for regulatory purposes and identifying the relevant use cases for the study. The other two were addressed to the market players and academics. It must be noted, however, that only one response from academia was received. The full list of respondents is available in ANNEX I.

2. LEGAL FRAMEWORK

In October 2017, the European Council invited "the Commission to put forward a European approach to artificial intelligence by early 2018"[9]. The European Council concluded that the EU needed a sense of urgency to address emerging trends: this includes issues such as AI and blockchain technologies, while at the same time ensuring a high level of data protection, digital rights and ethical standards. Following this Council invitation, the Commission published a European strategy in April 2018, the Communication on the Artificial Intelligence for Europe[10]. This strategy places people at the centre of the development of AI and aims at making the EU a world-class hub for AI. In April 2021, the Commission presented an AI package including a Communication on fostering a European approach to artificial intelligence[11]; an update of the Coordinated Plan on AI (with EU Member States),[12] a proposal for a regulation laying down harmonised rules on AI[13] (the draft Artificial Intelligence Act, hereinafter, AI Act), and the AI Liability Directive.

The AI Act aims at ensuring that AI systems in the EU are human centric, safe and in line with the EU law as well as providing legal certainty to facilitate investment and innovation in AI. The AI Act also provides a governance and enforcement framework for the application of fundamental rights and safety requirements on AI systems. Ultimately, the AI Act has to

---

[4] BoR (16) 97, https://www.berec.europa.eu/en/document-categories/berec/others/input-paper-on-potential-regulatory-implications-of-software-defined-networking-and-network-functions-virtualisation

[5] BoR (19) 106, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8599-berec-report-on-the-data-economy

[6] BoR (22) 138 https://www.berec.europa.eu/en/events/berec-events-2022/berec-workshop-on-open-ran

[7] BoR (16) 39, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

[8] BoR (22) 118, https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-high-level-opinion-on-the-ecs-proposal-for-a-data-act

[9] http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf

[10] ibid. pg. 4

[11] https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence

[12] https://ec.europa.eu/newsroom/dae/redirection/document/75787

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

The AI Act allows the differentiation of AI systems by considering:

a. **Unacceptable risk AI systems** that are particularly harmful and contravening Union values (e.g., AI systems that deploy subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm). Those AI systems are prohibited by the AI Act.

b. **High risk AI systems** that pose significant risks to the health and safety or fundamental rights of persons. The AI Act imposes a set of requirements on those systems and have to follow conformity assessment procedures before those systems can be placed on the Union market.

c. **Limited risk AI systems** on which only minimum transparency obligations are imposed (e.g., chatbots).

d. **Minimal risk** on which no legal obligations are imposed (e.g. spam filters).

The proposed rules are to be enforced at Member State level, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board is envisaged. Finally, measures to support innovation are also proposed, such as AI regulatory sandboxes[14].

At the moment of writing this report, the legislators are debating the classification of digital infrastructures under the different categories of the AI Act. The European Commission (EC) proposal includes as high-risk AI systems related to the management and operation of critical infrastructure those intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity, but not ECN/S. The respondents to the survey circulated to market players underlined that ECN/S should not be classified as high risk per se, but solely where it concerns the use of AI applications in ECN/S for the management of the mentioned critical infrastructures. BEREC notes that addressing this issue is not part of the scope of this Report.

In addition to the legislation specifically addressing AI, the EU *acquis* include a number of relevant pieces of legislation that regulate the conditions of access to data, an essential input for the development of AI. The main ones are the General Data Protection Regulation (GDPR)[15], the Directive on privacy and electronic communications[16], the Network and

---

[14] Although the AI Act is still under the legislative debate, Member States are already working on sandboxes. The first regulatory sandbox on Artificial Intelligence was presented by Spain in June 2022. https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=EN

Information Security (NIS) Directive[17], the Regulation on a framework for the free flow of non-personal data in the European Union[18], the Directive on open data and the re-use of public sector information[19], the Data Governance Act[20], as well as the proposed Regulation on harmonised rules on fair access to and use of data (Data Act)[21]. Recently, a proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)[22] was published.

3. ARTIFICIAL INTELLIGENCE FUNDAMENTAL ELEMENTS

The AI Act defines[23] AI systems as software that is developed with one or more of the techniques and approaches listed in its Annex I, and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

The AI techniques and approaches in Annex I of the AI Act encompass:

a) systems which employ machine learning (ML) approaches,

b) logic- and knowledge-based approaches, and

c) statistical approaches (including Bayesian estimation).

BEREC notes that, at the moment of drafting this report, this definition is under discussion by the legislators and, thus, subject to changes in the legislative process. Without pre-empting the outcome of the legislative process and taking into consideration that currently there is no AI system definition commonly agreed, BEREC draws on the AI Act definition for the preparation of this report. The lack of a common definition of AI was also raised by the stakeholders in their responses to the survey.

The overview provided in Annex I of this Report contains further technical details about these AI techniques and other technical aspects of the AI systems considered during the preparation of this Report.

---

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN
[22] https://ec.europa.eu/info/sites/default/files/1_1_197605_prop_dir_ai_en.pdf
[23] The EC defines "AI systems" building on the definition issued by the OECD Recommendation of the Council on Artificial Intelligence. The rationale of the EC for choosing this definition is that it is technology neutral and future-proof. Additionally, to further increase legal certainty, the definition is complemented with a list of specific approaches and techniques used for the development of AI systems included in Annex I of the AI Act. To ensure that this list is future proof, the EC will be able to update the use cases listed in high-risk use case areas by means of delegated acts.

The latest wave of AI has been possible thanks to ML techniques. ML is based on the use of very large amount of data to teach machines to solve determinate problems. On the basis of this data, the software can identify new patterns and create new rules. A concrete type of ML is deep learning or neuronal networks, which aim to imitate the processing of the human brain. The input data is processed at different layers. Each layer output is used as an input for the next layer.

Consequently, AI currently relies on a number of enablers or inputs: access to reliable data and ultimately large amount of data and capacity to store and process this data (i.e., computing processing power and data storage) as well as connectivity. It should be noted that beyond the application of AI systems by telecommunications providers, their services may play an important role for the use of AI – for instance, through the provision of low-latency connectivity services or through mobility data. In addition, it is expected that technologies such as edge computing architectures will contribute to fully exploiting the potential of AI, making it more accessible and enhancing its performance. Difficulties to access one or more of these enablers may imply unbalances in the possibilities to develop and adopt AI by different players.

Standards play a key role by facilitating interoperability and switching, and thus mitigate potential lock-in effects. According to van der Vorst et al. (2020), standardisation helps decreasing development costs and time to market, facilitating market surveillance, and enhancing a level playing field, as well as interoperability and innovation while ensuring ex ante control.[24] Along these lines, the lack of harmonised standards for AI to facilitate its use across Europe was also mentioned as a concern by the survey respondents.

The AI Act anchors compliance of high-risk AI systems with the Regulation in the compliance with relevant standards. For this reason, standards approved by CEN-CENELEC[25] are key to the implementation of the AI Act. These can include standards related to the data used for training[26], design[27] or the classification[28] of computational approaches for AI systems. Furthermore, the AI Act encourages voluntary compliance for all types of AI systems as well as the development of codes for important issues such as social and environmental sustainability.

Beyond the AI Act, a relevant standardisation body in particular for the telecommunications sector is the International Telecommunications Union (ITU) which has published a variety of standards for AI applications related to telecommunications[29], and set up multiple working

---

[24] Van der Vorst et al., 2020: Managing AI use in telecom infrastructures. Advice to the supervisory body on establishing risk-based AI supervision.

[25] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/

[26] For instance, the ISO/IEC standard ISO/IEC CD 5259-1 (https://www.iso.org/standard/81088.html?browse=tc).

[27] For instance, the ISO/IEC standard ISO/IEC DIS 25059 (https://www.iso.org/standard/80655.html?browse=tc).

[28] For instance, the ISO/IEC standard ISO/IEC TR 24372:2021 (https://www.iso.org/standard/78508.html?browse=tc). The definition of AI in the draft AI Act is itself not based on international technical standards.

[29] E.g. the Guidelines for intelligent network analytics and diagnostics ITU-T E.475 (https://www.itu.int/rec/T-REC-E.475-202001-I/en), the Recommendation ITU-T Y.3174 on a Framework for data handling to enable machine
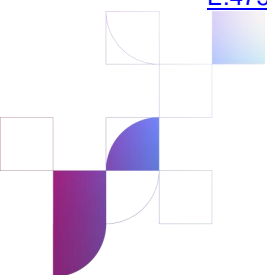
groups dedicated to particular topics, such as the Global Initiative on AI and Data Commons[30]. In the EU, the European Telecommunications Standards Institute (ETSI) is also carrying out extensive work related to AI in the telecommunications sector. On average, the survey respondents rated concerns about a lack of AI standards 3 on a scale of 1 (not important) to 5 (very important), while a respondent noted that the monitoring of the quality of the AI product/service on which they depend and which is supplied by a third party, presents a challenge for them, expressing the wish for third-party certification frameworks (such as ISO).

The AI ecosystem is shaped by a multitude of stakeholders and institutions. An overview of some of these actors is presented in ANNEX III. However, it is important to note that the activities of these stakeholders take place on a variety of levels. At the level of the EU, many of the activities are focused on the proposed AI Act and liability framework, and encompass stakeholders as diverse as data protection authorities, hardware and software providers, as well as standardisation bodies. At Member State level, AI strategies often shape the way businesses, research and Non-Governmental Organisations (NGOs) engage, and which topics are prioritised. Beyond the EU, the Council of Europe is working on a treaty with special regard to the human rights impacts of AI systems.

4. ARTIFICIAL INTELLIGENCE IN TELECOMMUNICATIONS

AI is a transversal technology that can be applied to a variety of use cases. In the telecommunications sector, processes are highly digitalised and digital data[31] are available for training and operating AI systems, thus facilitating the adoption of AI technologies. Furthermore, the scale of telecommunications networks and the complexity of managing networks as well as Customer Management Relationship incentivise the adoption of automated systems.

Mapping the impact of AI in the telecommunications sector requires detailed engagement with the involved actors, the datasets with which AI systems are trained, the hardware required to run AI systems, as well as an understanding of how telecommunications products and services integrating AI are being used by and affect consumers. With this report, BEREC seeks to provide an initial overview of the issues and some key applications areas in the telecommunications sector, which could provide a basis for deeper analysis in other work streams.

---

learning in future networks including IMT-2020 (https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14134), the Recommendation ITU-T Y.3116 on Traffic typization IMT-2020 management based on an artificial intelligence approach (https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14855), the Recommendation ITU-T Y.3178 on a Functional framework of artificial intelligence-base network service provisioning in future networks including IMT-2020 (https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14613) and others.

[30] https://www.itu.int/en/ITU-T/extcoop/ai-data-commons/Pages/default.aspx

[31] As long as this use is in line with the relevant data protection legislation (e.g. GDPR and E-Privacy Directive).

4.1. Benefits

AI technologies promise considerable savings in terms of costs and can help automate complex and/or repetitive processes. AI-based solutions are expected to assist telecommunication market players – network operators, equipment vendors and application providers – to provide personalized services to users and improve network quality, by extracting value from the analysis of massive amounts of data and applying improved prediction and decision-making processes. ECN/S providers collect highly valuable information both from their customers (e.g. traffic profile, geolocation, service use) and their networks (e.g. performance indicators, statistics, devices). These data sources could be efficiently exploited with AI techniques to optimize network operation, improve customer service or detect new business opportunities.

It is important to note that AI applications promise significant savings: in the case of virtual network topologies in connection with fixed networks, one application was calculated to save up to 20% in CapEX and 25% in OpEX (Mata et al., 2018, p. 51)[32]. The importance of cost savings was also highlighted by the survey respondents.

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

According to the survey conducted by BEREC, the top reasons for using AI systems were to remaining competitive by providing or adopting innovative solutions, to retain flexibility and agility (e.g. monitoring emerging problems and facilitating intervention), attaining security guarantees, and operations optimisation. The two least prioritised reasons were customisation and personalisation, and to consider AI systems as drivers of new business revenues (see Figure 4 When assessing whether to deploy a new AI solution, which benefits listed below do you pursue or prioritise? Average rating of survey respondents (n=7) in ANNEX II).

Another complementary source of information highlighting the value of AI for the telecommunications sector is the report recently published by Ericsson[33] based on a survey of more than 80 communications service providers (CSPs) around the world. In this report, a majority of providers believe that AI can result in IT and network OpEX reductions, as well as returns on investment between 5 and 10 percent. Most of them have AI deployment ongoing or planned, primarily focused on customer and service experience, security, and IT operations,

---

[32] The source does not specify if AI related costs (including cost of implementing and maintaining AI system, integration with legacy, qualified staff etc. …) were considered.

[33] https://www.ericsson.com/en/reports-and-papers/further-insights/ai-business-potential

and highlight the improved customer experience and network operations optimization as the main benefits of implementing AI.

4.2. Risks

Although AI technology is bringing benefits to the operation and service provision in telecommunications networks, a number of factors should be taken into consideration when evaluating the impact of AI systems in this field.

The risk described are based on the answers from the survey conducted by BEREC with market experts and focuses on those perceived as the most relevant. Nevertheless, BEREC notes that there are additional risks. Some examples include the potential lock-in of an operator to a given a supplier when becoming dependant on an AI model. Another example could be a vendor training its AI model using the data of a specific operator and reuse the same "trained" model for another operator. This allows gaining efficiencies in terms of time and (training) costs, however, raises questions around the ownership of the model, and, potentially, on privacy.

According to BEREC's survey, the risks and challenges of deploying AI systems related to undetected data bias, liability in case of error and access to reliable data were the highest areas of concern for the respondents (see Figure 5 Which of the following risks and challenges are you currently most wary of? Average rating by survey respondents (n=7, except for "Other competition risks", where n=6) in ANNEX II).

4.2.1. Availability of unbiased and reliable data

While not all computational approaches for AI systems require large amounts of data, access to the right, high-quality datasets is crucial for training and deploying AI systems. Low-quality data and in particular biased data will lead to low-quality and biased outputs, and may negatively impact not only the AI user, but also other stakeholders. The risk of biased data was one of the top concerns of the survey respondents (together with liability in case of error) in the context of AI deployment and/or development. At the same time, they highlighted the important role of the data ecosystem: two-thirds of the respondents agree that AI systems will drive the need for data governance to share data with partners or third parties, and that cloud providers will have a role in handling data from both the end-users and the CSPs (see **Error! Reference source not found.**).

AI systems demand significant resources during their development and their use. Besides the adequate data for training and testing AI systems, qualified personnel is also needed. The computing resources required for the deployment of AI systems are also not negligible. Survey respondents rated concerns around access to data rather highly, while the shortage of technical expertise was on average not a dominant concern. Asymmetries in access to these resources may, in turn, lead to a gap between smaller and larger telecommunications

providers. However, competition risks associated with such an unequal access to resources counted amongst the two risks that received the lowest ratings by survey respondents.

In the telecommunications sector, the digital divide remains an important issue that may be exacerbated, if the network enhancements driven by AI technology are only applied to urban deployments. It is possible that less data is available in rural areas compared to urban areas, which can lead to different outcomes for rural vs urban users. This is reflected in the concerns expressed by the survey respondents about risks created by the uncertainty about the reliability of AI systems due to the scenarios considered during their training. The respondents rated this risk at an average of 3.6 (out of 5, with 5 meaning "high importance of this risk"). Moreover, the lack of access to data and/or AI systems for local or regional initiatives deploying networks in rural areas could lead to a disadvantage for these actors in comparison to well-established telecommunications and digital providers.

4.2.2. Liability in case of error

The deployment of AI based solutions in networks involves various players of the value chain. Besides network operators and vendor suppliers, AI algorithm/application providers and external suppliers of data used by AI systems may also contribute, jointly with integrators specialized in providing customized end-to-end solutions. Given the heterogeneous nature of the ecosystem and automation of AI systems, there is uncertainty about the accountability and liability of each actor in the case of unexpected or mistaken outcomes. Although service-level agreements (SLA) agreements can include provisions in this regard, the accountability of who is responsible for the decisions taken by AI systems may be unclear. The importance of liability in case of error was also recognized by the survey respondents, ranking this risk second place.

4.2.3. 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.

AI *explainability* relates to the means that allow users to understand and trust AI outputs. When involving decisions or profiling involving individuals, the provisions in art 22 of the GDPR establish the data subject's right to obtain human intervention and an explanation of the decision reached (Rec 71 GDPR). There are several technical frameworks for Explainable AI and enhance transparency such as What-if Tool (tensor flow), LIME, DeepLIFT, Shapley etc.

Survey respondents rated concerns about the opacity of AI systems with an average of 3.4 (being 5 the highest rate). Several technical measures to ensure explainability and to increase

trust in the decision making have been implemented by the responding stakeholders, such as logging and reporting systems, levels of explanation tailored to stakeholder groups, detailed documentation and triggers with thresholds to identify critical deviations.

4.2.4. Privacy

Highly relevant in the context of data-sharing are also privacy aspects. In particular, whether data used by AI systems is managed with appropriate safeguards to prevent the monitoring of individual users. Survey respondents mentioned that they are guided by the provisions of the GDPR and the regulatory framework for telecommunications (European Electronic Communications Code -EECC- and ePrivacy Directive) and develop processes to ensure that data access and usage are compliant with the legal requirements, both in the interests of privacy protection and to ensure business confidentiality. A respondent noted that business confidentiality is ensured through non-disclosure agreements but added that these were insufficient to protect their business strategy.

Data privacy, security and AI integration are the main challenges faced by CSPs when implementing AI solutions mentioned in the Ericsson report. The data privacy concerns found in the report appear to stem from the reluctance to share data between different parts of the same organization.

4.2.5. Security

Cybersecurity research remains an important field for AI, in particular for detecting and preventing cyberattacks. At the same time, appropriate measures need to be taken to ensure that these AI systems for cybersecurity are robust and reliable. AI systems deployed by telecommunications providers themselves must also be appropriately secured in order to prevent malicious attacks with potentially wide-reaching impacts. As many AI algorithms are not deterministic, AI systems can be abused. They are vulnerable to automated adversarial attacks often led by other AI systems, where data is manipulated in order to cheat the model and result in wrong outcomes.[34] Another example of security risk would be the unauthorized access to data stemming from a lack of control when data is pooled across the company.[35] Concerns about security threats to AI-based systems and associated data came in fourth place when comparing the average ratings provided by survey respondents.

Securing AI is one of the areas on which the EU Agency for Cybersecurity (ENISA) is also working and a specific threat landscape report that is sector-agnostic was published[36]. As part

---

[34] Van der Vorst et al., 2020: Managing AI use in telecom infrastructures. Advice to the supervisory body on establishing risk-based AI supervision.
[35] https://www.ericsson.com/en/reports-and-papers/further-insights/ai-business-potential
[36] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

of the conclusions, the development of an AI toolbox is promoted, with specific mitigation measures for the AI threats identified in the landscape based on risk assessments.

4.3. Other challenges

In response to BEREC's survey, the market experts included other challenges or anticipated impacts that should be further taken into consideration with the increase in the uptake of AI solutions (see Figure 6 Do you anticipate any of the following changes to the CSPs' network architecture as a result of an increase in the uptake of AI solutions? in ANNEX II). The proliferation of the use of AI systems may also have an impact on the requirements for and the design of telecommunications networks. AI systems based on cloud instances may require low latency to function appropriately and could lead to decentralisation in terms of data centre distribution. Using AI systems within telecommunications networks may require new hardware,[37] such as processing chips. In particular, in the context of OpenRAN, issues could arise with the integration of different hardware and software components (the challenge of integrating AI in legacy systems was also mentioned by one of the survey respondents). AI systems are often deployed together with IoT infrastructure, such as sensors, and the large number of devices connected to one system may affect the network load in case of malfunctioning.

Five out of six survey respondents agreed that AI systems would drive the need for open and disaggregated architectures, while two-thirds supported the statement that "*AI solutions will drive further the need for Multi-Access Edge Computing and the uptake of new chipsets that can manage significant data at the edge of the network will increase*". The location of data processing is also a crucial question: whether at the edge, favoured for mobile, or in the centre, it also impacts the potential role of third parties in the data ecosystem. Conversely, the *softwarisation* and virtualisation of networks were mentioned by survey respondents as strong use cases for AI in the telecommunications sector.

AI systems can contribute to the efficient management of telecommunications networks and thus lower their environmental impact. The BEREC Report '*Sustainability Assessing BEREC's contribution to limiting the impact of the digital sector on the environment*' highlighted the potential of AI contributing to the enabling effect of ICT to bring about positive environmental impact in the section on stakeholder initiatives: an OECD Working Party on Communication Infrastructures and Services Policy (WPCISP) report[38] on future trends states that the use of AI systems could be considered when assessing the environmental impact of communications networks. At the same time, the development and deployment of AI systems is itself very resource intensive if not properly managed. This might impact the telecommunications sector

---

[37] The hardware requirements of AI were also highlighted as a concern by one of the respondents.
[38] '*Broadband Networks of the Future*', https://www.oecd-ilibrary.org/science-and-technology/broadband-networks-of-the-future_755e2d0c-en

through increased carbon emissions, even if those systems are not deployed by providers themselves, like in the case of cloud-based as well as on-device AI applications.[39]

AI systems are often not deployed by themselves, but integrated into larger systems comprised of other hardware, software, or linked to other AI systems. For this reason, it is vital that AI systems are appropriately tested together with the other components of the system before deployment, and that the interactions between different AI systems can be appropriately traced. These measures enable swift interventions to solve possible malfunctions, which could lead to wide-reaching errors or disruptions. To mitigate these risks, the survey respondents mentioned developing process management systems to analyse and classify automated systems, including internal auditing, defining the impact, advantages and challenges during the early phases of development, and minimising the risk of failures by design, as well as ensuring sufficient human oversight and intervention capacities. Furthermore, the challenges also include designing the connections between AI systems in a hierarchical manner and building in alert triggers to notify network and security operations centres.

Regarding the existing regulatory barriers for the adoption of AI by telecommunications providers, the majority of the survey respondents were adamant that use cases in the context of telecommunications should not be considered high-risk in the context of the AI Act, and that light-touch approaches, like guidelines or voluntary frameworks, are better suited. In particular, the necessity for regulators to develop a holistic view of the use of AI in telecommunications as well as the risks of overlapping legal frameworks and competences were stressed. The survey respondents currently do not see any regulatory impediments to the deployment of AI in the telecommunications sector, and one respondent is of the view that the EECC provides the basis for the use of AI in the telecommunications sector.

4.3.1. Future trends

According to the survey respondents, the adoption of AI in the operational procedures of every CSP will become a norm approximately in the next six to ten years. The scale of the required changes in the processes and architectures, the need for more mature standards, challenges related to legacy systems and the difficulties of developing fully-fledged digital twin simulations of the changes triggered by AI in the networks were mentioned as drawing out this period of adoption.

As suggested by the results of the desk research and some market players, future trends related to AI systems in the telecommunications sector may include the changes in networks driven or enabled by AI systems, in particular those technologies based on cloud networking[40],

---

[39] Gibney (2022): How to shrink AI's ballooning carbon footprint. https://www.nature.com/articles/d41586-022-01983-7
[40] Xavier & Kantarci, 2018: https://link.springer.com/article/10.1007/s12243-018-0629-4

such as network function virtualisation (NFV)[41] and software-defined networking (SDN) with major impacts on the configuration and architectural design of networks.[42] The softwarization of networks driven by SDN and NFV technologies, allows faster and easier network deployment, configuration, and update of network functions, providing programmable control and resource management functionality that are essential for implementing new enhanced features like network slicing in mobile networks. Network slicing divides the physical network infrastructure into multiple virtual networks to support diverse business services, enterprise applications and use cases, and represents a paradigm shift in the way 5G networks and beyond (6G) will be designed and operated. Incorporating AI-based solutions will potentially improve the network management automation and performance optimization of large-scale systems[43].

Further research also points towards the development of on-chip network applications, the joint operation of networks and computing resources, as well as the use of traffic data together with declarative intents for network orchestration.[42] With AI systems, the role of networks could also shift, for instance in cases where networks (e.g. fibre optics networks) or routers are used as sensors for AI applications[44] or for managing responses in case of disasters.[45] This research shows that AI systems could potentially impact what networks (can) do as well as how networks function. In the case of intent-based networking, for instance, instead of relying on engineers to lay out the path along which a network should operate, a high-level goal is provided and an orchestration system identifies the best process and executes it.

---

[41] Zheng et al., 2021: https://link.springer.com/article/10.1007/s12243-020-00772-5
[42] Mata et al., 2018: https://www.sciencedirect.com/science/article/pii/S157342771730231X
[43] Ssengonzi et al., 2022: https://www.sciencedirect.com/science/article/pii/S2590005622000133
[44] Muaaz et al., 2022: https://link.springer.com/article/10.1007/s12243-021-00865-9
[45] Tei et al., 2021: https://link.springer.com/article/10.1007/s12243-021-00847-x

Network Analytics at its Core

Analytics keep network operations aligned with original business intent throughout the service lifecycle.
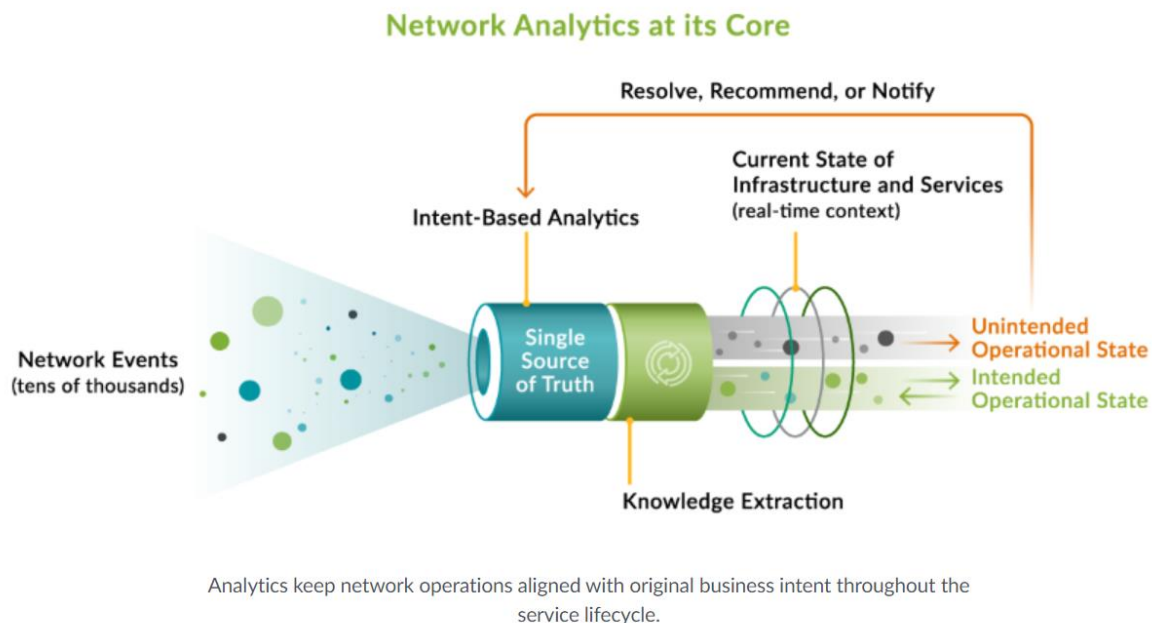
Figure 1 Visualisation of declarative intent-based network orchestration[46]

The exponential growth of mobile applications and, services as well as the development of new use cases, such as customized solutions based on 5G, will challenge the management of fixed and mobile network infrastructures, increasing the complexity of orchestration of different segments involved in the end-to-end network service delivery. The Zero-touch Network and Service Management (ZSM) concept -standardized by ETSI- has emerged to automatically orchestrate and manage network resources while assuring the Quality of Experience (QoE) demanded by users. The target is to enable largely autonomous networks driven by high-level policies and rules, that will be capable of self-configuration, self-monitoring, self-healing and self-optimization without human intervention. AI technology is being adopted as one of the key enablers to bring intelligent decision making to the ZSM network management framework, where operations will be data-driven, predictive and proactive, enabling business agility[47].

Besides these aspects pertaining to material infrastructure, other use cases may be implemented, for instance the targeting of subscribers to increase revenue (e.g. nudging subscribers to use all of their data allowance to incentivise them to buy top-ups) [48]. Another example would be the use of AI for marketing purposes (e.g. churn analysis for customer retention in the CRM area) in order to continuously follow and predict the next purchasing

---

[46] https://www.juniper.net/us/en/research-topics/what-is-intent-based-networking.html
[47] Gallego-Madrid et al, 2022: https://www.sciencedirect.com/science/article/pii/S2352864821000614
[48] Faulkner, 2015: https://www.proquest.com/docview/1898827114

decisions of the target consumers[49]. While such endeavours may sound far away, the development of explainability frameworks for such use cases shows that such use cases may not be as exotic as they seem at first glance.[50] Whether and how such practices impact user's rights and to what extent additional transparency requirements may be needed is beyond the main topic of research here but could be explored further in the future. This potential future work on the impact of AI on the end-user could take into account that customer management were signalled by several respondents as a key area for AI systems implementation in the sector.

In the view of the survey respondents, a series of topics will become important in the coming years, which partially revolve around the legal framework for AI (AI Act implementation, deep learning explainability), AI standards for deployment and operation at scale, and ethics (the latter being considered a hot topic for policy makers). From the point of view of telecommunications network development and management, zero touch operations, robot process automation, application-driven quality of service (QoS) (with networks and applications co-deciding how to handle individual packets, flows and services) as well as multi-topic streaming aggregation were considered to be future issues. Finally, the issue of data for the development of AI systems (including infrastructure documentation, the use of critical and non-critical infrastructure, as well as the integrity of infrastructure data) was noted as relevant for the future.

5. SELECTED ARTIFICIAL INTELLIGENCE USE CASE AREAS

The use cases described in this report were preselected by the NRAs considering the ones deemed to be the most relevant according to their remit. This chapter is therefore not meant to be exhaustive, but rather illustrative, in order to provide an overview of the variety of applications for AI systems in the telecommunications sector within these areas selected by the responding NRAs. Other AI systems mentioned by survey respondents include the support of sustainability measures (e.g. by reducing the electricity consumption of electronic communications networks and services), customer journey applications (e.g. related to customer relationship management), optical fulfilment and assurance, predictive maintenance, end-to-end slice management and location-based service provisioning. During the public consultation stakeholders signalled additional AI use cases for the provision of ECN/S. Those include improving reliability, allowing the return of lost coverage to subscribers more efficiently as well as improving the performance and efficiency of networks by performing various functions such as network optimization, predictive maintenance, traffic management, self-healing networks and resource allocation.

---

[49] Savica Dimitrieska et al. (2018) http://ep.swu.bg/images/pdfarticles/2018/ARTIFICIAL_INTELLIGENCE_AND_MARKETING.pdf
[50] Peterson & Daramola, 2020: https://link.springer.com/chapter/10.1007/978-3-030-58817-5_35

5.1. Network and Capacity Planning and Upgrades

5.1.1. Description of the use case

Network and capacity planning and upgrades are activities within the telecommunications sector that require massive resources, both financial as well as material. This is further complicated by the fact that networks are designed to handle predicted future usage, as they are built to last for decades. At the same time, the speed of development, especially in the mobile sector, requires frequent modifications of the networks (roll-out, upgrade or migration), which means that network planning and network upgrades are continuous activities. While much of the literature focuses on the usage of AI applications in mobile networks, AI applications also exist for fixed networks.

Precisely because network planning and upgrading is such a resource-intensive and continuous activity, AI applications that reduce the cost of deployment (financial or material) are highly attractive for telecommunications providers. This was also noted by survey respondents.

For telecommunications providers it is important to forecast the usage of a network and plan the infrastructure accordingly. Network capacity planning aims to provide such predictions and optimise the deployment or management of infrastructure to cope with the predicted usage. This can also mean that networks can be used for a longer time: for instance, in the case of fibre optics networks, space-division-multiplexing using AI models can increase the capacity of a single fibre and prolong the lifetime of the existing infrastructure, delaying the need for deployment of new fibre optics cables.[51]

5.1.2. Related applications

AI systems to facilitate network and capacity planning and upgrades can be applied to both fixed and mobile networks. They may, for instance, predict priority sites, identify optimal locations or routes for deployment, maximise energy efficiency, minimise the required number of transmitters or base stations, or design new network architectures. For instance, Chu et al. (2021) developed a deep learning model capable of recognising possible antenna mounting points in the context of fixed wireless access deployment to aid developing coverage estimation reports.

As stated by the survey respondents, the applications currently implemented include AI systems for traffic prediction, network softwarisation and virtualisation, route optimisation and cable upgrade optimisation or planning 5G networks.[52]

---

[51] Jatoba-Neto et al., 2018: https://opg.optica.org/jocn/abstract.cfm?uri=jocn-10-12-991
[52] The example on planning 5G networks was focused mostly on eMBB and FWA services in the planning stage.

Route optimisation and cable upgrade optimisation include applications, such as data-assisted decision for copper reconstruction, or automated optimal routing and migrating decision-making for in-house fibre routes.

Traffic and capacity demand prediction techniques allow simulating several possible scenarios and adapting the network design and investments to ensure the QoS and network performance required by the customers. One such application identified through desk research would be the simulation of the impact of different forms of switching solutions.[53] In the case of network softwarisation and virtualisation, AI systems are considered to be crucial enablers, helping to bring about the change to dynamic network operations due to their capacity for real-time processing of large datasets, and for swiftly executing tasks in an automated manner. Another example is the use of AI in optimization of Content Delivery Network (CDN). This allows to proactively identifying network traffic patterns and appropriately respond to communications traffic demand, so that the users can experience an improved content performance. That is, AI helps in this case to better address the problem of which edge server will the CDN direct the user request to[54]

Challenges for the development of AI systems for network planning and upgrade purposes include the lack of access to sufficient amounts of reliable data and the lack of computational capacity to train and deploy these models. These challenges can be resolved in a variety of ways, for instance by drawing on specific techniques, e.g. generative adversarial networks,[55] or by combining data-driven and model-driven approaches. With machine learning approaches, the issues of data corruption are equally important for both the training and the deployment phases. The respondents to the survey also noted that the need to access data from different sources and in different formats remains a challenge.

The survey respondents indicated that they plan to analyse traffic and performance data to plan network capacities with mitigation and automation hubs, to employ AI systems for predictive maintenance, to automate data processing for network capacity planning, and to optimise 4G networks. Regarding predictive maintenance, one survey respondent noted that predictive models help to anticipate potential issues in the network related to network service degradation or potential failures related to several aspects (such as obsolescence and breakdown of equipment, load problems, energy use optimisation, etc.) that can help to establish an action plan to mitigate the impact on customers.

One detailed use case provided in the context of the survey concerns the use of AI systems for capacity planning to reduce electricity consumption. Based on historical data, capacity for mobile sites may be reduced or shut off in times when the load is predicted to be lower at certain times (nights, weekends) or in certain areas (summer-house areas), while the connectivity layer remains functional. If traffic increases, the additional capacity layers may be

---

[53] Jatoba-Neto et al., 2018: https://opg.optica.org/jocn/abstract.cfm?uri=jocn-10-12-991
[54] https://www.medianova.com/en-blog/how-artificial-intelligence-and-machine-learning-are-changing-cdns/)
[55] See Annex I AI techniques (Game Theory).

turned on again. Through such measures, power savings by a factor of about 2.8 are estimated without any network degradation.[56]

Another concrete use case provided by a market expert concerns mobile networks congestion mitigation. In particular, the application of AI to mobility load balancing in the radio network, with the aim of optimally offloading traffic from congested cells to neighbouring cells with reduced load.

In the context of capacity planning, some of the identified challenges included dealing with the trade-offs of different types of implementation and the associated investment costs.[51]

5.1.3. Conclusions and regulatory implications

Both the desk research as well as the survey responses indicate that there are many potential areas, where AI systems could be developed and applied to support activities related to network and capacity planning and upgrades. Stakeholders foresee that AI will play a major role in this domain in telecoms in the future. On the regulatory side, NRAs consider it highly relevant for BEREC to closely follow the technological advances that AI may bring to network planning and monitoring, and to be aware of the possible implications to the strategic objectives on connectivity and open and sustainable markets. Some of the issues that might arise are presented here in an illustrative way.

Many governments fund broadband deployment (fixed/mobile). Using AI tools could potentially help to reduce the cost of deployment in different scenarios, such as the case of selecting the best location points to install cells (in particular, small cells deployment), or the most adequate routes for fibre deployment. Whether these AI systems could be shared by operators and municipalities using an AI commons approach like the one proposed by the ITU[57], would merit for further investigation.

The potential savings, which could be achieved, particularly in the context of network planning and upgrades, show that operators have an incentive to use AI models in their networks. Given that stakeholders other than traditional telecommunications providers may be involved in network roll-out, the question arises whether alternative network providers (e.g. municipalities in the case of fibre optics networks roll-out) have access to the required data and robust models to achieve similar savings. Finally, the different levels of data availability for particular regions and a focus on urban instead of rural areas[58] may lead to unequal levels of maturity or application of AI models.

Transparency about the weights and trade-offs included in AI algorithms at network levels may prove to be necessary, for instance if MVNOs file complaints about being affected negatively by algorithms deployed by their host MNOs to manage capacity. In such cases, NRAs and

---

[56] Use case submitted by a telecommunications provider.
[57] https://www.itu.int/en/ITU-T/extcoop/ai-data-commons/Pages/default.aspx
[58] E.g. Patri et al., 2019: https://opg.optica.org/jocn/abstract.cfm?uri=jocn-11-7-371

telecommunications providers may need to find common approaches for evaluating the impact of AI systems and ensuring explain ability.

As the example of using AI systems to reduce the electricity consumption of mobile networks shows, there can be significant benefits from employing AI systems for sustainability measures. However, some users may experience delays in receiving the full capacity and may not be aware of such measures. This issue in particular may be exacerbated, if users in rural areas are affected differently by such measures than users in urban areas. Finally, such AI systems may not be fully in the control of telecommunications providers, as they may be embedded in the network hardware.

5.2. Channel Modelling, Prediction and Propagation

5.2.1. Description of the use case

Channel modelling is one of the most important research topics for wireless communications, 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 the network planning and optimization. Channel models are based on data collected during measurement campaigns in representative scenarios. The usage of multiple-input multiple-output (MIMO) antennas, beamforming and millimetre waves in the new generations of wireless communication networks creates the need for developing new channel models, possibly with the help of AI algorithms.

The available literature provides descriptions of various models developed in order to predict the channel usage, some of them being based on neural networks. Jiang and Schotten (2016)[59] consider that the challenge in the channel prediction is the parameters estimation. This estimation itself is based on the current and past channel impulse responses. In order to develop the model, they have used recurrent neural networks (RNN), a class of machine learning that uses both training data and its memory of past states, while the phases are the same as in any AI technique (training and inference). The results have shown the effectiveness of the RNN against the outdated channel state information, while having a moderate computational complexity. The predictor can be applied in frequency-flat and frequency-selective MIMO fading channels.

---

[59] 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

Ding and Hirose (2014)[60] proposed prediction methods based on complex-valued neural networks. These include a combination of time and frequency, and reduced learning costs.

Rappaport et al. (2017)[61] mention the importance of channel models for simulating propagation in "a reproductible and cost-effective way" and for the design and comparison of radio air interfaces and system deployment. The overview of different models and different standards has shown that the propagation models are vital for the improvement of the mobile industry.

5.2.2. Related applications

The results of the survey within BEREC point towards a high interest in the subject, most of the responses being in the higher range of the scale. The answers for the entire category of planning and monitoring are justified, in principle taking into account the strategic objective related to promoting connectivity. Some respondents mentioned that some of the applications are already related to the regulatory activities, one pointing out specifically channel modelling.

Out of the five answers received from the industry regarding the deployment or the plans to deploy AI applications for channel modelling, prediction and propagation, three were positive, therefore indicating an interest in this area. 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. It was also pointed out that channel modelling is mostly provided by vendors of mobile radio network equipment.

The answers are the more relevant in the context in which improved prediction and decision-making models and cost reduction are amongst the higher ranked perceived benefits of AI solutions deployment.

At the same time, the respondent who indicated that the applications are mostly provided by vendors mentioned as a specific risk/challenge the dependency on the quality of the delivered product and the quality control, which could be mitigated by a certification by a third party (e.g. ISO).

5.2.3. Conclusions and regulatory implications

Both the regulators and the stakeholders consider channel modelling an important aspect for network monitoring. For the NRAs, this is relevant especially in the context of promoting connectivity as well for their own activities, and for the stakeholders in relation to the benefits in terms of cost reduction and QoS.

---

[60] https://ieeexplore.ieee.org/abstract/document/6755477/authors#authors
[61] https://ieeexplore.ieee.org/abstract/document/7999294

5.3. Dynamic Spectrum Sharing

5.3.1. Description of the use case

Radio spectrum is a fundamental economic resource in the electronic communications sector, and its importance has increased in recent years due to the massive expansion of the amount of traffic of wireless services[62]. Given that, by its nature, spectrum is a scarce resource, it is crucial to have an adequate management in order to ensure that it is efficiently used, and that it maximizes all the value that it can deliver. Recital 107 of the EECC states that *radio spectrum is a scarce public resource with an important public and market value. It is an essential input for radio-based electronic communications networks and services and, insofar as it relates to such networks and services, should therefore be efficiently allocated and assigned by national regulatory or other competent authorities in accordance with harmonised objectives and principles governing their action as well as to objective, transparent and non-discriminatory criteria, taking into account the democratic, social, linguistic and cultural interests related to the use of radio spectrum*.

The classical spectrum management, based on a fixed spectrum allocation policy, leads to inefficient usage due to underutilization. For instance, according to different estimates for several countries, only a fraction of the allocated radio spectrum is actually used, in some cases with very low occupancy rates[63] [64].Thus, a dynamic approach to spectrum management could increase efficiency[65].

Under its 5G Action Plan, the EC wants to *boost EU efforts for the deployment of 5G infrastructures and services across Europe*. Jointly with the EECC, and among other things, it wants to ensure the *timely assignment and availability of radio spectrum*[66]. The EC has identified and quantified the spectrum requirements that will be needed to comply with its

---

[62] According to some estimates, global traffic per year will reach 4.8 zettabtyes at the end of 2022, while global internet users will reach 4.8 billion and 28.5 billion devices will be connected to the network https://www.globenewswire.com/en/news-release/2018/11/27/1657381/0/en/Cisco-Predicts-More-IP-Traffic-in-the-Next-Five-Years-Than-in-the-History-of-the-Internet.html

[63] The spectrum indoor occupancy rate in Germany for the band 20 MHz-3 GHz is around 32%, whereas occupancy for frequency bands between 3-6 GHz is very low. See M. Wellens, J. Wu, P. Mahonen, Evaluation of spectrum occupancy in indoor and outdoor scenario in the context of cognitive radio https://ieeexplore.ieee.org/document/4549835. Similarly, spectrum occupancy in Barcelona and Poznan is between 20%-30%.

[64] In the US spectrum average occupancy rates over 3 GHz are below 20%. See T. Taher, R. Bacchus, K. Zdunek, D. Roberson, Long-term spectral occupancy findings in Chicago https://ieeexplore.ieee.org/abstract/document/5936195

[65] Recital 124 of the EECC states that *network infrastructure sharing, and in some instances radio spectrum sharing, can allow for a more effective and efficient use of radio spectrum and ensure the rapid deployment of networks, especially in less densely populated areas. Whereas establishing the conditions to be attached to rights of use for radio spectrum, competent authorities should also consider authorising forms of sharing or coordination between undertakings with a view of ensuring effective and efficient use of radio spectrum or compliance with coverage obligations.*

[66] 5G Action Plan https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan

objectives under different sharing scenarios. In the no-sharing scenario, around 76 GHz will be needed to meet users' needs, whilst in a full-sharing scenario 19 GHz will suffice, which would imply a drastic reduction in spectrum requirements. [67]

5.3.2. Related applications

ML techniques are used to optimise the flow of data between base stations and mobile networks. A well-functioning network needs different parameters that define the capacity and efficiency of radio spectrum, such as distance to users and connected users. Those parameters can be improved by AI.

The Citizens Broadband Radio Service (CBRS)[68] allows for more dynamic mapping of spectrum, partially solving some of the underutilization problems. Under this system, several certified automatic platforms (Spectrum Access Systems, SAS) are authorized to dynamically award permissions to devices (CBSD) to use assigned channels based on geo-location information, real-time information from a sensing network (Environmental Sensing Capability, ESC) and database of awarded priority licenses.[69]

According to Ying-Chang Liang (2020)[70], the most relevant benefits of applying AI techniques to dynamic spectrum management are autonomous feature extraction (AFE), because AI schemes can automatically extract features from data. Further benefits relate to robustness to the dynamic environment (RDE), which implies that, thanks to the data-driven approach and continuous learning, spectrum management is not affected by changes in the radio environment, and decentralized implementation (DI), which means that the central controller is no longer needed and each device can autonomously obtain its required spectrum resource; and reduced complexity (RC).

Following Ying-Chang Liang (2020), there are three important recent applications of ML techniques that could contribute to a better spectrum management and partially solve issues regarding accuracy, performance, complexity and underutilization.

- **Machine learning for spectrum sensing**

Spectrum sensing is a primary technology for cognitive radio. Its purpose is to avoid interference with licensed users and assist them to detect the status of the spectrum and its

---

[67] Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe https://op.europa.eu/en/publication-detail/-/publication/2baf523f-edcc-11e6-ad7c-01aa75ed71a1/language-en

[68] Citizens Broadband Radio Service (CBRS) is a 150 MHz wide broadcast band of the 3.5 GHz band (3550 MHz to 3700 MHz) in the United States. In 2017, the US Federal Communications Commission (FCC) completed a process which began in 2012 to establish rules for commercial use of this band, while reserving parts of the band for the US Federal Government to limit interference with US Navy radar systems and aircraft communications

[70] Y.C, Liang. Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence. Springer Open (2020) https://link.springer.com/book/10.1007/978-981-15-0776-2.

availability[71]. With the aim of increasing the accuracy of spectrum sensing, several spectrum sensing algorithms have been developed: estimator-correlator detector, the semi-blind energy detector ant the blindly combined energy detection.

Recent evidence suggests that methods based on deep learning techniques perform better than traditional spectrum sensing methods (i.e., maximum-minimum eigenvalue ratio-based method and frequency domain entropy-based method)[72].

- **Machine learning for signal classification**

The ability to classify signals is a fundamental task that has many different applications, and in an age of mass wireless communication, it is more important than ever to identify and classify electromagnetic signals with fast and accurate tools. In recent years, deep learning techniques are being applied to detect radiofrequency signals. They can identify the presence of a signal without requiring full protocol information, and can also be used to detect non-communication waveforms, like radar-signals[73]. In order to achieve better performance with low computational complexity, ML techniques have been introduced in solving classification problems and have shown superior performances than conventional methods.

- **Deep reinforcement learning for dynamic spectrum access**

Conventional dynamic spectrum access is based on centralized control node that is responsible for the spectrum allocation to users. Prior to making decisions, this centralized node needs to collect information across the network. For instance, information regarding the users' position and base stations. This information is complex and disperse. The difficulties of obtaining this information hinders the appropriate functioning of the network when there is a sufficient large number of users, which, ultimately, could yield to poor performance.

To solve this problem, reinforcement learning can be used. This technique consists of a learning process, where an agent can periodically make decisions, observe the results, and then automatically adjust its strategy to achieve the optimal policy[74]. However, there are also limitations, mainly referred to the amount of time that is necessary to reach a solution since it requires gaining knowledge of an entire system. Fortunately, Deep Reinforcement Learning (DRL) can overcome those limitations and improve the learning speed and the performance of algorithms. Hence, it enables centralized control nodes to solve non-convex and complex problems, to achieve optimal solutions without complete and accurate network information.

---

[71] Ian F. Akyildiz, Brandon F. Lo, Ravikumar Balakrishnan, Cooperative spectrum sensing in cognitive radio networks: A survey, Physical Communication, Volume 4, Issue 1, 2011, Pages 40-62, ISSN 1874-4907 https://www.sciencedirect.com/science/article/abs/pii/S187449071000039X

[72] S. Zheng, S. Chen, P. Qi, Huaji Zhou, X. Yang. Spectrum Sensing Based on Deep Learning Classification for Cognitive Radios. arXiv. 2019 https://arxiv.org/abs/1909.06020.

[73] Elyousseph, Hilal, and Majid L. Altamimi. "Deep learning radio frequency signal classification with hybrid images." *2021 IEEE International Conference on Signal and Image Processing Applications (ICSIPA).* IEEE, 2021.

[74] N.C. Luong, D.T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, D.I. Kim, Applications of deep reinforcement learning in communications and networking: a survey. IEEE Commun. Surv, Tutor. (2019)

5.3.3. Conclusions and regulatory implications

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 need multidisciplinary approach from different fields, such as machine learning, computer networking, information theory or signal processing. In recent years, there is a trend for a more flexible approach to spectrum regulation. For instance, in November 2008 the Federal Communications Commission (FCC) presented a document with proposals for removing unnecessary regulations that restricted the development of spectrum markets[75]. In the UK, the Office of Communications (OFCOM) proposed to allow licence exempt use of interleaved spectrum for cognitive devices[76]. That being said, there are already several market practices aimed at increasing efficient use through spectrum sharing approaches. For instance, the DSS feature is in use for 4G/5G band sharing to provide both services in the same frequency band based on the actual traffic demand. Other market practices that try to encourage spectrum sharing are network sharing agreements between operators, roaming agreements and network slicing.

Reviewed evidence in this section shows that there exists room for improvement in spectrum management, and AI techniques are a well-suited technology to foster this new dynamic approach that will be needed to satisfy future demand. These AI-based Dynamic Spectrum Management mechanisms have shown to achieve better performance and robustness than conventional schemes. However, there are also some challenges that must be addressed, both technologically and regulatory. To maximize the value of these algorithms, regulators should shift from a fixed to dynamic and more flexible approach.

5.4. Quality of Service Optimization and Traffic Classification

5.4.1. Description of the use case

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 videocalls and streaming services. With the adoption of 5G, the demand for real-time communication, for example for virtual reality (VR)-applications, increases. This makes the tool of QoS optimisation essential for internet service providers (ISPs), if they want to continue to provide end-users with the level of service they require.

The responses received from stakeholders notes that AI is applied to achieve a better QoS / QoE typically in the following applications (not exhaustive list): RAN congestion prediction,

---

[75] Notice of proposed rulemaking. Report ETDocketNo. 00-402, Federal Communications Commission (2000)
[76] Digital dividend review: a statement on our approach to awarding the digital dividend. Technical report, Office of Communications (2007).

network traffic forecasting, network traffic classification and routing, congestion control, predictive maintenance, fault management and security mitigation solutions.

ISPs can employ various QoS techniques in their network, such as classification, marking, policing, shaping, congestion avoidance and queuing. These methods rely on a number of measurements including latency, error rate or jitter. AI can be used to optimize QoS by, for example, collectively analysing a number of these parameters, such as those concerning the radio environment, quality of the perceived signal or the number of packets lost.

All QoS techniques are particularly well suited for the adoption of AI and can benefit from the automation of processes, because they can easily be processed and analysed in all layers of the network from its control system. The adoption of AI can enhance QoS and avoid over-provisioning of services, hence allowing a more efficient use of the network resources. The next section further zooms in on the adoption of AI in traffic classification, policing and queuing, as these techniques are a key part of the QoS mechanisms.

5.4.2. Related applications

With an increasing number of applications and services being transmitted and OTT operators sharing the same network, traffic management becomes more sophisticated. Mature technology currently implemented in networks lacks capacity to accommodate unpredicted overloads of a specific traffic type. Instead, certain ML techniques can be used to achieve optimal traffic management by influencing routing or traffic engineering policies, avoiding traffic loss or oversizing for bulk loads of traffic. Nonetheless, any traffic management measures have to respect the provisions of the Open Internet Regulation (OIR).

Network slicing is one of the most important techniques to guarantee QoS in 5G networks, meaning it is an architecture that allows the division of the network in multiplexed virtualized and independent network sharing the same physical infrastructure. AI may help creating each slice end-to-end isolated and designed to meet the requirements needed for a specific application. In Balmer et al. (2020), ISPs indicated that they also see a role for equipment manufacturers in this area. For example, equipment providers increasingly provide 5G cells, which use AI to optimise traffic management.[77]

5.4.3. Conclusions and regulatory implications

NRA's have identified AI use cases in QoS and traffic classification as an area of special interest. The OIR and the BEREC Guidelines on the implementation of this regulation (BEREC OI Guidelines)[78] are the most relevant regulatory instruments for QoS and traffic management.

---

[77] Balmer, R.E., Levin, S.L., and Schmidt, S. (2020) "Artificial Intelligence Applications in Telecommunications and other network industries" *Telecommunications Policy 44(6)*, p. 6.
[78] BEREC Guidelines on the Implementation of the Open Internet Regulation, BoR (22) 81, https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0.

This section shortly outlines the relevant provisions and indicate their relationship with the employment of AI in these use cases.

The OIR lays down rules for ISPs when they provide internet access services to end-users. Article 3(3) of the Regulation states that all traffic is to be treated equally, irrespective of the sender or receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. Equal treatment also means no discrimination of restriction or interference with the traffic. This provision, however, does not prevent ISPs from implementing *reasonable* traffic management measures. In order to be considered to be "reasonable", traffic management would have to be based on objectively different technical Quality of Service (QoS) requirements of specific categories of traffic. Such measures are not allowed to monitor specific content (i.e. anything from the transport layer protocol payload).

Additionally, the Regulation contains rules for the provision of services other than internet access services, which are optimized for specific content, applications or services, also known as specialised services. Article 3(5) specifies that ISPs may only offer such services, if they meet the necessity requirement, and if the network capacity is sufficient. These rules apply regardless of the use of AI in these services.

Jull and Schmidt (2009) found that a principle-based approach is superior to prescriptive rules "in situations where technology can quickly overtake any such short-term prescriptive rules".[79] Balmer et al. (2020) indicated that for AI in telecommunication services, it will generally be sufficient to regulate outcomes, such as reliability, or to regulate through principles such as reasonability, necessity and non-discrimination.[80] Considering that the OIR and the BEREC OI Guidelines follow the principle-based approach contributes to their durability.

QoS optimisation is a challenging topic on a technical level, but these challenges can play out differently in specific situations. For instance, handover optimisation (e.g., based on user mobility prediction, as in Bahra & Pierre, 2021) in border regions and/or in roaming situations may have an effect on end-users due to the different billing systems applied for roaming and domestic use. Another example where QoS optimisation is crucial for end-users is seamless handover to enable the use of autonomous vehicles. This may necessitate closer cooperation between telecommunications providers across borders.

Lastly, it is important to keep in mind that for AI and ML techniques to properly work, very large datasets are required. ISPs, particularly smaller ones, may want to work more closely together and share more data to be able to offer more innovative or specialised services to end-users.[81]

---

[79] K. Jull, S. Schmidt. (2009) "Preventing harm in telecommunications regulation: New matrix of principles and rules within the ex ante versus ex post debate" *Canadian Business Law Journal 47(3)*, p. 329-362.

[80] Balmer, R.E., Levin, S.L., and Schmidt, S. (2020) "Artificial Intelligence Applications in Telecommunications and other network industries" *Telecommunications Policy 44(6)*, p. 9.

[81] Balmer, R.E., Levin, S.L., and Schmidt, S. (2020) "Artificial Intelligence Applications in Telecommunications and other network industries" *Telecommunications Policy 44(6)*, p. 7.

In short, optimising QoS through the adoption of AI allows for a more efficient use of network resources. It thereby contributes to the ability of networks to sustain more and more real-time traffic that requires high bandwidths without congestion. Regardless of the presence and use of AI, the OIR and the BEREC OI Guidelines ensure the equal treatment of traffic and regulate the network capacity and necessity for specialised services.

5.5. Security Optimization and Threat Detection

The research on AI related to security purposes especially in the context of telecommunications is extensive. The broad topic of security optimization can be described as proactively strengthening a network to better respond to evolving security threats, as well as to planned and unplanned events. [82] There are various proposals to achieve this goal via the introduction of AI and especially machine learning.

ML technology has become mainstream in a large number of domains, and cybersecurity applications of machine learning techniques are plenty, as Hanada et al. (2019) [83] illustrate. Examples include malware analysis, especially for zero-day malware detection, threat analysis, anomaly based intrusion detection of prevalent attacks on critical infrastructures, and many others. Due to the ineffectiveness of signature-based methods in detecting zero day attacks or even slight variants of known attacks, ML-based detection is being used by researchers in many cybersecurity products.

The convergence of data science and cyber security in recent years, as outlined by Sarker et al. (2020)[84], gave birth to the concept of cybersecurity data science, which provides more effective solutions to cyber threats than traditional methods.

Benzaïd et al. (2020)[85] describe AI as pivotal in empowering intelligent, adaptive and autonomous security management in 5G and beyond networks, due to its potential to uncover hidden patterns from a large set of time-varying multi-dimensional data and deliver faster and accurate decisions, while AI's capabilities and vulnerabilities make it a double-edged sword that may also jeopardize the security of future networks.

An ENISA report[86] outlining the contributions of standardisation to the mitigation of technical risks, and therefore to trust and resilience in the 5G ecosystem, rather advocates security by

---

[82] Cisco Security Optimization Service, https://www.cisco.com/c/dam/global/en_sg/training-events/security_techbyte/files/sos_ds.pdf, retrieved 04.10.2000

[83] Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9*(4), e1306.

[84] Sarker, I.H., Kayes, A.S.M., Badsha, S. *et al.* Cybersecurity data science: an overview from machine learning perspective. *J Big Data* **7**, 41 (2020).

[85] Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G networks: a cyber-security defense or offense enabler?. *IEEE Network, 34*(6), 140-147

[86] Cosquer, F., Zamora, F., Zugenmaier, A. (2022, March) *5G Cybersecurity Standards,* ENISA. DOI 10.2824/700472

design and solid basics with proven methods. The mentioning of AI within the report is limited to the consideration of new technologies with regard to detection tactics.

Nonetheless, many solutions to the variety of security related challenges the telecommunications sector faces could benefit from using AI. Probably the most common use cases can be summarized as security breach and threat detection. ML based AI can be trained to recognize deviating behaviour (anomaly detection), and therefore correctly detect security attacks. AI can also be implemented to analyse a large number of alerts issued by security solutions in order to react to security breaches or threats within the network.

According to Zaman et al. (2018)[87], an intrusion detection system can be described as a software that monitors a single or a network of computers for malicious activities (attacks) that are aimed at stealing or censoring information or corrupting network protocols.

Various approaches to enhance the traditional intrusion detection and prevention systems (IDPS) have been brought forward. An example of an IDPS can be seen in Figure 2 depiction of a typical IDPS (source Dilek et al., 2015)Figure 2. This system *"can detect possible intrusions and attempt to prevent them. Intrusion detection and prevention systems provide four vital security functions: monitoring, detecting, analysing and responding to unauthorized activities."* [88]

---

[87] Zaman, M., & Lung, C. H. (2018, April). Evaluation of machine learning techniques for network intrusion detection. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium (pp. 1-5). IEEE.
[88] S. Dilek, H. Caku and M. Aydin, (2015), "Applications of Artificial Intelligence Techniques to Combating Cyber Crime: A Review", International Journal of Artificial Intelligence & Applications, p. 24.
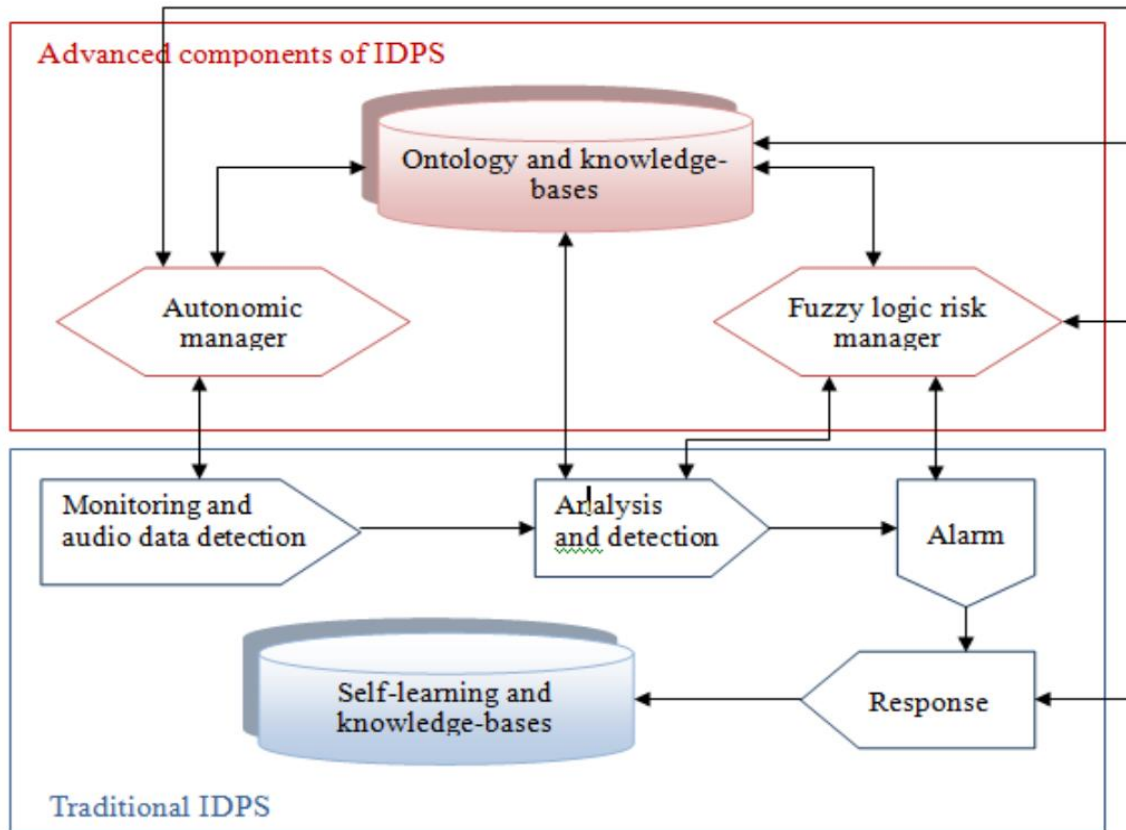
Figure 2 depiction of a typical IDPS (source Dilek et al., 2015)

Unfortunately, it is rather difficult to determine exactly whether and how much of this research has actually found its way into the market. Many vendors claim to have AI powered solutions while the limitations inherent to ML introduce new uncertainties, such as limited datasets, black box algorithms and high cost of human resources and computing power. Due to these circumstances many experts within the security field are wary of the hype that surrounds AI. [89][90]

According to the survey's responses, stakeholders employ a variety of anomaly detection and pattern recognitions techniques to detect threat and attacks early. Due to the vast amount of data passing through the networks and the evolving nature of cyberthreats, effective identification and mitigation of such threats requires automated analysis capability as well as autonomous decision-making, to ensure rapid and accurate responses to threats. Such AI

---

[89] Top Three Use Cases for AI in Cybersecurity https://www.datacenterknowledge.com/security/top-three-use-cases-ai-cybersecurity

[90] Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560.

systems help reducing the number of events that technicians must attend, reducing the number of false positives alerts and even activating of preventive controls. However, compared to stakeholders' answers on more central topics like network planning and management, the response on security topics were rather sparse.

5.6. Fraud Detection and Prevention

While ECN/S have always been exposed to fraud, the number of attacks and their impact are particularly increasing in the last years. The Communications Fraud Control Association (CFCA)[91] estimates the total amount of global telecom revenue loss in 2021 due to fraud at 2.22% of revenues ($39.89 Billion), increasing a 28% ($11.6 Billion) compared to 2019. In addition, it must be considered that fraud does not only impact telecommunication providers, but often target their users.

According to Europol[92], some of the reasons behind this trend are the increased automation and spread of the ECN/S. A network becomes 10 times more scalable, meaning that attacks using that infrastructure will have 10 times the effect, damage, and cost. Furthermore, criminals also benefit from the increased ECS speeds and use it against the carrier itself. The increased capability of the networks enables more cases of fraud during the time required to detect and respond to the attack.

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

- Spoofing: hiding the origination of identity to perform frauds by modifying IP address, the Calling Line Identification (CLI) or Automatic Number Identification (ANI). One example of spoofing is the modification of the CLI of calls from third countries to benefit from regulated EU termination rates.

- Wangiri/ One Ring and Drop: a call back fraud based on massive missing calls. If the user responds, the call, unknowingly for the user, is charged as a premium rate.

- Subscription Fraud: creation of false identities to access services with no intention to pay

- PBX[93] hacking allows fraudsters to take control of phone lines by exploiting unsecured phone networks and, ultimately, make fraudulent calls.

- SIM boxes are used to route international calls through the internet using VoIP and terminate those calls through a local phone. The caller pays the call as an international

---

[91] CFCA Fraud Loss Survey Report 2021 https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf
[92] Cyber-Telecom Crime Report 2019. https://www.europol.europa.eu/publications-events/publications/cyber-telecom-crime-report-2019#downloads
[93] PBX (private branch exchange) is a telephone system within an enterprise that switches calls between users on local lines, while enabling all users to share a certain number of external phone lines.

call, the local operator receives the revenue of a local call while the fraudsters retain the difference.

At the same time, applications for fraud detection have evolved and have become more sophisticated, often making use of ML based AI for a faster detection and prevention of frauds, such as text message scams and robocalls from reaching the public. One example is Virtual Assistant verification[94].

Fraud detection systems typically rely on a rules-based method for the identification of telecom fraud. Traffic data[95] is analysed against a set of rules to find anomalies that can be potential fraud cases. Those rules need to be constantly updated and adapted to changing consumer behaviours. The detection models based on ML AI are able to adapt and create new rules for fraud detection. For instance, the recent Electronics Communications Committee, Report 338 (June 2022) about CLI spoofing[96] explicitly supports "the encouragement of the installation by operators of traffic pattern analyses tools based on artificial intelligence".

Nevertheless, according to the CFCA Fraud Loss Survey Report 2021, the use of AI based fraud management systems to detect fraud is still low.
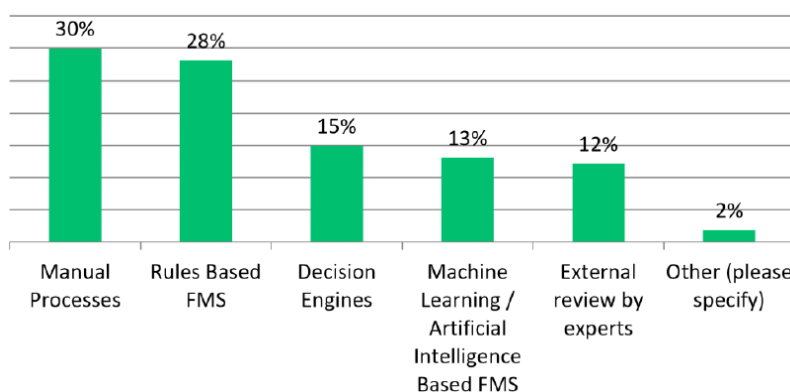

Figure 3 Industry tools used to detect fraud. Source: CFCA Fraud Loss Survey Report 2021

The responses to BEREC's survey point in the same direction. Most of the market stakeholders participating in the survey have deployed or are planning to deploy AI applications within their network operations with the aim of fraud detection and prevention. Respondents acknowledged the capacity of AI, together with other measures, by means of anomaly detection algorithms, to spot unusual usages patterns of network and voice services. This input is further analysed and possibly actioned upon by human specialists. In addition,

---

[94] https://ieeexplore.ieee.org/abstract/document/9474299
[95] Including both the monitoring of call detail records (CRD) and signal records.
[96] https://www.nkom.no/telefoni-og-telefonnummer/telefonsvindel/_/attachment/download/34a76b0e-011b-4bc0-b060-cc7761c0ffef:7b521945f6d348bd22fd3569e53458c8347fa51d/ECC%20Report%20338.pdf

the respondents point out that vendors specialised in fraud detection and prevention solutions are currently developing new R&D solutions based on AI.

Most NRAs are competent for the implementation of art. 97(2) EECC (formerly, in the same terms, art. 28(2) Universal Service Directive). This provision allows for the blocking access to numbers or services on a case-by-case basis where this is justified by reasons of fraud or misuse, and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues. In this context, the detection and prevention of fraud committed by means of ECS has been subject of several BEREC reports and activities, including a cooperation coordination procedure to address cross-border fraud.

According to the BEREC report on cross-border issues under Article 28(2) Universal Service Directive, only a few NRAs have implemented proactive methods to detect this kind of fraud. Therefore, most NRAs rely on the complaints received by the end users and ECS providers. BEREC acknowledges in this report that already in 2010 most European operators used automated systems for detecting fraud.

6. USE OF ARTIFICIAL INTELLIGENCE SOLUTIONS BY NRAs

6.1. The use of AI in the public sector

While noting that there is thus far little information available on the impact of the use of AI in the public sector, van Noordt and Misuraca (2022)[97] describe how AI systems could be and are being used to improve processes related to policy-making, public service delivery and public authorities' internal management.

---

[97] van Noordt, C. and G. Misuraca, 2022: Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union. Government Information Quarterly 39 (2022) 101714. https://doi.org/10.1016/j.giq.2022.101714

Table 1 An overview of AI functions in government (van Noordt & G. Misuraca, 2022, p. 4)

Governance function	Potential AI use
Policy making	1. To detect social issues more quickly 2. To improve public policy decisions (and to estimate potential effects on policy) 3. To monitor the implementation of policy (and to evaluate existing policy) 4. To enhance citizen participation in policy making
Public Services	1. To improve the information services of the organization 2. To improve public service delivery to business and citizens 3. To develop new innovative public services
Internal management	1. To improve the allocation of human resources 2. To improve recruitment services of the public organization 3. To improve financial management of the organization 4. To improve the detection of fraud and/or corruption 5. To improve maintenance 6. To improve public procurement processes 7. To improve organizational (cyber)security. 8. Other

According to the authors, policy-making could be improved by the capacity of AI systems to process large quantities of different types of data, e.g. images, text, audio, video or data streams from sensors, in an automated fashion. This could allow public authorities, comprising NRAs, to include not only more types and amount of data into their decision-making processes but also to involve more stakeholders, in particular citizens, in their policy development and facilitate an inclusive approach to devising regulatory action. One simple measure suggested by van Noordt and Misuraca would be reducing the language barrier by using tools to translate documents in an automated manner.[98] Of the 250 cases analysed in detail by the authors, about 23% were classified as belonging into this category.

For the delivery of public services, the authors suggest that improvements may be possible by tools, which personalise or automate interactions with public services, such as requests for information. The automation of repetitive tasks, for instance reporting, could free up the staff of NRAs to dedicate more time to personalised support and other tasks. In the sample analysed by the authors, 46% of the cases fell within this category.

---

[98] The European Commission provides a free-of-charge translation tool which appears to be trained primarily on legal/policy documents for text snippets (https://webgate.ec.europa.eu/etranslation/translateTextSnippet.html) as well as for documents (https://webgate.ec.europa.eu/etranslation/translateDocument.html).

This aspect ties in with the third area, AI for enhancing internal management. Here, the authors mention AI tools for prioritisation of resources, such as inspection, for monitoring operations of the staff, digitalising or anonymising documents, as well as identifying anomalies, or for procurement, e.g. by supporting the drafting of contracts. NRAs might also use AI systems for their own cybersecurity purposes. The authors found that about 30% of the cases analysed were used for internal management purposes.

6.2. Adoption of AI by NRAs

Some NRAs have studied the use of AI by the telecommunications sector, such as ARCEP's study on the Networks of the Future[99], or TRAI's consultation paper on the use of AI and Big Data for QoS, Spectrum Management and Network Security.[100] However, the responses to BEREC's survey to NRAs show that the adoption of AI by the NRAs is still at its infancy. Very few of the NRAs, which participated in BEREC's study, have undertaken or are planning to conduct studies to explore ways how AI can be adopted within the internal processes of the NRA. Those who have responded in the affirmative mentioned the following topics:

- Introduction of AI technology in the internal operations of the NRA

- Radio Channel Modelling including new techniques available for spectrum sharing among services with both equal status and unequal status;

- Detecting illegal/prohibited content online with AI

- Customer Relations Management Platform including a customer complaint classification using machine learning and text analysis tools;

- Monitor the market to ensure that products for sale online comply with the product safety rules in the EU (SAFE AI tool) [101]. The SAFE search tool employs AI in the form of image recognition and ML to identify dangerous and non-compliant products for sale online. SAFE is funded by the EC and is available to all interested EU/EFTA market surveillance authorities.

BEREC's desk research of the publicly available studies and initiatives that NRAs and Governments have undertaken has resulted in the following list of studies and initiatives undertaken by NRAs and Governments:

- The Government of Canada has awarded a contract to Ecopia AI to provide next generation mapping data to address the digital divide by identifying better connectivity

---

[99] "Réseaux du future - Note n° 6 - L'intelligence Artificielle dans les réseaux de télécommunications" Jan 2020 source: arcep.fr/uploads/tx_gspublication/reseaux-du-futur-IA-dans-les-reseaux-janv2020.pdf

[100] "Consultation Paper on Leveraging Artificial Intelligence and Big Data in the Telecommunication Sector", Aug. 2022, source: https://www.trai.gov.in/sites/default/files/CP_05082022_0.pdf

[101] https://www.sik.dk/en/business/nyheder/new-digital-fine-toothed-comb-denmark-about-make-more-300-million-european-consumers-safer

gaps in order to accelerate the deployment of broadband infrastructure across the country[102].

- The Australian Communications and Media Authority is looking at developing further its data analytics processes[103] and is also open to proposals to trial Dynamic Spectrum Access technology[104].

- OFCOM looked into the use of AI to measure online experiences[105].

- The FCC has set up a Technological Advisory Council Working Group on Artificial Intelligence and Computing to analyse the impact that AI may have on the nation's networks. This Working Group's proposals include the adoption of AI in broadband mapping, AI for radio frequency interference detection and to generate further knowledge from the databases that the FCC manages[106].

- According to the French Conseil d'État, competition authorities are considering the use of AI systems to detect cartels formed through algorithmic collusion.[107, 108]

For NRAs considering the adoption of AI technologies, BEREC notes that the following factors may be taken into consideration:[109]

- Data used for training AI systems should be thoroughly checked for biases and quality (van Noordt & Misuraca, 2022, p. 3). The Good Practice Principles for Data Ethics in the Public Sector developed by the OECD could provide a helpful starting point.[110] In

---

[102] "Ecopia AI Awarded Contract from Canadian Government to Support Rural Broadband Mapping Across the Country" Jan 2022, source: https://www.ecopiatech.com/news-post/ecopia-ai-awarded-contract-from-canadian-government-to-support-rural-broadband-mapping-across-the-country

[103] "Artificial intelligence in communications and media" July 2020 source: https://www.acma.gov.au/sites/default/files/2020-07/Artificial%20intelligence%20in%20media%20and%20communications_Occasional%20paper.pdf

[104] "Five-year spectrum outlook 2021–26 work program" ACMA, Sept 2021 source: https://www.acma.gov.au/sites/default/files/2021-09/FYSO%202021-26.docx

[105] "Automated approaches to measuring online experiences: Executive Summary, June 2021, source: https://www.ofcom.org.uk/__data/assets/pdf_file/0015/220425/automated-tooling-report.pdf

[106] "The Importance of Artificial Intelligence and Data for the Telecommunications Industry and the FCC," Jan 2021 Source: https://www.fcc.gov/sites/default/files/fcc_aiwg_2020_whitepaper_final.pdf

[107] https://www.conseil-etat.fr/actualites/s-engager-dans-l-intelligence-artificielle-pour-un-meilleur-service-public

[108] However, the likelihood of autonomous algorithmic collusion (without agreement between companies) is still debated, with the German Federal Cartel Authority (and the French Competition Authority) remaining thus far less certain about the applicability of experimental results to real market conditions (https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_6.pdf?__blob=publicationFile&v=3). On the other hand, the UK's Competition and Market Authority underlines the current paucity (not lack) of empirical evidence for this phenomenon, thus not disputing that autonomous algorithmic collusion can be achieved in real market conditions (https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers#theories-of-harm); this is the line of argument followed by the French Conseil d'État.

[109] For further details, see the CAHAI's provisional document on Artificial Intelligence in the Public Sector: https://rm.coe.int/cahai-pdg-2021-06-2779-3226-6755-v-1/1680a29927

[110] https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm

general, it has been noted that the problems of data availability as well as accessibility are often underestimated.[111]

- The results of AI systems should lead to equitable outcomes for different types of stakeholders that can be explained (van Noordt and Misuraca, 2022, p. 3).

- Introducing an AI system may require qualification training for staff[112] as well as changes of the data flow within NRAs or their processing capacities.

- Impact assessments should be completed prior to deployment, and adequate accountability structures should be set up.[113]

From a different perspective, NRAs could support the implementation of the AI Act at a national level, in particular when AI is used in the provision of ECN/S.

7. CONCLUSIONS

AI is a transversal technology that can be applied to a variety of use cases. In the telecommunications sector, processes are highly digitalised and digital data are available for training and operating AI systems, thus facilitating the adoption of AI technologies. Furthermore, the scale of telecommunications networks and the complexity of managing networks as well as Customer Management Relationship incentivise the adoption of automated systems.

Although the potential benefits of AI are paramount, there are also risks associated with the use of AI, which vary according to the context of deployment. Unbiased and reliable data are the basis for good decision-making. But how the algorithms use the data is often not clear, possibly leading to a lack of trust in the automated decision making. Privacy and security also remain important aspects that justify close monitoring of AI solutions.

With the growing importance of AI, NRAs have to acquaint themselves with the risks associated with AI, the methods of monitoring and the methods of assessing. A good knowledge of AI is required to study the outcome of AI, or the workings of the algorithm itself.

Whereas operators have found many ways to apply AI solutions, the NRAs have not made much use of AI so far. Literature and some examples from some regulators in Europe and abroad show a good number of use cases for AI. AI solutions could be used for policy making, public services or internal management. BEREC expects AI to mature over the years, both with operators and NRAs, and thus for AI to increasingly play a role for BEREC. Therefore, BEREC will continue supporting NRAs in gaining further understanding of the use and

---

[111] Vial, Gregory, Jinglu Jiang, Tanya Giannelia, and Ann-Frances Cameron (Winter 2021) The Data Problem Stalling AI. In: MIT Sloan Management Review. Massachusetts Institute of Technology.

[112] For this purpose, NRAs could consider Elements of AI as a starting point, which is a popular introductory online course developed by the University of Helsinki and MinnaLearn: https://www.elementsofai.com/

[113] https://algorithmwatch.org/en/accountability-in-the-use-of-ai-for-public-administrations/

implications of AI in the sector. A possible area of BEREC's future work in this field could be to assess whether and how AI impacts the user rights and the features of AI systems for customer management.

BEREC signals that NRAs could play a role in the implementation of the AI Act in a national level, in particular when AI is used in the provision of ECN/S by coordinating with other relevant bodies and providing technical support in based on their specialized knowledge and experience in the sector. NRAs should also be equipped to address sectoral competition concerns that might arise in the future regarding the application of AI.

ANNEX I. Techniques for AI systems

The techniques used in the literature reviewed can be grouped into a series of sub-fields. This Annex briefly explains these techniques and references areas in which these methods have been applied in telecommunications[114]. Other techniques may include expert systems and other approaches, which are however not addressed by research included in this report.

It is important to note that many AI systems apply a combination of techniques from different fields. For instance, an AI system to ensure the quality of service and dynamic bandwidth allocation in Passive Optical Networks (PONs) may draw on both genetic algorithms (which are considered part of the search methods and optimisation theory group) as well as neural networks (a learning method).

Cognitive systems, while also applied in telecommunications (e.g. for fault detection, topology mapping or network virtualisation), are different from AI approaches in that they draw on some of these techniques, but incorporate other approaches as well.[115]

Search methods and optimisation theory

This group of techniques includes mathematical formulations (e.g. mixed integer linear programming), breadth-first search and tabu search, as well as a group of techniques related to local search algorithms and metaheuristics. This sub-group includes teaching-learning based optimisation, simulated annealing and genetic algorithms, as well as a further subgroup of methods related to swarm intelligence (which in turn includes techniques such as ant colony optimisation, artificial bee colony algorithms, gravitational search algorithms, fire-fly algorithms and particle swarm optimisation).

These techniques are applied, amongst others, for survivable optical networks, regenerator placement, connection establishment, resource allocation, splitter placement in PONs, placement of Optical Network Units (ONUs), transmitters, QoS guarantees and dynamic bandwidth allocation in PONs, network reconfiguration and reduction/estimation of burst loss.

Statistical models

The group of techniques based on statistical models includes Bayesian methods, Kalman filters and hidden Markov models.

Applications for statistical models include transmitters, receivers, non-linearity mitigation, statistical solutions for prediction, QoS guarantees and dynamic bandwidth allocation in

---

[114] Drawing on Mata et al. (2018) Survey of AI methods in optical networking.
[115] https://www.iks.fraunhofer.de/en/topics/cognitive-systems.html

PONs, reduction/estimation of burst loss, failure/fault detection, linear impairment identification and connection establishment.

Decision-making algorithms

Techniques grouped as decision-making algorithms include Markov decision processes. These are a type of reinforcement learning algorithm seeking to optimise its performance by automatically determining their ideal behaviour.

Resource allocation, connection establishment, and intra-data centers number amongst the possible applications of these techniques in telecommunications.

Learning methods

By far the most well-known branch of AI techniques, learning methods include the sub-group of probabilistic learning methods (which include Bayesian learning and expectation maximisation) and machine learning. Through machine learning, a mathematical model can be built on the basis of a data set. This model predicts/infers previously unknown variables on the basis of the original data set and can be applied to new data sets, e.g. for classifying or categorising data.

Machine learning can be further subdivided into reinforcement learning (which includes Q-learning), supervised learning and unsupervised learning. The group of techniques classified as supervised learning includes neural networks (which in turn also encompass deep neural networks), support vector machines, linear regression, logistic regression, random forests and instance-based learning (such as K-nearest neighbours or case-based reasoning). Unsupervised learning techniques include principal component analysis and K-means clustering.

Applications for machine learning approaches in the context of telecommunications include resource allocation, modulation format recognition, receivers/non-linearity mitigation, connection establishment, linear impairments identification, reduction/estimation of burst loss, network reconfiguration, software-defined networking, QoS guarantees and dynamic bandwidth allocation, intra-data centers, optical amplification control, OSNR monitoring, intelligent ROADM, QoT estimation, as well as transmitters.

Game theory

Game theory emerged from applied mathematics as a framework for understanding how individuals make decisions or act to maximise their returns in situations with predefined rules. This theoretical branch can be applied in AI development in a variety of ways. For instance, drawing on game theory, two neural networks can be combined into a generative adversarial

network, where one neural network creates an output which is then judged by the second neural network as true or false. The aim of the consecutive interaction between these two neural networks is to maximise the quality of the output of the generating neural network. AI applications in telecommunications based on game theory include solutions for connection establishment and statistical solutions for prediction.
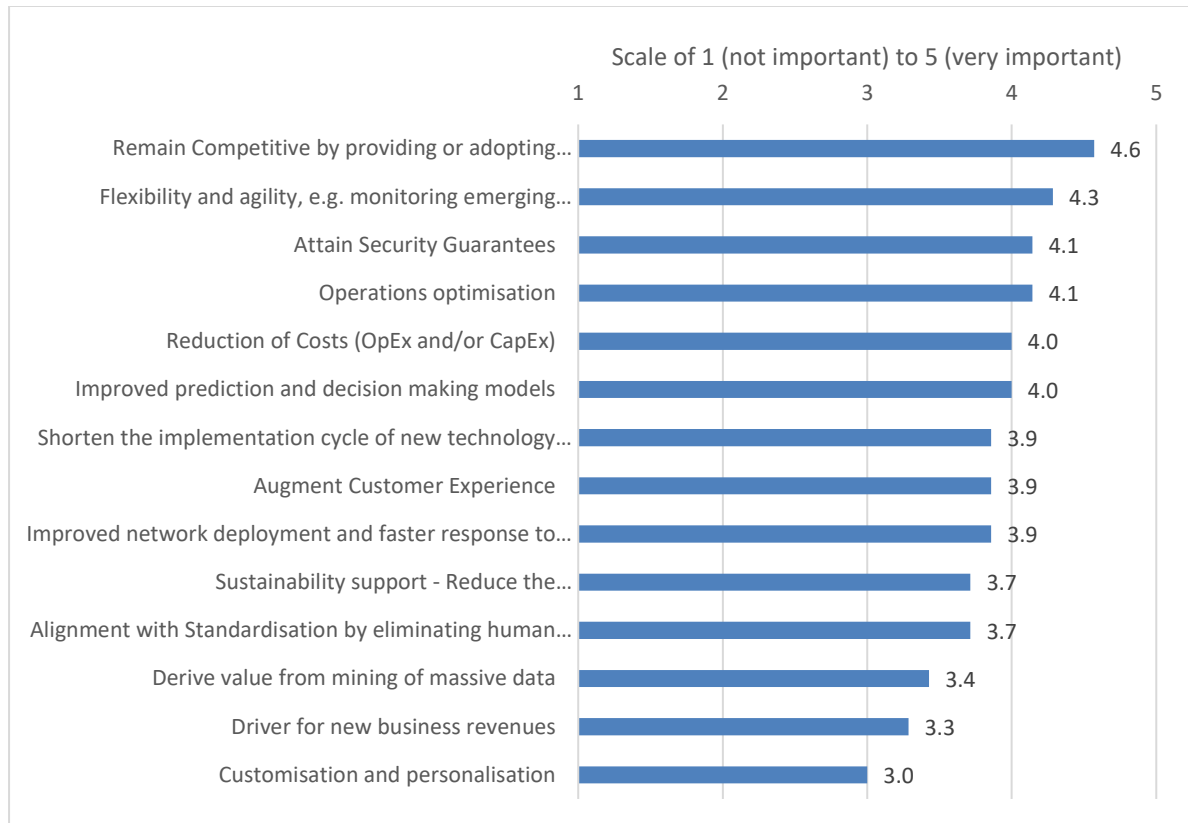
ANNEX II.   Overview of survey responses

Figure 4 When assessing whether to deploy a new AI solution, which benefits listed below do you pursue or prioritise? Average rating of survey respondents (n=7)

Average rating from 1 (not important) to 5 (very impor

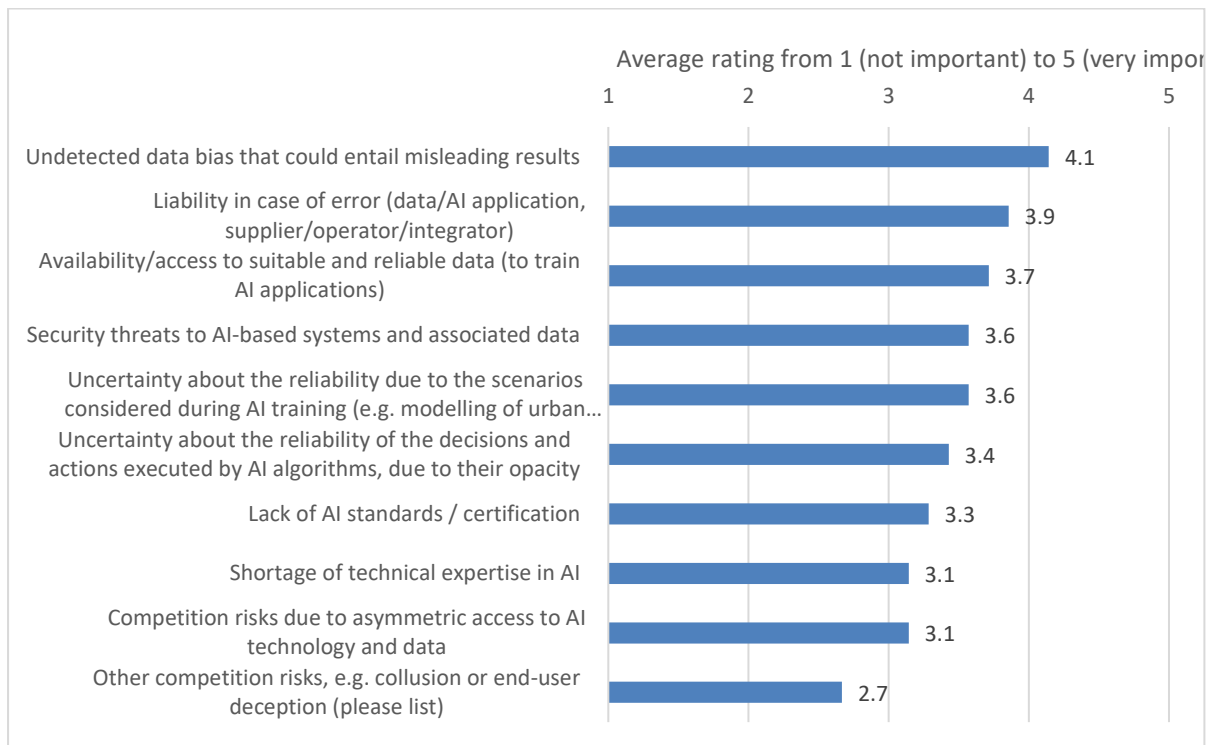|	
Undetected data bias that could entail misleading results	4.1
Liability in case of error (data/AI application, supplier/operator/integrator)	3.9
Availability/access to suitable and reliable data (to train AI applications)	3.7
Security threats to AI-based systems and associated data	3.6
Uncertainty about the reliability due to the scenarios considered during AI training (e.g. modelling of urban…	3.6
Uncertainty about the reliability of the decisions and actions executed by AI algorithms, due to their opacity	3.4
Lack of AI standards / certification	3.3
Shortage of technical expertise in AI	3.1
Competition risks due to asymmetric access to AI technology and data	3.1
Other competition risks, e.g. collusion or end-user deception (please list)	2.7

Figure 5 Which of the following risks and challenges are you currently most wary of? Average rating by survey respondents (n=7, except for "Other competition risks", where n=6)
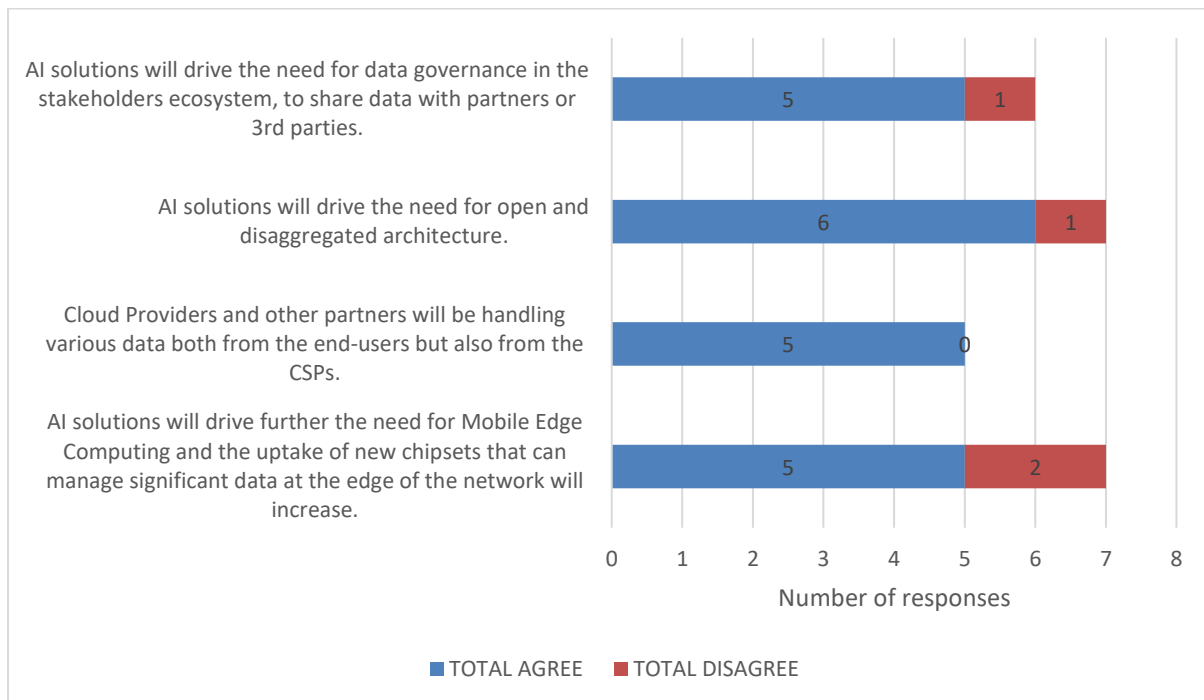
Figure 6 Do you anticipate any of the following changes to the CSPs' network architecture as a result of an increase in the uptake of AI solutions?

ANNEX III. Key public bodies and stakeholders in the context of AI

PUBLIC BODIES & STANDARIZATION ORGANIZATIONS	TASKS AND ACTIVITIES RELATED TO AI	
INTERNATIONAL ORGANIZATIONS		
International Telecommunications Union (ITU)	The ITU has published a variety of standards for AI applications related to telecommunications[116] and set up multiple working groups dedicated to particular topics, such as the Global Initiative on AI and Data Commons[117].	
Council of Europe	The Council of Europe has set up a Committee on Artificial Intelligence[118], focusing on the human rights impacts of AI technologies	
EU		
EC	The EC is tasked with approving standards developed by CEN-CENELEC for the implementation of the AI Act, as well as fulfilling a role in the European AI Board to be set up under that Act. Furthermore, Art. 39 EECC grants the EC the power to publish non-compulsory standards or to request CEN, CENELEC or ETSI to develop such standards.	
EUROPEAN STANDARDS ORGANIZATIONS	European Committee for Standardization (CEN) & European Committee for Electrotechnical	A CEN-CENELEC Joint Technical Committee on Artificial Intelligence has been established. Standards approved by CEN-CENELEC[119] are key to the implementation of the AI Act. These can include standards related to the data used for training AI systems[120], for

---

[116] E.g. the Guidelines for intelligent network analytics and diagnostics ITU-T E.475 (https://www.itu.int/rec/T-REC-E.475-202001-I/en), the Recommendation ITU-T Y.3174 on a Framework for data handling to enable machine learning in future networks including IMT-2020 (https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14134), the Recommendation ITU-T Y.3116 on Traffic typization IMT-2020 management based on an artificial intelligence approach (https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14855), the Recommendation ITU-T Y.3178 on a Functional framework of artificial intelligence-base network service provisioning in future networks including IMT-2020 (https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14613) and others.

[117] https://www.itu.int/en/ITU-T/extcoop/ai-data-commons/Pages/default.aspx

[118] https://www.coe.int/en/web/artificial-intelligence/cai

[119] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/

[120] For instance, the ISO/IEC standard ISO/IEC CD 5259-1 (https://www.iso.org/standard/81088.html?browse=tc).

	Standardization (CENELEC)	the design of AI systems[121] or for the classification of computational approaches for AI systems[122].
	European Telecommunications Standards Institute (ETSI)	In June 2020, ETSI published a whitepaper: Artificial Intelligence and future directions for ETSI[123]. ETSI work related to AI is underway in the following areas: 5G Systems; Network Optimization and End-to-End Service Assurance; IoT, Data Acquisition & Management, Governance and Provenance; Security and Privacy; Testing and Health and Societal Applications of AI (e.g. use of AI for geo-localization in case of emergencies).

National
Most MS have developed AI strategies setting out their priorities[124]. Regulatory and data protection authorities also play a strong role in the development of Europe's approach to the regulation of AI.

Market	
STAKEHOLDERS	**ROLES RELATED TO AI**
ECN/S providers	Telecommunications providers show varying degrees of activity related to AI; some are actively engaged in research, and many have developed their own AI strategies. Some of these activities are also organised at European level, e.g. by the GSMA[125]
AI and hardware providers	Providers of AI systems or the hardware required for the use of these systems form an important part of the ecosystem and are often closely involved in standardisation efforts.

---

[121] For instance, the ISO/IEC standard ISO/IEC DIS 25059 (https://www.iso.org/standard/80655.html?browse=tc).
[122] For instance, the ISO/IEC standard ISO/IEC TR 24372:2021
(https://www.iso.org/standard/78508.html?browse=tc). The definition of AI in the draft AI Act is itself not based on international technical standards.
[123] Artificial Intelligence and future directions for ETSI. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp34_Artificial_Intellignce_and_future_directions_for_ETSI.pdf
[124] https://oecd.ai/en/dashboards/countries/EuropeanUnion
[125] https://www.gsma.com/artificialintelligence/

NGO/civil society	NGOs such as AlgorithmWatch[126] or the Green Software Foundation[127] are specialized in monitoring the use of AI systems and its potential impact on society.

---

[126] https://algorithmwatch.org/en/projects/
[127] The Green Software Foundation developed a tool for monitoring the carbon intensity of software (https://github.com/Green-Software-Foundation/software_carbon_intensity/blob/dev/Software_Carbon_Intensity/Software_Carbon_Intensity_Specification.md) which was applied by Dodge et al. (2022) to AI based in the cloud: https://arxiv.org/abs/2206.05229

ANNEX IV. Acronyms

AI – Artificial Intelligence

ANI - Automatic Number Identification

CBRS - Citizens Broadband Radio Service

CEN-CENELEC European Committee for Standardization (CEN) &

European Committee for Electrotechnical Standardization (CENELEC)

CDN - Content Delivery Network

CLI - Calling Line Identification

CFCA - Communications Fraud Control Association

CSP – Communications Service Provider

EC – European Commission

ECN/S - Electronic Communication Networks and Services

EECC - European Electronic Communications Code

ETSI - European Telecommunications Standards Institute

EU – European Union

GDPR - General Data Protection Regulation

IDPS - intrusion detection and prevention systems IoT - Internet of things

ISP – Internet Service Provider

ISO - International Organization for Standardization

ITU - International Telecommunications Union

MIMO- Multiple-Input Multiple-Output

ML - Machine Learning

NFV – Network Function Virtualization

OSNR - Optical signal-to-noise ratio

OTT – Over The Top

PBX - private branch exchange

PONs - Passive Optical Networks

QoS – Quality of Service

QoT - Quality of Transmission

RAN - Open Radio Access Network

ROADM - Reconfigurable Optical Add-Drop Multiplexer

RNN - Recurrent Neural Networks

SLA – Service Level Agreement

SDN – Software Defined Networking

ZSM - Zero-touch network and Service Management

ANNEX V. PARTICIPANTS IN THE STUDY

TRANSATEL

Telefonica, S.A.

Liberty Global

Telia Company

ECTA (European Competitive Telecom Association)

KPN

Telefónica Germany

Turkcell

Amazon Web Services

Dialogic innovation & interaction