HUMANE AI NET

AI Research agenda for the telecommunications industry

axiata etno GSMA O2 orange stc Telefónica

telenor Telia TELSTRA TIM TURKCELL vodafone

Authors:

- Dr. Richard Benjamins. Chief Responsible AI Officer, Telefónica.
- Mojca Cargo. Director, AI4I, GSMA.
- Gökçe Çobansoy Hızel, Data Privacy. Competition and New Technology Law Associate Director, Turkcell.
- Lisa Green. Customer and Data Intelligence Group Owner, Telstra.
- Emilie Hien. Responsible AI Program Manager, Orange.
- Dr. Raffaele de Peppe. Strategy Officer, Telecom Italia Mobile.
- Ahmed Saady Yaamin. Head of Axiata Group Analytics, Axiata.
- Xhoana Shehu. Policy Manager, European Telecommunications Network Operators' Association (ETNO).

The workshop that has led to this report received support from the HumanE AI Net project funded by the European Commission under Grant Agreement Number: 952026.

Table of contents

1. Introduction

In collaboration with the Humane AI net project[1], the German Research Centre for Artificial Intelligence (DFKI), Telefónica, GSMA, The European Telecommunications Network Operators' Association (ETNO) and German Entrepreneurship organised a closed-door industry workshop which took place on 29 November 2022 in Munich, Germany to discuss promising artificial intelligence (AI) research areas for the telecommunications industry.

1.1 The origin of this research agenda

This invitation-only workshop provided a unique opportunity to generate an AI research agenda for the telecommunications industry based on input from key players in the sector itself. The document you are reading is the final deliverable published under a Creative Commons By license

The objective of the workshop was to define the telecommunications industry research agenda in AI. More than 10 mobile network operators (MNOs) participated from Europe and from the rest of the world (Australia, Middle East) including Axiata, O2 Germany, Orange, stc, Telefónica, Telenor, Telia, Telstra, TIM, Turkcell and Vodafone, and they came together for two days to discuss what is needed from AI in the future. The full list of participants appears in Annex 2: Participants of the workshop.

During the workshop, the Humane AI net project explained the major trends in AI research. Then, several companies shared how they are using AI currently in their operations and business practises. Finally, the respective companies explained what AI capabilities they would be interested in for the future.

[1] https://www.humane-ai.eu/

This last part has been the input for the telecommunications industry AI research agenda. The detailed agenda of the workshop can be found in Annex 1: Agenda of workshop.

1.2 The positive impact of artificial intelligence (AI)

AI can be defined as the ability of a machine or computer to emulate human capabilities through learning and automation. Drawing on advanced automated feedback loops, AI systems continually optimise the algorithms they use to achieve a specific goal, via a process known as machine learning (ML).

Over the past decade, many AI systems have progressed to a point where they can be used to accurately transcribe or translate text, write code, recognise a vast range of images, anticipate when a machine will break down and optimise complex industrial systems and processes.

At the same time, the vast expansion in connectivity with the rollout of 5G and the Internet of Things (IoT) is enabling organisations and individuals to collect more real-world data in real-time. This data can be used to further improve AI systems so that they become increasingly sophisticated and capable. In effect, these technologies can create a powerful virtuous circle that can generate immense socio-economic benefits.

The European Parliament has noted[2] that “AI can increase the efficiency with which things are done and vastly improve the decision-making process by analysing large amounts of data. It can also spawn the creation of new products and services, markets and industries, thereby boosting consumer demand and generating new revenue streams.”

The consultancy PWC has estimated[3] that AI could add 14% to global GDP – the equivalent of up to US$15.7 trillion by 2030. It says the economic impact of AI will be driven by productivity gains from businesses automating processes, as well as augmenting their existing labour force with AI technologies, and increased consumer demand resulting from the availability of more personalised and higher-quality products and services.

2. The regulatory landscape

2.1 The AI Act

The AI Act[4] is a proposed European law on AI – the first law on AI by a major regulator anywhere. The law assigns applications of AI to four risk categories. First, applications and systems that create an **unacceptable risk**, such as government-run social scoring

2 https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf
3 https://www.pwc.co.uk/economic-services/assets/macroeconomic-impact-of-ai-technical-report-feb-18.pdf
4 https://artificialintelligenceact.eu/the-act/

of citizens or deliberate manipulation to create harm, are banned. Second, **high-risk applications**, such as a CV-scanning tool that ranks job applicants and results in hiring, are subject to specific legal requirements. Third, applications with **limited risk**, such as the creation of deep fakes, come with a transparency obligation. Lastly, applications of **low risk** are largely left unregulated, though with a recommendation for self-regulation.

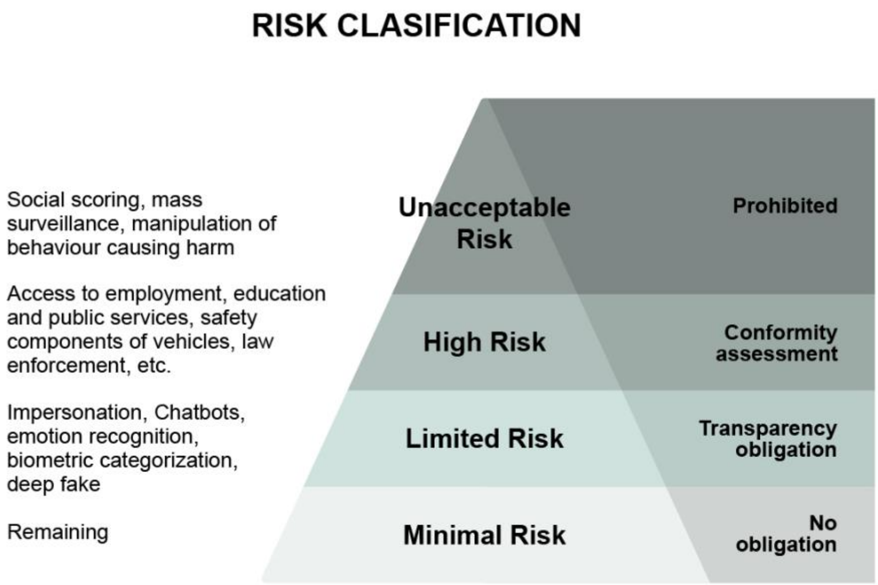


Figure 1 The risk-based approach proposed in the European AI Act.

During the creation process of the AI Act, several topics were much debated, Including the definition of AI, high-risk definition and general-purpose AI. At the time of writing there were multiple ongoing conversations:

Definition of AI. The original definition in the AI Act had a strong technological component enumerating specific technologies. After several versions, the non-finalised definition of AI from the European Parliament in April 2023 was: a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments, which is in line with the OECD AI definition[5].

- **High risk definition**. In April 2023 European Parliament's non-final version of high-risk definition in the AI Act is: "*Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are met:*

[5] https://oecd.ai/en/ai-principles

A. *the AI system is intended to be used as a safety component of a product or system, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex II of the AI Act;*

B. *the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment related to risks for health, safety, or fundamental rights of natural persons (AM 1421, 1431) with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II."*

"*In addition to the high-risk AI systems referred to in paragraph 1, AI systems falling under one or more of the critical areas and use cases referred to in Annex III of the AI Act shall be considered high-risk if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons."*

- **General purpose AI (GPAI)**: during the discussions of the AI Act, generative AI systems such as ChatGPT, Dall-e and Stable Diffusion attracted much debate as potential high-risk system. This led the European Parliament to include General Purpose AI as a separate category of AI systems in the AI Act, proposing specific obligations for such systems. The discussion is on whom the obligations should be incumbent, taking into account that the responsibilities should lie with the actors in the value chain that are best positioned to mitigate the risks of GPAI. The proposed definition in April 2023 for General Purpose AI: "*(1a) (new) means an AI system that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of tasks."*

2.2 AI liability directive

The AI Liability Directive complements the EU civil liability framework, introducing specific rules on damages for harm caused by AI systems.

The new rules ensure that victims of harm caused by AI technology can avail of a remedy, in the same manner as if they were harmed under any other circumstances. The Directive introduces two main measures[6]:

- the 'presumption of causality', which will relieve victims from having to explain in detail how the damage was caused by a certain fault or omission. "*If victims can show that someone was at fault for not complying with a certain obligation relevant to the harm, and that a causal link with the AI performance is reasonably likely, the court can presume that this non-compliance caused the damage. On*

[6] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5793

the other hand, the person allegedly liable can rebut such presumption (for example, by proving that a different cause caused the damage)."

- and the access to relevant evidence from companies or suppliers, when dealing with high-risk AI. "*Victims will be able to ask the court to order disclosure of information about high-risk AI systems. This will allow victims to identify the person that could be held liable and to find out what went wrong. On the other hand, the disclosure will be subject to appropriate safeguards to protect sensitive information, such as trade secrets.*"

2.3 Data Act

The European proposal for the Data Act regulation is a legislative initiative aiming at fostering the European Union's data economy by addressing the challenges related to data access, usage, and sharing within the Single Market. The proposal builds upon existing regulations, such as the General Data Protection Regulation (GDPR) and the Open Data Directive, to create a harmonised framework for data governance across EU member states. Key objectives of the Data Act include promoting data sharing among businesses and public sector organisations, enhancing data portability for individuals, and ensuring fair competition in the data-driven economy, especially for small and medium-sized enterprises (SMEs). Overall, the European Data Act regulation aspires to bolster innovation, drive economic growth, and protect rights in the age of digital transformation.

Some of the key points include Business-to-business data sharing and Business-to-Government data sharing, which are relevant for this research agenda.

3. Current uses of AI in the telecommunications industry

With the rollout of 5G and the Internet of Things (IoT), more sensors, devices, machinery, and vehicles are becoming connected, enabling cellular networks to capture a very wide range of data. At the same time, AI systems are becoming increasingly sophisticated and capable. Together, these technologies can create a powerful virtuous circle that can improve business operations and generate immense socio-economic benefits.

AI can help organisations to improve prediction, optimise operations, allocate resources more efficiently, and personalise digital solutions, to name just a few.

The telecommunications industry is no different. AI is at the core of operational and business models for an increasing number of mobile network operators (MNOs). It is enabling MNOs to improve both connectivity and their customers' experience. By using AI to optimise and automate networks, MNOs can provide better services and enable more people to become connected.

In Chapter 3, we give an overview of the AI use cases that the workshop participants are using in their respective companies.

3.1 Network-related use cases

AI can be used to improve the mobile network in several ways.

Network planning entails the forecasting of network traffic and then generate the right investments to the right locations to anticipate the increase in traffic. It involves smart functions that recommend deployment updates to improve customer experience and/or other selected metrics. Some MNOs use ML to find the best cell parameter configurations to improve mobile network quality without the need for new hardware installation or to predict the number of connected users to a cell and therefore act on network planning.

Similarly, **network optimisation** uses AI algorithms to analyse network data and identify bottlenecks, congestion, and other issues that can affect network performance. This information can then be used to optimise network configuration and resource allocation for improved efficiency, coverage and capacity.

AI can also be used to predict peak network traffic by analysing historical traffic data, identifying patterns, and making predictions about future traffic levels. Relevant AI techniques include time-series analysis, ML, deep learning, and predictive analytics.

3.1.1 Network monitoring and traffic management

Network monitoring entails the detection and tracking of problems in the network that impact network operation and enables a root-cause analysis and subsequent remediation to be performed. AI can help human supervisors to detect the pattern of problems more quickly and easily.

Traffic management uses AI to analyse network traffic patterns and dynamically adjust network resources to ensure that the most critical traffic is prioritised and that network congestion is prevented.

3.1.2 Predictive and proactive maintenance of the network ("Network Assurance")

Network operation centres deal with enormous volumes of data. Together with a huge amount of network-generated alarms to look at, the ability to perform analytics in real time is one of the important challenges. A data-driven prioritisation module or predictive algorithms, support network alarms prioritisation and automation of issue tickets creation and dispatching process. Specific examples include:

- Predictive maintenance: AI can be used to analyse data from network equipment and predict when maintenance or repairs are needed, which can help reduce downtime and improve network availability.

- Anomalous events can be detected automatically in the network using ML after which MNOs can decide on further actions.

- Service delivery process failures directly impact final users. Predictive algorithms can be used to detect potential failures in advance to intervene in time, and to prevent failures in the service-delivery process.

- Supporting predictive maintenance: AI can pinpoint patterns that indicate a network component is nearing the end of its natural life, enabling it to be replaced before it fails.

- Self-healing networks: AI can be used to automatically detect and diagnose network issues and make real-time adjustments to prevent or mitigate network failures.

3.1.3 Energy optimisation of the telecommunications network

Energy optimisation can be achieved by data-driven energy management and an optimisation tool with data exploration features; namely AI systems can optimise different elements of the network, so that they use just the right amount of energy required to deliver the desired level of performance and hence optimise costs that are a significant burden on the MNOs. AI can also be applied to determine the best type of power to consume.

Moreover, ML can be used for generating alerts on specific sites that need the attention of an energy manager.

3.1.4 Enhancing network security and reducing fraud

AI-based systems can analyse network traffic in real-time and detect anomalies or suspicious patterns that may indicate a cyber-attack. They can also use ML algorithms to identify new, unknown threats and adapt to changing attack patterns.

AI can also help identify actors and devices that are seeking to disguise their identity for financial gain. Tools and expertise can continuously identify and immediately stop multiple kinds of fraud in near real-time and through its activities reduce fraud.

3.2 Marketing and customer-related use cases

AI systems can also strengthen and enable personalised and meaningful interactions with customers, ultimately improving customer experience and engagement. For example, they can be used to improve automated communications, virtual assistance, customised pricing, and technical support. In the security sphere, AI systems can help to detect and prevent fraud, fend off cyber-attacks, and counter unlawful robo-calling.

3.2.1 Next-best activity (NBA)

Next Best Activity or Action is a customer-specific approach that use analytics and/or ML to predict various actions that could be implemented for a specific customer and then chooses the best possible option to implement. For example, AI can be used to understand customers' questions, and their context, and then provide them with appropriate answers. This is today moving toward Next Best Experience and hyper-personalisation, taking customer engagement to the next level with Next Best Experience[7].

[7] https://www.pega.com/insights/articles/taking-customer-engagement-to-the-next-level-with-next-best-experience

3.2.2 Churn prediction

Churn prediction is the process of identifying customers who are likely to leave a company or discontinue using a product or service. AI can be used to predict churn by analysing customer data, identifying patterns and factors associated with churn, and making predictions about which customers are most likely to leave and ultimately assessing more accurately how to retain more loyal customers.

3.2.3 Smart pricing

Smart pricing is the process to optimise pricing strategies and improve revenue by analysing data on customer behaviour, market trends, and competition. There are many strategies which include price optimisation, dynamic pricing, and personalised pricing.

3.2.4 Credit scoring

With the support of AI MNOs can improve credit scoring. This is based on MNO data by analysing customers' usage of telecommunications services and identifying patterns that indicate creditworthiness.

3.2.5 Recommendation of devices

AI can be used to recommend mobile devices to customers based on their preferences, usage patterns, and other factors. Some MNOs use a combination of deep learning and reinforcement learning to find the right device at the right time to recommend.

3.2.6 Product and service recommendation

Products and services can be recommended with the support of AI based on customers' preferences, purchase history, and other factors. Relevant AI techniques include collaborative filtering, content-based filtering, and a combination of both. Recommendation systems can also incorporate external information such as customer reviews, social media, and events data to improve the accuracy of the recommendations.

3.2.7 Digital assistant for 365/24 customer service (chatbots)

Chatbots and digital assistants are currently used by many MNOs to offer an “around the clock” customer service. Search services include both frequently asked questions (FAQs) as well as personalised customer service using data on the specific situation of customers. They are also used to qualify the request, give a first-level answer and if needed give the floor to a human assistant.

Generative AI is appearing as an important opportunity to build a fluent, personalised, efficient relationship with customers.

3.3 External monetisation

Further, MNOs can provide governments and public agencies with the AI solutions and big data analytics they need to tackle a wide range of problems. MNOs can deliver valuable insights that can help to address pressing policy challenges, such as climate change and pollution, the need for better healthcare and transport, and sustainable development, while also responding effectively to extreme weather, natural disasters and epidemics.

Anonymised and aggregated network data can be used for generating crowd insights for retail, town and city councils, tourism & events, public transport, and travel emissions insights. Mobile devices constantly generate movement data in our network. Each device will generate up to 200-400 data points per day, depending on how active the user is. The network can be divided into geographical areas large enough to ensure that individuals cannot be identified. It then irreversibly anonymises the data before aggregating and extracting it as crowd data; and analyses the crowd movement between different parts of the city: for example, where people commute to and from each day. It also allows the analysis of crowd density in different parts of the city at different times of the day. This gives useful insights into the way crowds move.

Some MNOs already provide AI capabilities to third parties on a commercial basis. They may deliver AI as a platform capability or they may employ AI to process mobile network data for analytics for third-party organisations, such as governments, traffic planning authorities, energy providers and other commercial organisations.

Some examples include[8]:

Better cities and public infrastructure: Town and city councils can use data tools and insights developed by MNOs to enable better planning, service delivery and transport. For example, mobile network

8 https://www.gsma.com/betterfuture/resources/ai4i-use-cases

data showing population movements could be used to help plan a new bus route or train line.

Curbing climate change and protecting the environment: MNOs can help governments understand how climate change and environmental issues will impact communities. For example, MNOs can develop tools that enable AI systems to forecast how weather patterns will change and predict future population movement.

Managing disasters and pandemics: MNOs can provide public agencies with tools that can provide an early warning of a disaster, support the subsequent response, and inform specific recovery and rehabilitation initiatives. For example, a country experiencing an outbreak of a contagious disease could use these tools to help track and mitigate the spread of the disease.

Supporting industry and commerce: Businesses can use MNOs' insights and tools to achieve greater transparency, and thereby improve operational planning and financial access. For example, connected sensors and monitors can collect real-time data that can be used by AI systems to optimise industrial and commercial processes.

Driving social inclusion: MNOs' insights and data tools can help enhance equity, social welfare, public access and health, and inform effective solutions to pressing social challenges. For example, AI systems can analyse mobile network data to detect gradual changes in populations and ensure that local public services, such as education and healthcare, are appropriately resourced.

4. Artificial intelligence research agenda for the telecommunications industry

The workshop demonstrated that AI is at the heart of the future of the telecommunications industry. Companies stated that within five years AI will be adopted at scale, and that 100% of the business processes will be improved with AI ("AI everywhere"). AI will enable new ways of working including the use of AI as a general innovation platform.

In order to make this happen, MNOs will have to invest in their data foundations. Without this, it is not possible to scale AI to every corner of the business, especially because of the sheer data volume and low latency requirements. Moreover, the application of AI and ML needs to be industrialised. AI will not only be used to improve business services, but also when providing innovative products and services for external customers, citizens, businesses, and governments. In this Chapter 4, we will present the research topics that were identified for the telecommunications AI research agenda.

Notice that when a topic is identified on the research agenda, this means that it needs more research for the telecommunications industry. It does not necessarily mean that more research is needed in general AI; it might just mean that it needs to be applied to the telecommunications industry.

4.1 Data foundations

Data foundations are important for AI because they provide the raw material that AI algorithms use to learn and make predictions. Without access to high-quality, diverse, and relevant data, AI systems would not be able to perform their tasks effectively. Data foundations also play a critical role in ensuring the privacy, fairness, accountability, and transparency of AI systems, by providing the ability to understand how the algorithms make decisions and by identifying and mitigating any biases in the data. Additionally, having a robust data foundation can help to ensure the scalability and maintainability of AI systems over time.

4.1.1 Foundations

Data foundations for AI consist of the various elements that are required to ensure that an AI system has access to high-quality, diverse, and relevant data. These elements include:

- Data collection: the process of gathering data from various sources. This can include structured data from databases, as well as unstructured data from text, images, and videos.
- Data cleaning: the process of removing errors, inconsistencies, and irrelevant data from the collected data. This can include tasks such as dealing with missing values, correcting inaccuracies, and removing duplicates.
- Data integration: the process of combining data from multiple sources into a single, cohesive dataset.
- Data annotation: the process of labelling or adding metadata to the data to make it more useful for training AI models.
- Data governance: the process of managing the overall data foundation, including ensuring data quality, privacy, security, and compliance with regulations.
- Data storage and management: The process of storing the data in a way that makes it easy to access and use, as well as having a system in place to ensure data integrity and accessibility.

In current practice, many of these activities are still manual. Therefore, research that aims to automate parts of these activities, particularly given the sheer volume of data and low latency requirement, will be important to scale the use of AI across the business.

Moreover, for many MNOs, data silos exist between network and customer areas, and it is a challenge to manage trans-silo use cases that include different teams. Adding to this complexity is that networks are composed of equipment from different vendors complicating further the data challenge.

4.1.2 Privacy

Privacy is important for AI for several reasons:

- Data protection: MNOs collect and store large amounts of personal data, such as customer location, usage, and browsing history. Ensuring the privacy and security of this data is crucial to protect customers from data breaches and unauthorised access.
- Compliance: MNOs are subject to a variety of laws and regulations that govern the collection, storage, and use of personal data, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the US. Adhering to these regulations is essential to avoid legal penalties and reputational damage and ultimately lost trust.

- Trust: Protecting customer privacy helps to build trust between the MNOs and its customers. Customers are more likely to use and recommend a company that they trust to protect their personal data.

- Innovation: Privacy-enhancing technologies, such as homomorphic encryption and federated learning, can enable new and innovative use cases for AI without compromising customer privacy.

- Data ethics: Apart from legal and regulatory issues, the use of personal data for AI also implies ethical considerations, such as lack of transparency, potential for bias and discrimination.

The research challenge identified in the workshop was related to the trade-off between usefulness of the data versus maintaining maximum privacy. Ensuring maximum privacy while preserving the usefulness of data is indeed a challenging task when using data anonymisation techniques.

Further research is needed on topics such as:

- How to use multiple anonymisation techniques: Different techniques, such as generalisation, suppression, perturbation, and masking, have different trade-offs between privacy and utility. Combining multiple techniques can help to achieve a balance between them.

- How to minimise the amount of data disclosed: Only disclose the minimum amount of data necessary to achieve the desired level of utility, this will help to reduce the risk of re-identification.

4.1.3 Data anonymisation

Data anonymisation is an important tool to scale the use of AI. Perfect anonymisation would “free” AI practitioners from privacy regulations and trust risks, while stimulating innovation, data sharing and data monetisation. It would also enable the use of additional data sets from other parties to enhance existing data sets without adding privacy risk.

Research themes identified at the workshop included:

- **Re-identification:** Even with anonymisation techniques, it may still be possible for individuals to be re-identified through a combination of publicly available information and the anonymised data.

- **Loss of utility:** Anonymisation can sometimes result in the loss of important information that is needed for the research or analysis. This is also captured in the previous research topic.

- **Adversarial attacks:** With the development of sophisticated ML algorithms, anonymised data can still be vulnerable to adversarial attacks, where an attacker could re-identify individuals by exploiting weaknesses in the anonymisation process.

- **Dynamic data:** anonymising dynamic data such as social media or IoT devices presents new challenges as the data updates frequently and may contain contextual information which can be used to re-identify the individuals.

- **Unstructured data:** most anonymisation processes are carried out on structured data, however, there is an enormous amount of unstructured data such as text, images/video and audio that also needs to be anonymised before it can be used at scale for AI.

- **Assessing the risk:** assess the risks of re-identification and other privacy threats before releasing the data.

4.1.4 Synthetic data

Synthetic data is important because it allows realistic data to be generated that can be used for AI research, analysis, and testing without compromising the privacy of individuals.

The current state of synthetic data is rapidly evolving, with advances in technology, also because of the growing awareness of the importance of protecting personal data. Some trends that are currently shaping the field of synthetic data include:

1. Improved data generation methods: New algorithms and techniques are being developed to generate synthetic data that is more realistic and representative of real-world data.

2. Increased adoption: More organisations are recognising the benefits of synthetic data and are starting to implement it in their operations, particularly in industries such as healthcare and finance.

3. ML and AI-based synthetic data: The use of synthetic data in ML and AI is becoming more prevalent, and synthetic data is increasingly used to train models and algorithms.

4. Open-source libraries: There are several open-source libraries available for synthetic data generation, which makes it more accessible to the wider community.

As the field of synthetic data continues to evolve, it is likely that new technologies and techniques will emerge to further improve the quality and realism of synthetic data.

Research challenges of synthetic data include:

1. Representativeness: Synthetic data needs to be representative of the real-world data it is meant to replace, this can be a challenge as the data may contain complex interactions between variables and different populations.

2. Data bias: Generated synthetic data may contain bias if the underlying data used to generate it is biased.

3. Evaluation of synthetic data: Evaluating the quality of synthetic data and its representativeness is still an open research challenge.

4.2 Scaling AI

Most MNOs have started to use AI to improve their businesses in several different respects, as we have seen. However, a remaining challenge is how to scale the use of AI to every corner of the business: optimisation, operation, marketing, customer interaction, new products and services, new business opportunities, and horizontally in digital transformation processes.

4.2.1 Standardisation of “commodity” telecommunications use cases

Standardisation of the most-commonly used use cases of AI in the telecommunications industry will help to speed up the scaling of AI.

Research is needed to define how standard should look like; potentially including the purpose of the use case, the business case, the data needed, privacy-related aspects, the algorithm or algorithms that can be applied to the data, potential security issues, operational aspects to consider, and the potential ethical or social impacts to be considered.

4.2.2 AI industrialisation with MLOps

Another topic that needs to be applied on a wider scale is related to the concept of MLOps (Machine Learning Operations), which entails the implementation of a set of processes and practices that enable the efficient and effective development, deployment, and management of AI models. While this is already a well-known concept in AI, it needs to be applied on a wider scale. Research is therefore desired to improve or automate one or more of the following topics:

1. Automating the model development and deployment process, such as automated testing, continuous integration, and continuous delivery of AI models. It is also related to data foundations.

2. Monitoring and management of AI models in production, such as monitoring model performance, detecting and diagnosing issues, and implementing automated rollbacks and updates.

3. Collaboration and version control, such as using tools such as Git to collaborate on model development and track changes, as also Kubernetes to deploy models and manage their infrastructure.

4. Data management, such as managing the data used to train and test models, as well as managing the data used to make predictions in production.

5. Ethics and compliance, such as ensuring that AI models and the data used to train models comply with legal and ethical standards.

4.3 AI applied to the network

As mentioned in chapter 3, the telecommunications industry is using AI to improve its core infrastructure, the network, in several ways. In this section, we enumerate several other applications of AI to the network that require more research before they can be applied at scale.

*Notice that the AI research topics included that are applicable to the network are relevant and actionable for MNOs. The research agenda does not necessarily include topics that are in the realm of traditional network providers and vendors.

4.3.1 5G core and RAN

AI can help reduce costs in 5G core and RAN (Radio Access Network) by automating tasks, optimising network performance, network slicing and improving security. Therefore, research on the following topics is of interest for the industry:

1. Automation of network management tasks: AI can be used to automate tasks such as network optimisation, troubleshooting, and maintenance, reducing the need for manual intervention and reducing labour costs.

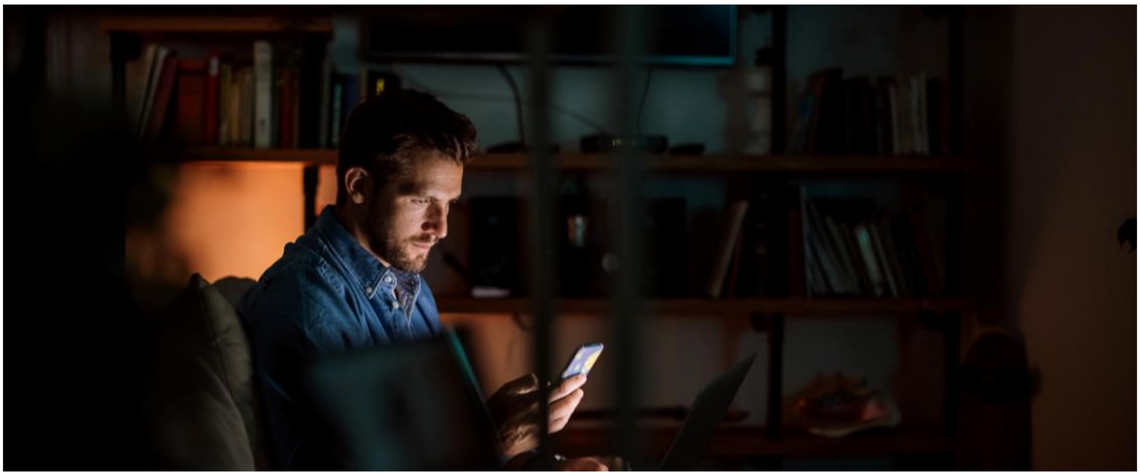
2. Predictive maintenance: AI can be used to predict when equipment is likely to fail, allowing for proactive maintenance and reducing the need for costly repairs and downtime.

3. Self-organising networks: AI can be used to optimise network configuration and adapt to changing network conditions, reducing the need for manual configuration and increasing network efficiency.

4. Traffic optimisation: AI can be used to optimise the allocation of resources in real time, reducing the need for expensive over-provisioning and increasing network capacity.

5. Quality of Service: AI can be used to dynamically adjust the Quality of Service based on the traffic demands, reducing the need for expensive over-provisioning of resources.

6. Security: AI can be used to detect and respond to security threats in real time, reducing the risk of costly security breaches and enhancing the overall security of the network.



4.3.2 Near real-time optimisation of network

Near real-time optimisation of network can contribute to energy efficiency through the notion of smart energy management: AI can be used to predict and optimise the energy consumption of the network, by dynamically adjusting the energy consumption based on traffic demand and network conditions, leading to energy savings and environmental benefits.

4.3.3 Network automation

Network automation refers to the use of software and technology to automatically manage and configure network devices and systems. This can include tasks such as provisioning new devices, monitoring network performance, and troubleshooting issues. The goal of network automation is to improve efficiency and reduce the need for manual intervention, which can help to minimise errors and reduce costs.

According to Alot[9], “Closed-loop automation in Communication Service Provider (CSP) networks is a continuous process that monitors, measures, and assesses real-time network traffic and then automatically acts to optimise end-user Quality of Experience (QoE). CLA continuously:

- Identifies types of network traffic and collects performance metrics
- Calculates bandwidth demands and resource availability
- Maps these metrics to user service levels and perceived QoE
- Instantly sets optimal bandwidth allotment for each traffic component

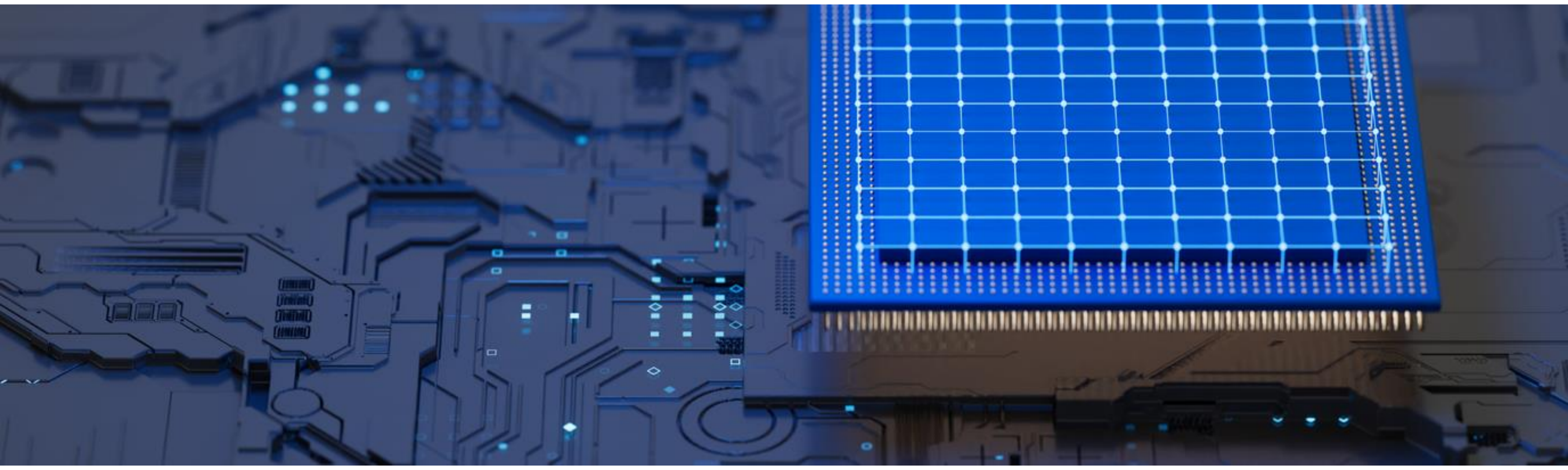
It is also called Zero touch management (ZTM), which refers to the ability to deploy, configure, and manage network devices and systems without the need for manual intervention. The goal of ZTM is to automate as much of the network management process as possible, from initial deployment to ongoing maintenance and troubleshooting. Top of Form Bottom of Form

4.3.4 Anomaly detection

There are several research issues in anomaly detection, including:

1. Scalability: Anomaly detection algorithms need to be able to handle large amounts of data from various sources, such as network traffic and sensor data, in real time and with low latency.
2. False positives and negatives: Anomaly detection systems need to be able to accurately distinguish between true anomalies and false alarms.
3. Adaptability: Telecommunications systems are constantly changing and evolving, so anomaly detection algorithms need to be able to adapt to these changes.
4. Data privacy and security: MNOs need to protect sensitive customer data, so anomaly detection systems need to be able to do so while still providing accurate results.
5. Handling imbalanced data: Anomaly detection algorithms often struggle with imbalanced datasets, where the number of normal instances is much higher than the number of anomalous instances.

[9] https://www.allot.com/network-intelligence/technology/closed-loop-automation/



4.3.5 Explainable AI on anomaly detection

As the telecommunications industry is heavily regulated, it is important to be able to explain the decision-making process of the anomaly detection algorithms to auditors, regulators, and customers if required.

4.3.6 From correlation to causality

This is a relevant research topic as moving from correlation to causation enables the active control of parameters and establishes a link between actions and desired outputs; and enable scenarios to be created that cannot be monitored/inferred from real world data (counterfactual learning).

There are, however, several challenges that need to be overcome. In ML, getting from correlation to causation is not a straightforward task and requires additional information and methods. Correlation is a measure of the relationship between two variables, while causation is a relationship in which a change in one variable causes a change in another variable. Methods that can be used to infer causation from correlation include:

1. Controlled experiments: One of the most reliable ways to establish causation is through controlled experiments, where a variable is manipulated and the effect on other variables is measured.
2. Time ordering: If a variable precedes a change in another variable, it is more likely to be the cause.
3. Mechanistic explanation: If a plausible mechanism can be identified that explains how a variable could cause a change in another variable, this can help to infer causation.
4. Reverse causality: If there is a chance that the causality may be reversed, it is important to consider this possibility and test it.
5. Additional data: By collecting more data, such as data on other variables that might be confounding the relationship, it may be possible to infer causality.

4.3.6.1 Scalability of complex causation models

Complex causation models can be difficult to scale because they require a large amount of data and computational resources and may not generalize well to new situations. It is important to balance the complexity of the model with the available data and computational resources to make sure the model is both accurate and scalable.

4.3.6.2 Data collection framework

Data collection for generating complex causation models is not trivial and may require a combination of different methods, such as surveys and questionnaires, controlled experiments, data mining, among others.

4.3.6.3 Identifying confound variables in complex models

A spurious correlation is a situation where two variables are statistically related (correlated), but there is no causal link between them. This relationship is often caused by a third variable that is not being accounted for, called a confounding variable, or a hidden variable. There are several methods to identify and confounding variables, but it is not always possible to identify and control all confounding variables in a complex causal model.

4.3.7 Digital twins

Digital twins, which are digital replicas of physical systems, can offer a number of opportunities. Several of the research topics presented so far can also be seen as part of a digital twin of the network. Research on network digital twins could potentially lead to the following benefits:

- Network optimisation: Digital twins can be used to simulate and optimise network performance, allowing for more efficient use of resources and improved service quality.
- Predictive maintenance: Digital twins can be used to monitor the health of network equipment, predict when maintenance will be needed, and optimise maintenance schedules.
- Network design and planning: Digital twins can be used to test new network designs and configurations before they are deployed in the field, helping to identify and resolve potential issues before they become problems.
- Real-time monitoring: Digital twins can be used to monitor network performance in real-time, providing insights into network behaviour and enabling quick response to any issues that may arise.
- Improved customer experience: Digital twins can be used to monitor network performance from the customer's perspective, providing insights into customer experience and enabling proactive resolution of any issues that arise.
- Cost reduction: By using digital twins to optimise network performance, predict equipment failures, and improve network design, telecommunications companies can reduce costs associated with network maintenance, downtime, and customer complaints.

Overall, digital twins can help improve network performance, reduce costs, offer better products to large enterprise customers, and enhance the overall customer experience.

4.3.8 Network as a Service (NaaS)

Network as a Service (NaaS) is a type of service model that allows businesses and organisations to outsource the management and maintenance of their network infrastructure to a third-party provider. Reaching the full potential value of telecommunication networks such as 5G, WiFi6 or Edge Computing requires to progress MNOs' digital transformation into the next level and to extend softwarisation into the connectivity services development process and how these connectivity services are integrated with other digital services. The cornerstone for this to happen is network APIs (Application Programming Interface)[10].

NaaS provides a flexible, scalable, and cost-effective way for companies to access and manage their networks, without the need for significant capital expenditures or in-house expertise. It enables customers to consume network resources as a service, similar to how they consume other utility services like electricity or water. This allows customers to focus on their core business functions and reduce the burden of managing and maintaining their own networks.

Traditional NaaS providers typically offer a range of network services, such as virtual private networks (VPNs), wide area networks (WANs), and software-defined networking (SDN). This can include the provisioning, configuration, monitoring, and management of network resources, as well as additional services such as security and compliance. However, with the upcoming metaverse and web3, network capacity will be needed on demand for high-demanding applications through APIs. Such network APIs represent a change in the way network resources are consumed, so that network capabilities can be incorporated into applications (by the MNOs themselves or by third parties) in a programmatic way, encouraging a much more agile environment for innovation and co-creation of services.

There is an expectation that AI can significantly contribute to the creation, consumption and maintenance of such network APIs.

As a concrete example[11] pilot of NaaS, consider Network as a Service (NaaS) for bandwidth control. Singtel has run a field trial based on surveillance drones. These drones send SD (standard definition) video to a central control centre. When a human operator at the central control centre observes a specific event or anomaly in the video sent by one of the drones, the operator may need a more detailed view with a higher resolution. With one click, the operator asks the drone to send HD (high definition) video

[10] https://www.telefonica.com/en/sustainability-innovation/innovation/open-gateway/

[11] https://www.gsma.com/futurenetworks/wp-content/uploads/2022/03/GSMA-TEC-Value-Whitepaper-v13.pdf

to the control centre to immediately see in greater detail the thing the operator wishes to inspect.

From a network connectivity point of view, all drones, during regular operation, are sending video in standard definition resolution to optimise the mobile data bandwidth usage. However, the drone application allows the user to switch to high-definition resolution in real-time via a NaaS (Network-as-a-Service) API, which enables device connectivity characteristics to be changed, such as data bandwidth, as in this case, or the Quality of Service (QoS) literally on the fly. At MWC 2023 in Barcelona, NaaS is referred to as the Open Gateway initiative of the GSMA[12].

4.4 Operations and marketing

In the previous section, we have identified AI research topics which applied typically to the MNOs, the network. However, MNOs have also many business processes in common with other industries such as marketing and operations, etc. This section discusses additional relevant AI research topics.

4.4.1 Real-time AI

Real-time AI refers to the use of AI algorithms and systems to process and analyse data in real-time, as it is being generated. This enables faster decision-making, automated actions, and the ability to respond to changing conditions quickly. Some examples of real-time AI applications include real-time marketing, industrial automation and predictive maintenance.

4.4.2 Combining optimisation and machine learning

Any business process that leaves a digital trail can be optimised with AI. ML can be used to improve optimisation by providing a better understanding of the process or problem, guiding the search for an optimal

[12] https://www.gsma.com/futurenetworks/gsma-open-gateway/

solution, and making it possible to handle more complex and dynamic optimisation problems. ML can be applied to optimisation in several ways, including:

1. Model-based optimisation: using ML techniques, such as regression or neural networks, to create a model of the system being optimised. This model can then be used to predict the optimal solution for a given set of inputs.

2. Heuristic optimisation: using ML techniques, such as genetic algorithms or particle swarm optimisation, to generate heuristics that can be used to guide the search for an optimal solution.

3. Reinforcement learning: using ML techniques to train an agent to make decisions that will lead to the best long-term outcome. This can be applied to optimisation problems where there is a clear reward or objective function.

4. Bayesian optimisation: using ML techniques to model the uncertainty of the optimisation problem and use this information to guide the search for an optimal solution.

5. Multi-objective optimisation: using ML techniques to optimise multiple objectives at the same time, it can be used to find the trade-offs between different objectives.

4.5 Customer interaction (chatbots and virtual assistants)

Chatbots and virtual assistants are helping companies to interact 24/7, 365 with their customers in a real-time and personalised manner. Current research topics that need further investigation include proactivity in the interaction and better dialogue capacities.

4.5.1 Proactivity in the interaction

Proactivity is important in customer interaction as it allows to anticipate the needs of the user and provide relevant information or perform tasks without the user having to specifically ask for it. This can save the user time and improve their overall experience with the assistant. Additionally, a proactive interaction can learn the user's preferences and habits over time, and provide customised and personalised assistance.

It is, however, important to find the right balance between personalisation, and proactivity and, generating the impression of "spamming" the user.

Finding the right balance between personalisation and spam can be achieved through different strategies. One approach is to give users the ability to control the level of personalisation they receive, allowing them to opt-in or opt-out of certain types of personalised content or notifications. Additionally, one could provide transparency about how user's data is used, and provide clear and easy-to-understand settings for managing personalisation preferences. Another approach is to use ML algorithms that can detect and filter out unwanted or irrelevant content, while still delivering personalised content that is of value to the user.

Further research is needed to determine the best approaches.

4.5.2 NLP and conversational AI

4.5.2.1 From QA to coherent dialogues

So far, most chatbots AKA conversational assistants, are more oriented towards question-answering and FAQs rather than to hold coherent conversations about individual interests. This is changing with generative AI developments such as ChatGPT, that to some extent can hold a dialogue.

Generative AI refers to a type of AI system that is capable of creating new and original content, such as text, images, music, or even videos, that has never been seen before. Many of the state-of-the-art generative AI models, such as GPT-3, use transformer architectures. Transformers are a type of neural network architecture that have revolutionised natural language processing (NLP) by allowing models to process entire sequences of input data (such as sentences or paragraphs) all at once, rather than one word at a time.

Generative AI systems can be used for a wide range of applications, such as creating realistic images for computer games, generating new product designs, writing creative stories, or composing music. One of the most well-known examples of generative AI is GPT (Generative Pre-trained Transformer), which is a language model that can generate human-like text based on a given prompt or topic.

One of the key challenges in developing generative AI models is ensuring that the generated content is of high quality and does not contain errors, hallucinations or inconsistencies. This requires careful training of the model and ongoing refinement to ensure that it continues to generate accurate and high-quality content.

Further research is required to ensure enterprise quality of all answers produced by generative AI.

4.5.2.2 Multi-languages chatbots

Many MNOs are multinational corporations, and their digital assistants or NLP activities require various languages. Sometimes a mix of languages is used in a same dialogue (also known as code alternation, code-switching, or code-mixing: the phenomenon of alternating between two or more languages or language varieties within a single conversation or stretch of discourse.). This is a challenging task as it requires an AI model to be able to identify and handle multiple languages within a single input.

Further research is needed to handle this phenomenon in a satisfactory way.

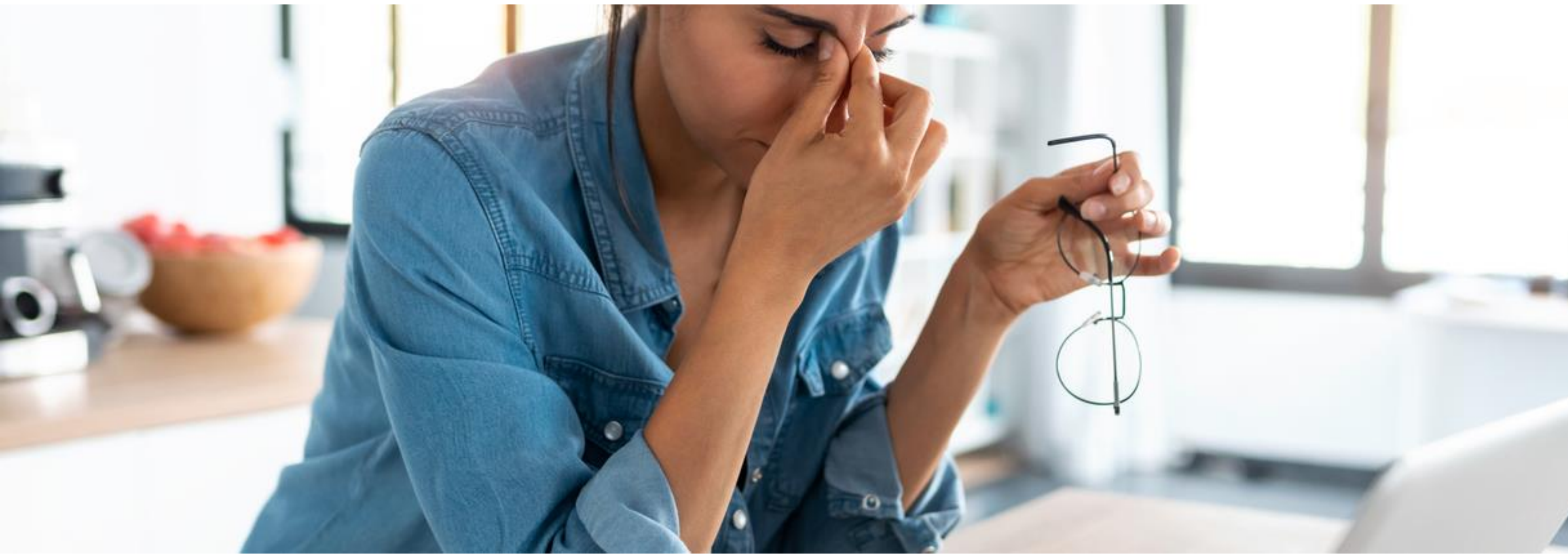
4.6 Responsible business

Responsible business practices are receiving increasing attention for several reasons. Firstly, there is a growing awareness among the general public about the impact that businesses have on society and the environment. Consequently, there is a demand for companies to take greater responsibility for their actions. Secondly, there is an increasing body of research that shows that companies that prioritize social and environmental responsibility tend to perform better in the long-term. This is due to the fact that they are better able to attract and retain customers, employees and investors. Thirdly, governments, non-governmental organisations and other international organisations are putting pressure on companies to be more responsible through regulations, standards, and initiatives. Finally, businesses are acknowledging that being responsible is not only the right thing to do, but also a means of creating value for their stakeholders and building a sustainable future.

One part of responsibility is related to the ethical use of AI. In light of the increasing prevalence of AI, it is imperative that businesses operate with transparency and accountability in their use of it, whilst also ensuring responsible usage. Potential unintended consequences, such as bias, privacy breaches and security risks, must be considered when deploying AI applications. Compliance with applicable regulations and standards is also essential. It is therefore necessary for businesses to use AI in an ethical and responsible manner, given its proliferation across a broad range of industries.

4.6.1 AI ethics

The significance of AI ethics today cannot be overstated as the advancements in AI technology can have both positive and negative impacts on society. While AI has the potential to enhance healthcare, education, transportation, and communication, it can also lead to job losses, biased decision-making, and privacy concerns. To fully harness the benefits of AI while mitigating potential risks, it is imperative that AI be designed, developed and deployedin an ethical and responsible manner. Furthermore, as the application of AI becomes more prevalent, there is an increasing need to deliberate on the ethical implications of this technology.



Ethical AI is a matter of great concern at both the European and international levels evidenced by, for example, the upcoming AI Act. There are, however, several countries that are falling behind, which may have significant implications in the context of a global economy. The growing number of institutes and recommendations on the topic of AI ethics, the large volume of research papers, and the numerous AI ethics-related events happening worldwide underscore the importance of the matter.

The ethical use of AI has been embraced by the telecommunications industry, evidenced by the published ethical AI Playbook[13] and self-assessment questionnaire[14] created by several MNOs in coordination with the GSMA. Moreover, ETNO and GSMA have created a joint AI taskforce[15] for which ethics is an important topic.

Not only is ethical AI the right course of action, it also has practical benefits for businesses. The Economist in its article Staying ahead of the curve – The business case for Responsible AI[16] lists multiple business reasons on why it is important to implement responsible AI:

- Improves firm's top- and bottom-line growth by increased customer engagement, broadened revenue streams, procurement advantages in competitive bidding processes, and increased pricing power in the marketplace;
- A potential source of competitive advantage through enhanced product quality;

[13] https://www.gsma.com/betterfuture/resources/ethicsplaybook
[14] https://www.gsma.com/aiethics-saq/
[15] https://etno.eu/library/positionpapers/446-etno-gsma-position-paper-on-european-commission-proposal-for-an-artificial-intelligence-act.html

[16] https://www.eiu.com/n/staying-ahead-of-the-curve-the-business-case-for-responsible-ai/

- Sustainable investing and strengthen relationships with stakeholders, including competitors, industry associations, academia and governments;
- Better data management, security and privacy;
- Better talent acquisition, retention and engagement; and
- Better preparedness and readiness for imminent AI regulation.

Whilst ethical AI is being promoted and currently implemented in the telecommunications industry, there are several topics that require additional research effort.

4.6.1.1 Deliver homogeneous risk qualification

Most approaches for the ethical use of AI are risk-based: the higher the risk, the more ethical and legal checks need to be performed to ensure no negative consequences. The European AI Act indeed is risk-based, identifying uses of unacceptable, high, limited, and low risk. Nevertheless, determining the potential hazards of an AI system in a uniform manner across diverse sectors is a complex task that calls for additional investigation.

4.6.1.2 How to include external providers

In the telecommunications industry, (AI) systems are often procured from providers in the market. How to enforce and ensure the requirements of ethical AI across the value chain in an automatic and consistent way is an important research topic for the telecommunications industry.

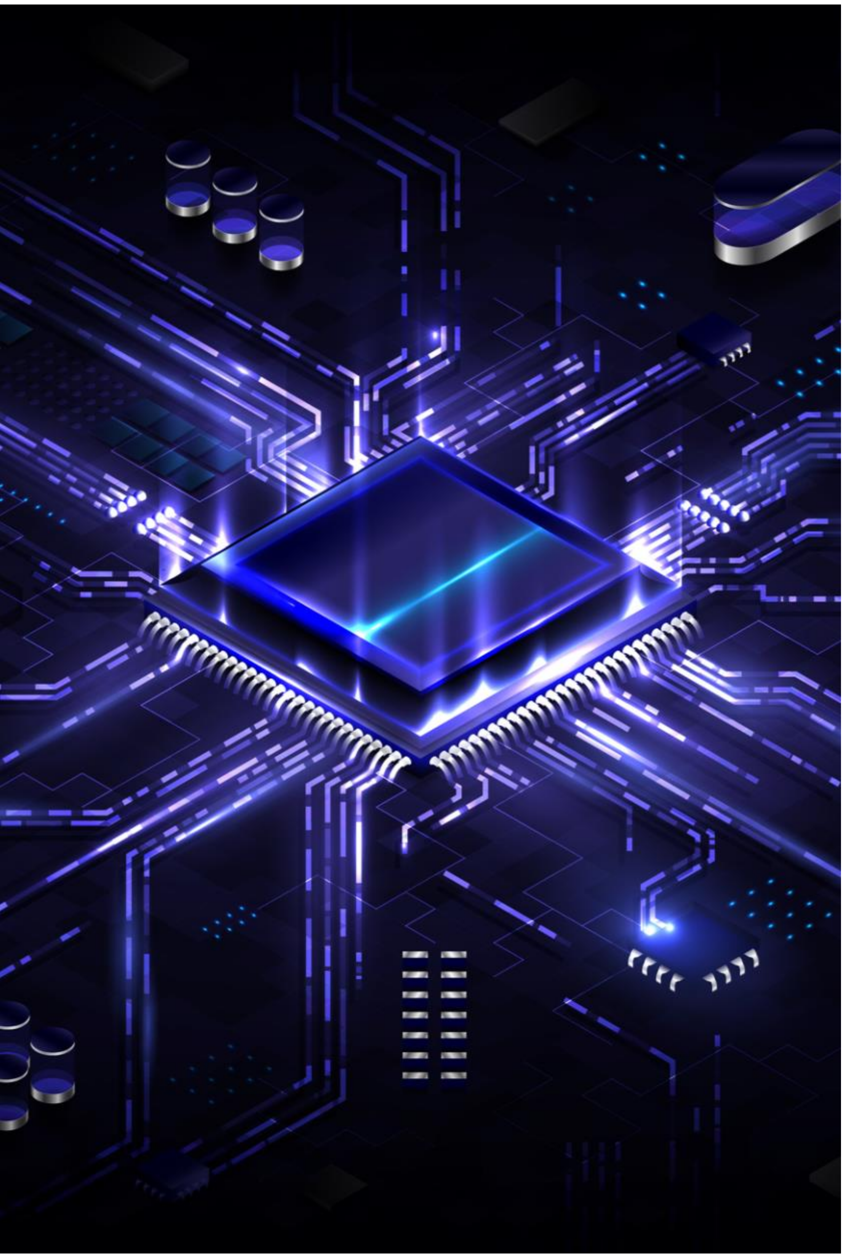
4.6.1.3 Tools for ethical AI

Although there are numerous AI Ethics documents that have been published by governments, international organisations, civil society and the private sector, putting principles into practice and assessing whether AI systems and applications are following the principles is one of the most challenging issues for private sector as well as MNOs. Three of the main challenges for the ethical use of AI are privacy, bias and explainability.

4.6.1.3.1 Privacy tools

When used and progressed in a responsible and ethical manner, AI technology presents greater potential, and the importance of data cannot be overstated in this field. While data use is prevalent in AI, it can undermine trust in the technology's efficacy. For this reason, AI technologies that prioritise privacy preservation are poised to outperform others.

As privacy is an inalienable right that has been enshrined in all international and regional human rights instruments as well as national legal systems, it is imperative that further



research be conducted on tools to address the mounting concerns arising from the intersection of privacy and AI as already explained in Section 4.1.2

4.6.1.3.2 Bias tools

Bias in AI refers to the systematic error that can occur when an algorithm is trained on data that is not representative of the population it will be used on. This can lead to unfair, inaccurate, or discriminatory decisions. For example, if an AI system is trained on a dataset that contains mostly images of light-skinned individuals, it may not be able to accurately recognise or classify individuals with darker skin tones. Similarly, if an AI system is trained on data that has been collected in a biased manner, it may perpetuate or even amplify the biases present in the data. Bias in AI can also occur when the algorithm is designed in such a way that it gives preferential treatment to certain groups over others.

There are various types of bias that can occur in AI, such as:

- Representation bias, which occurs when an algorithm is trained on a dataset that does not accurately represent the population it will be used on.
- Measurement bias, which occurs when an algorithm is trained on data that has been collected in a biased manner.
- Algorithm bias, which occurs when an algorithm is designed in such a way that it gives preferential treatment to certain groups over others.

Managing and mitigating bias in AI is an important and ongoing challenge, and it requires a multi-disciplinary approach that involves computer scientists, data scientists, statisticians, and social scientists.

Broadly speaking, there are three methods to detect and mitigate bias in AI:

1. Pre-processing: These techniques are applied before the ML algorithm is trained in order to remove biases in the very early stage of the learning process. This involves for example techniques such as oversampling and under-sampling to balance the dataset and reduce bias.

2. In-processing: These techniques are applied during the training process by including fairness optimisations constraints along with cost functions in ML models. For example, fairness constraints are mathematical equations that are used to ensure that the model does not discriminate against certain groups. Or adversarial training which is a technique where the model is trained using inputs that are specifically designed to fool the model, in order to make it more robust against bias.

3. Post-processing: Employed after the algorithm is built, these are the less intrusive techniques because they do not modify the input data or the ML algorithm. This technique is especially appropriate for mitigating biases in models that already exist.

Each technique applies the mitigation process in different phases of a typical analytics pipeline and the choice must be made to fit the particular case, but in terms of model performance, it is better to apply pre-processing or in-processing techniques.

In addition, once the model is ready, several tests can be applied to test and verify that no unfair bias exists, including:

- Auditing, which involves testing the model with a variety of inputs to check for any disparities in the output.

- Counterfactual analysis, which involves examining what the model's output would have been for a specific input if certain features of the input were different.

- Transparency, by providing visualisations and explanations of the model's decision-making process, to make it easier to detect and correct bias.

4.6.1.3.3 Explainability tools

Explainability is important in AI as it allows for transparency and understanding of how the model is making decisions. This is crucial in many applications, such as finance, where the consequences of a mistake can be severe. Additionally, it can help build trust in the model and increase its acceptability among stakeholders. Explainability also helps identify and correct errors and biases in the model.

A black box model is a model whose inner workings are not transparent or interpretable to the user. The user can input data and receive an output, but they do not have insight into how the model arrived at that output. These models are often considered to be more accurate and efficient, but they can be difficult to understand and trust. Examples of black box models include deep neural networks and many ensemble models.

On the other hand, a white box AI model is a model whose inner workings are transparent and interpretable to the user. The user can understand how the model arrived at its output and can also see the reasoning behind the model's decisions. These models are often considered to be more trustworthy and acceptable to users, but they may be less accurate and efficient. Examples include decision trees, linear regression, and rule-based systems.

It's important to note that there's a spectrum between black-box and white-box models, and some models are considered to be grey-box models, which provide some level of interpretability. Additionally, some methods, like LIME, SHAP and others, can be used to make black-box models more interpretable.

For the techniques and tools to mitigate bias and black box algorithms, the following research topics are important:

- Maturity of tools: proprietary tools versus open source
- Validation and standardisation of tools
- How to select appropriate tools - are there any metrics for tool selection?
- A framework for defining the appropriate level of explainability
- Adapted explanations to different types of users

4.6.1.3.4 Regulation-compliant tools

Self-assessment questionnaires are popular tools for ensuring internal and external compliance. However, most of these tools are still manual. Research is needed to drive automated responses and to maintain results consistent over time.

4.6.1.4 Metaverse ethics and social impact

The Metaverse/Web3 is attracting a huge amount of attention as the next version of the internet, and companies are starting to explore the many new business opportunities it provides. However, based on experience with AI, we know that there will also be potential negative ethical and social consequences of the massive use of technology that must be dealt with.

The metaverse is only just beginning and this creates a unique opportunity to build a metaverse that we want to live in or with. It will have a profound impact on our lives and therefore it is very important -from the start- to think about potential consequences and act accordingly. This will help moving away from the current "break, apologise and fix” approach to a more proactive one. As for many industries, investigating the social and ethical impact of the metaverse is important for the telecommunications industry[17],[18].

4.6.2 Towards sustainable AI

It is estimated that the information technology (IT) sector will be responsible for 20% of emissions in 2030[19]. Faced with this challenge, a new research area has emerged that studies and tries to mitigate this risk: green computing, which consists of two branches:

- **Green by** IT tries to use technology to reduce the carbon footprint, as for example to use AI in the fight against climate change.
- **Green in** IT deals with minimising emissions from the use of IT.

In turn, these two areas can be divided into software and hardware.

4.6.2.1 Green AI and green computing

For AI, what is relevant is the "green in" due to the impact on emissions of AI algorithms, that is, its carbon footprint. Large natural language processing models such as GPT-3, which process 1.5 billion parameters, have a significant carbon footprint. Some studies have shown that training a single model once had the same carbon footprint as five cars over its lifetime[20]. The GPT-3 model training process came with a multimillion-dollar electricity bill. And while this currently only happens with very large models, one should keep in mind that this is the cost of one training session. Before an AI model works well, many training sessions are needed, and large AI models are expected to run in almost any organisation of certain size in the future. To address this unintended negative consequence of AI, various research activities have started to systematically measure the power consumption of AI algorithms with the aim of developing tools for measuring power consumption, creating guides for programming, and selecting AI algorithms that take energy consumption into account by design. The final objective is to measure and limit the data and AI carbon footprint.

This is a key research area given the scale of AI used in the telecommunications industry and the importance of energy efficiency.

---

[17] https://www.telefonica.com/en/communication-room/the-social-and-ethical-challenges-of-the-metaverse/
[18] https://responsiblemetaverse.org/resources/ethical-metaverse-principles/
[19] https://unfccc.int/news/ict-sector-helping-to-tackle-climate-change#:~:text=According%20to%20the%20Global%20e,intelligently%20use%20and%20save%20energy

[20] https://www.technologyreview.com/2019/06/06/239031/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/

4.6.2.2 AI for sustainability

AI for sustainability is a sub area of AI for Good, where AI is used to solve large societal and environmental problems. This is an active area in GSMA's AI4I initiative and also in UN's ITU AI4Good initiative.

A specific AI4I initiative focused on using MNOs mobile big data analytics and AI to estimate the carbon emissions of large infrastructure construction works[21].

Further research is needed to find out whether and how this initiative can be put into practise an add real value at scale to the climate change problem.

4.7 B2B/B2G data sharing and the data economy

Companies are holding vast amounts of data, which -as we have seen in this document- are mostly used to benefit the businesses of those companies. There is, however, also a huge opportunity for data sharing between companies, within and across sectors. This is also referred to as the data economy, an upcoming economy that is still in an incipient state. Currently, there are several organisations whose aim is to stimulate this data economy (IDSA[22], GAIA-X[23], BDVA[24], FIWARE[25]). While today this is mostly a European initiative (referred to as data spaces), it is applicable across the world. As part of the European data strategy[26], new regulations are being

[21] https://www.gsma.com/betterfuture/resources/ai4i-climate-overview
[22] https://internationaldataspaces.org/
[23] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[24] https://www.bdva.eu/
[25] https://www.fiware.org/
[26] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

adopted to stimulate and regulate the data economy, in particular the Data Governance Act[27] and the Data Act[28].

The data economy is important for the telecommunications industry for several reasons:

1. MNOs may benefit from data available in data spaces to improve their business.

2. MNOs hold vast amounts of data, especially network data, that can benefit a variety of other industries, including transport, tourism, healthcare, logistics, retail, etc.

Given the early stage of business to business (B2B) and business to government (B2G) data sharing, there are several issues to be resolved and researched before this phenomenon can scale up.

4.7.1 Standardisation and interoperability of data sets

Standardisation and interoperability are important for sharing data sets between companies and sectors as they ensure the data can be easily exchanged and understood by different systems and software. Without standardisation, data sets may be stored in different formats, use different units of measurement, or have different structures, making it difficult or impossible for one company to use data from another company. Interoperability ensures that different systems and software can work together seamlessly, allowing for the easy exchange of data between companies. This can lead to more efficient and effective collaboration, as well as the ability to combine data from multiple sources for better decision making and analysis.

4.7.2 Trust and sovereignty

Trust is important because it allows organisations to share data with confidence and awareness it will be used in an appropriate and ethical manner. Without trust, organisations may be hesitant to share sensitive or proprietary information, which can limit the potential benefits of data sharing.

Sovereignty refers to the control and ownership of data - governance. Ensuring sovereignty is important as it allows organisations to maintain control over their data and understanding of its access and purpose.

4.7.3 Privacy of personal data

While not all data shared between organisations will be personal data (much data will come from sensors and machines), it is very important to ensure personal data privacy.

[27] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[28] https://digital-strategy.ec.europa.eu/en/policies/data-act

This challenge leads to the same research topics as discussed in Sections 4.1.2. and 4.1.3. Other techniques that help maintain privacy include federated data sharing and federated ML.

4.7.3.1 Federated data sharing

Federated data sharing refers to a method of sharing data across multiple organisations, where each organisation maintains control over its data and the data remains on the original organisation's servers. In a federated data sharing system, the data is not centralised or pooled in a single location, but is instead distributed across multiple organisations. This allows organisations to share data while maintaining control and ensuring compliance with privacy and security regulations.

4.7.3.2 Federated ML

Federated machine learning (FML) is a method of training ML models on distributed data sources without the need to centralize or pool the data. In FML, each data source, or "node", maintains control over its own data and the model training is conducted locally on each node. The local models are then combined, or "aggregated", to form a global model. This allows for the training of models on sensitive or proprietary data without compromising data privacy and security.

4.7.4 Ethical use

A data sharing ecosystem is a very powerful concept on top of which major applications can be built to solve all kinds of big problems or enable new business opportunities. However, that same data can also be used for obscure businesses, undemocratic governmental actions or even for organised crime. It is therefore very important to install a governance system that ensures an ethical use of data.

4.8 Additional research topics

4.8.1 AI as a Service

AI as a service (AIaaS) is a business model in which AI technology is provided as a service over the internet, rather than as a product that is purchased and installed on a customer's own hardware. AIaaS allows organisations to access AI capabilities and expertise without the need to invest in expensive hardware or software, or to hire specialised staff. A clear example is Open AI's GPT family of services including ChatGPT. MNOs could use AIaaS to power their digital assistance and chatbots in multiple languages, as also to offer AIaaS to the market.

This is still an incipient phenomenon, and more research is needed to understand MNOs' role.

4.8.2 Metaverse

The metaverse, a term used to describe a virtual world where users can interact and engage with each other and digital objects, is an opportunity as it presents a new market[29]. As the metaverse becomes more prevalent, MNOs will be able to offer new services such as high-speed internet, 5G networks, and edge computing to support the demands of the metaverse, like streaming and low-latency applications. This is also referred to as Network as a Services (NaaS, see Section 4.3.7), where network capabilities are offered on demand by APIs which will become available through hyperscalers (During MWC23 GSMA launched the Open Gateway AI initiative underpinning this concept). Additionally, MNOs can also explore new revenue streams, such as virtual real estate and virtual goods and services, which are prevalent in the metaverse.

Moreover, MNOs can also leverage the metaverse to improve customer engagement and retention. They can use the metaverse as a platform to offer new and innovative services to customers, such as virtual customer service, a virtual store, and virtual events. Digital Twins may also be handled as a metaverse application.

Since the metaverse is still in its early stage, many research aspects related to the metaverse are relevant for the telecommunications industry. In addition, research topics related to specific mobile applications are also of common importance as well as the social and ethical impact of the metaverse as described in Section 4.6.1.4.

4.8.3 Quantum computing

Quantum computing is important for the telecommunications industry because it has the potential to significantly improve the performance and security of telecommunications networks.

One of the key benefits of quantum computing is its ability to quickly process large amounts of data, which can be used to optimise network routing and improve the

29 https://www.gsma.com/asia-pacific/wp-content/uploads/2022/02/270222-Exploring-the-metaverse-and-the-digital-future.pdf

efficiency of network operations. Additionally, quantum computing can also be used for ML and AI, which can be used to enhance network performance, predict and prevent network failures, and improve security.

Another important application of quantum computing is in the field of quantum cryptography, which uses the principles of quantum mechanics to create highly secure communications. Quantum cryptography can be used to protect against eavesdropping and other forms of cyberattacks, making it an essential tool for securing sensitive data and communications.

Lastly, quantum computing can also be used to simulate complex systems, such as wireless networks, which can help design, test and optimise networks before deployment.

5. Acknowledgements

We would like to thank all the participants of the workshop for their inspiring contribution that has led to this document. Special thanks also to the Humane AI Net project for funding the holding of the workshop. Thanks to German Entrepreneurship for hosting us.

We would also like to thank ChatGPT for helping with some of the text of this document, which has been duly revised before including it.

The workshop that has led to this report received support from the Humane AI Net project funded by the European Commission under Grant Agreement Number: 952026.

6. Annex

Annex 1: Agenda of workshop

09:00 – 09:20	**Welcome remarks** *Delivered by DFKI, GSMA, Telefónica*
09:20 – 10:20	**AI Landscape** *Delivered by Humane AI-Net partners*
10:20 – 10:50	**Regulatory landscape** *Delivered by ETNO, GSMA*
10:50 – 11:50	**AI use: State of Play & 5 years vision** *Presented by MNOs*
11:50 – 12:00	**Coffee break**
12:00 – 13:00	**AI use: State of Play & 5 years vision** *Presented by MNOs*
13:00 – 13:45	**Lunch**
13:45 – 15:15	**Research agenda 1: New business opportunities.** *Moderated session*
15:15 – 16:30	**Research agenda 2: Policy and regulatory aspects** *Moderated session*
16:30 – 16:45	Planning post workshop work
16:45 – 17:00	**Closing remarks** *Delivered by DFKI, GSMA, Telefónica*

Annex 2: Participants in the workshop

Axiata	Ahmed Saady Yaamin	Virtual
O2 Germany	Iryna Dewiwje	FTF
O2 Germany	Dr. Ignacio Santabarbara	FTF
Orange	Thierry Barba	FTF
Orange	Emilie Hien	FTF
Stc	Ziyad Moraished	FTF
Stc	Albatool L. Alaqeel	FTF
Telefonica	Richard Benjamins	FTF
Telefonica	Joaquina Salado	FTF
Telefonica	Silvia Diaz Fernandez	FTF
Telenor	Ieva Martinkenaite	FTF
Telia	Efthymios Stathakis	FTF
Telstra	Lisa Green	Virtual
TIM	De Peppe Raffaele	Virtual
Turkcell	Gokce Cobansoy Hizel	FTF
Vodafone	Edward Ellerby	FTF
DFKI (Humane AI Net Project)	Paul Lukowicz	FTF
DFKI (Humane AI Net Project)	Agnes Gruenerbl	FTF
ETNO	Xhoana Shehu	FTF
German Entrepreneurship	Andreas Keilhacker	FTF
GSMA	Mojca Cargo	FTF

GSMA	Jeanine Vos	Virtual
GSMA	Mahima Dalal	Virtual
GSMA	Niall Magennis	Virtual
Jozef Stefan Institute	Marko Grobelnik	FTF
Ludwig-Maximilians-Universität München	Albrecht Schmidt	FTF

HUMANE AI NET